HOW PRIVILEGE UNDERMINES CYBERSECURITY

Daniel Schwarcz, Josephine Wolff, and 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. To 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 predominantly 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 that are 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 that is 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 zeal to preserve the confidentiality of incident response efforts, lawyers frequently 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 forensic firms and clients, insist on hiring forensic firms that have no familiarity with the client's

[*] Schwarcz (Schwarcz@umn.edu) is the Fredrikson & Byron Professor of Law, University of Minnesota Law School. Wolff (josephine.wolff@tufts.edu) is associate professor of cybersecurity policy at The Fletcher School at Tufts University. Woods (daniel.woods@uibk.ac.at) is a Lecturer of Cybersecurity at the University of Edinburgh's School of Infomatics. For helpful comments and suggestions, we thank Matthew Bodie, Rainer Böhme, danah boyd, Jim Graves, Gus Hurwitz, Orin Kerr, Jeff Kosseff, Susan Landau, Jamie MacColl, Bill McGeveran, Sasha Romanosky, Alan Rozenshtein, Jayshree Sarathy, Andy Sellars, 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.

networks or internal processes, and strictly limit dissemination of the forensic firm's conclusions to the client's internal personnel. To ensure that any legal confidentiality protections are not inadvertently waived by their clients, 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 forensic firms not to craft any final report regarding a breach whatsoever. These practices, we find, substantially 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 that 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

INTRODUCTION

In recent years, attacks on the computer systems of corporations, non-profits, 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 undermined consumer privacy, [3] distorted world geopolitics, [4] and even resulted in death and bodily harm.[5] Efforts to prevent

[1] *See, e.g.*, 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. 296, 320 (2019); Sasha Romanosky, *Examining The Costs And Causes of Cyber Incidents*, 2 J. CYBERSECURITY 121, 129-33 (2016).

[3] *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (2019); Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM L & CRIMINOLOGY 667 (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 (2018); Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520 (2020).

[5] 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 CAL. L. REV. 513, 515 (2015).

or mitigate the consequences of such cyberattacks abound; potential victims spend massive sums attempting to harden their computer systems and insure against the prospect that these defensive efforts will fail,[6] while governments at every level implement policies designed to promote cybersecurity.[7] And yet, the risk of cyberattack only continues to climb.[8]

The rising risks of cyberattacks have not, however, been bad news for many lawyers. To the contrary, lawyers that 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. Moreover, while cyberattacks that jeopardize individuals' personal data can indeed raise significant legal questions under state breach notification laws,[12] many cyberattacks—including the

---

[6] *See* Charlotte Tschider, *Locking Down 'Reasonable' Cybersecurity Duty*, YALE LAW & POLICY REV. (2022, Forthcoming); Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 995 (2018).

[7] *See* Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 812 (2020); 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 (January 2022).

[10] *Id.*

[11] More than 4,000 cyber-incidents in 2018 were handled in this manner. *See* ADVISEN'S CYBER GUIDE: THE ULTIMATE GUIDE TO CYBER SERVICE PROVIDERS (2019), https://www.advisenltd.com/2019-Cyber-Guide-Survey. Similarly, the cybersecurity firm Crowdstrike reports that 50 percent of its investigations were directed by an attorney in 2020. *See* CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT (2020), at https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf. 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 DEFENSE QUARTERLY (2020), at http://www.icemiller.com/MediaLibraries/icemiller.com/IceMiller/PDFs/publications/IDQ-2020-01-Reynolds-Kim.pdf.

[12] *See, e.g.*, Mark Verstraetea1 & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803 (2021). 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*

ransomware attacks that now predominate[13]—do not necessarily trigger these legal complexities.[14] Yet firms that experience a non-cyber accident or intrusion typically only hire lawyers when they need assistance resolving specific legal questions or are on notice of a potential lawsuit, and they rarely rely on these lawyers to coordinate all non-legal elements of their response.[15]

Lawyers' dominant role in cyber-incident response is driven predominantly by their purported capacity to ensure that information that is produced during the breach-response process remains confidential, particularly in any subsequent lawsuit.[16] Attorneys are uniquely able to provide this protection by interposing themselves between a client and any third-party consultants that are 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.[17] 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.[18]

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

---

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 unless and until a potential lawsuit emerges. *See generally* Daniel J. Solove & 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 under-developed the law is in this arena. *See* McGeveran, *supra* note 3; Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1508 (2017).

[13] *See* Tom Baker & Anja Shortland, *Government and Insurance: Lessons for Ransomware*, REGULATION AND GOVERNANCE (forthcoming, 2023).

[14] 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.

[15] 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 INSURANCE SERVICES OFFICE, COMMERCIAL GENERAL LIABILITY COVERAGE FORM (2012). Even then, a general liability insurer will typically not appoint a lawyer to hire an insured unless and until suit is actually brought.

[16] *See infra* Part II.

[17] *See, e.g.*, United States v. Kovel, 296 F.2d 918, 922-23 (2d Cir. 1961).

[18] Fed. R. Civ. P. 26(b)(3)(A)(i)-(ii).

of individuals' personal information.[19] Legal costs and settlement fees were often 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, such as ransomware, where litigation was less common and legal fees represented a smaller portion of overall remediation and recovery costs.[20] 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, meaning that successful efforts to avoid disclosure through other legal processes can shield firms from reputational and regulatory consequences.[21] 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.

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 zeal to preserve the confidentiality of their clients' incident response efforts, lawyers frequently undermine the long-term cybersecurity of their clients and society more broadly.[22] In large part, this outcome stems from

---

[19] *See* SOLOVE & HARTZOG, *supra* note 1, at 17-34.

[20] *See* Josephine Wolff & Bill Lehr, *Roles for Policymakers in Emerging Cyber Insurance Industry Partnerships*" TPRC 46: THE 46TH RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND INTERNET POLICY 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3141409.

[21] *See* Paul Vaaler & Brad Greenwood, *Do Us State Breach Notification Laws Decrease Firm Data Breaches?* (Draft, 2022).

[22] 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, 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. INF. SOC. 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. 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. 1-125, 11 (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?scroll=1&related=1 (last accessed Oct. 30, 2021). Some courts, however, have dismissed these concerns. *See In re* Cap. One Consumer Data Sec. Breach Litig., No. 1:19MD2915, 2020 WL 3470261, *7, n.8 (E.D. Va. June 25, 2020).

lawyers' efforts to orchestrate cyber-incident response so as to maximize the chances that attorney-client privilege and work product protections will attach. Towards 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 on hiring forensic firms to assist with incident response that have 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 any legal confidentiality protections are not inadvertently waived by clients, lawyers also routinely refuse to share any written documentation regarding a breach with third parties like insurers, regulators, and law enforcement.[23] Collectively, these lawyer-driven strategies substantially impair impacted firms' ability to learn from cybersecurity incidents and implement long-term remediation efforts. Furthermore, they inhibit insurers' efforts to understand the efficacy of different security countermeasures[24] and regulators' capacity to investigate cybersecurity incidents.[25]

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.[26] At bottom, this is because cyber-incident response virtually always involves a thorny blend of legal and business considerations, both of which fundamentally rely on technical expertise that can only be supplied by third-party cybersecurity firms. Yet the doctrines 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, on the one hand, or business-oriented goals, on the other.[27]

The uncertain protections that attorney-client privilege and work product immunity provide for lawyer-coordinated breach response efforts is nicely

---

[23] 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).

[24] 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. (forthcoming, 2022); Asaf Lubin, *Insuring Evolving Technology*, 28 CONN. INS. L.J. 130 (2022); Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Business,* 43 LAW & SOC. INQ. 417 (2018).

[25] 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 (2014); Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1331 (2008).

[26] *See* Sedona Report, *supra* note 22.

[27] *See infra* Part I.

illustrated by the pivotal 2020 *Capital One* case.[28] That case arose out of 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.[29] 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. Towards 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. After months of investigation, Mandiant wrote a final report that included a thorough timeline of the breach as well as 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.[30] 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.[31]

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, a federal district court held that Capital One must turn over the report to plaintiffs.[32] The court reasoned that the Mandiant 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."[33] In reaching this conclusion, the court

---

[28] *See In re* Cap. One Consumer Data Sec. Breach Litig., No. 1:19MD2915 (AJT/JFA), 2020 WL 3470261 (E.D. Va. June 25, 2020). *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, 193 (E.D. Va. 2019).

[29] 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.

[30] 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. APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS, 1 (2013), https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf; MARSHALL HEILMAN & CHRISTOPHER GLYER, *South Carolina Department of Revenue: Public Incident Response Report*, (2012), https://oag.ca.gov/system/files/Mandiant%20Report_0.pdf.

[31] *See In re Cap. One*, 2020 WL 3470261.

[32] *See id.*

[33] *Id.*

emphasized, among other things, 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.[34]

The *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 that they spearheaded.[35] 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. 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 more strictly communicating that the forensic firm's sole role is to assist counsel in providing legal services to the client.

Second, and even more troublingly, *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 in the wake of *Capital One*, 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.[36] To be sure, lawyers conducting internal investigations often opt for oral rather than written reports to limit litigation risk.[37] But lawyers that impose this practice on forensic firms' breach response efforts, we conclude, dramatically impair the ability of both breached firms and third parties to prevent future cyberattacks.

We detail these conclusions in three Parts. First, Part I lays the foundation for the analysis by examining attorney-client privilege and work product

---

[34] *See id.*

[35] *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?scroll=1&related=1. Even prior to *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. Kosseff, *supra* note 22, at 261-62. Similarly, a detailed 2020 report from the Sedona Conference Working Group on Data Security and Privacy Liability notes 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 22.

[36] *See infra* Part II.

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

doctrines in the context of pre- and post-breach cybersecurity efforts. In doing so, Part I emphasizes the uncertainty that this law creates with respect to firms' ability 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.

The heart of the Article is contained in Part II, 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 *Capital One* and lawyers' resulting efforts to preserve the confidentiality of firms' cybersecurity efforts. These strategies, Part II shows, substantially impact everyone involved in incident response, including the forensics specialists carrying out those investigations, the impacted firms' personnel who are tasked with remediating the breach and bolstering the firm's cybersecurity, the insurers responsible for covering costs associated with these incidents, and regulators who may want to further investigate the breaches. Part II also details how these effects can, and often do, weaken the cybersecurity efforts of both impacted firms and society more broadly.

Finally, Part III considers possible interventions to address the challenges that confidentiality concerns create for cybersecurity. It ultimately suggests 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, the Article aims to remove existing barriers to effective incident response while preserving incentives for firms to take cybersecurity seriously.

I. 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.[38] The two primary legal tools that firms use to help achieve this goal are familiar to lawyers: the attorney-client privilege and work product doctrines. The former protects all oral and written

[38] *See, e.g.*, Melanie L. Cyganowski, Erik B. Weinick & Aisha Khan, *Protecting Privilege in Cyberspace, the Age of COVID-19 and Beyond*, NY LITIGATOR (2020); Brian Mund & Leonard Bailey, *Privilege in Data Breach Investigations*, DOJ JOURNAL OF FEDERAL LAW AND PRACTICE (2021).

communications between privileged persons that are made in confidence for the purpose of providing or obtaining legal advice.[39] Crucially, this privilege extends to communications between attorneys and third-party consultants, such as cybersecurity firms, that attorneys rely upon to provide legal advice to a client.[40] Work product immunity provides distinct, but often overlapping, assurances of confidentiality. In particular, it shields from discovery documents or mental processes of attorneys and their consultants that are prepared in reasonable anticipation of litigation or for trial.[41] Like the attorney-client privilege, then, 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.[42] In part, this is because the rules governing these doctrines vary across states, on the one hand, and federal and state courts, on the other.[43] Just as importantly, courts applying these doctrines frequently embrace vague multi-factored tests, resulting in courts reaching seemingly inconsistent holdings in apparently similar cases, while latching on to factual distinctions that even the most sophisticated firms and lawyers fail to anticipate.[44] Finally, some key legal questions–such as the applicability of the common interest doctrine to communications between breach-counsel and cyber-insurers–remain largely unanswered in the caselaw due to commonly accepted, though highly contestable, narratives about what practices are necessary to preserve confidentiality.[45]

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 breach will result in that work being privileged or protected by work product immunity. Section B then considers when a cybersecurity consultant's work prior to a potential breach may be deemed confidential. Finally, Section C considers

---

[39] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (2000).

[40] *See, e.g.*, United States v. Kovel, 296 F.2d 918, 922-23 (2d Cir. 1961).

[41] Fed. R. Civ. P. 26(b)(3).

[42] *See* Sedona Report, *supra* note 22, at 8 ("The goal of [this] Commentary is to address the absence of 'settled law' on" the "application of the attorney-client privilege and work-product protection to documents and communications that an organization generates in the cybersecurity context.").

[43] Timothy P. Glynn, *Federalizing Privilege*, 52 AM. U. L. REV. 59, 60 (2002).

[44] *See infra* Part I.A.

[45] *See infra* Part I.C.

the law, or lack thereof, regarding when and if disclosures of a cybersecurity consultant's work product to third parties can jeopardize any confidentiality protections that would otherwise apply.

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

When businesses suspect that they may have experienced a cyber-incident, their first call is often to a lawyer.[46] 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.[47] 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.[48]

In reality, however, it is often unclear when or if advice received from cybersecurity experts in the aftermath of a breach will be protected by either attorney-client privilege or work product doctrines.[49] Fundamentally, this is because breach investigations inevitably implicate an interconnected web of legal and non-legal 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. Courts facing assertions of attorney-client privilege and/or work product immunity with respect to materials produced in post-breach investigations must consequently balance the primacy of the legal and non-legal goals that drove

---

[46] *See* Daniel W. Woods & Rainer Böhme, *Incident Response as a Lawyers' Service*, 20 IEEE SEC. & PRIV. 68 (2021); Daniel W. Woods & Rainer Böhme, *How Cyber Insurance Shapes Incident Response: A Mixed Methods Study,* THE 20TH ANN. WORKSHOP ON THE ECONS. OF INFO. SEC. (2021).

[47] *See* sources cited *supra* note 42.

[48] *See* sources cited *supra* note 42.

[49] Even when these protections attach, they are subject to various potential limitations and exceptions. For instance, attorney-client privilege universally does not extend to any facts that are contained within privileged communications. *See* Sedona Report, *supra* note 22, at 14. And work product immunity can be surmounted by plaintiffs who can show a substantial need for the covered information and that they 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* Capital One Consumer Data Security Breach Litigation, No. 1:19md2915, 2020 WL 2731238, n.2 (E.D. Va. May 26, 2020).

a particular investigation.[50] And they do so by considering a broad range of factors that vary across jurisdictions and courts.[51] Subsection one, below, 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 and/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 anticipated litigation (in the case of work product immunity) when it is hired by the breached firm's external counsel after a potential breach.[52] This can, and often does, take the form of a tripartite agreement among the breached firm, its external counsel,

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

[51] Glynn, *supra* note 43, 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) (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").

[52] *See, e.g.*, New Albertson's, Inc. v. MasterCard International, No. 01-17-04410, slip op. at 6 (Idaho 4th Dist. Ct., May 31, 2019); *In re* Experian Data Breach Litig., No. SACV1501592AGDFMX, 2017 WL 4325583 (C.D. Cal. May 18, 2017); *In re* Target Corp. Customer Data Sec. Breach Litig., 2015 WL 6777384 (D. Minn Oct. 23, 2015).

and the forensic firm.[53] By contrast, courts often are 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.[54]

Application of 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.[55] Other courts, however, interpret these circumstances to suggest that the forensic firm was, in practice, hired by the breached firm to provide non-legal services.[56] These courts have suggested that firms wishing to ensure that forensic investigators' post-breach communications are shielded from discovery should hire a different firm to conduct this investigation than the firm they used to conduct pre-breach surveillance.[57]

b. Did External Counsel Supervise the Cybersecurity Firm?

In addition to considering whether external counsel *hired* a cybersecurity firm in the aftermath of a breach, courts also assess the purpose of a cybersecurity firm's work under the attorney-client privilege and work product doctrines 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 where these terms specify that its work will be done solely at the

---

[53] *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 LAW (Sept. 2021), https://www.foley.com/en/insights/publications/2021/09/maintaining-privilege-over-forensic-reports.

[54] *See, e.g., In re Cap. One*, 2020 WL 3470261, at 1.

[55] *See, e.g.*, *New Albertson's*, No. 01-17-04410, at 6 (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); *Experian*, 2017 WL 4325583, at *1 ("Mandiant's previous work for Experian was separate from the work it did for Experian regarding this particular data breach.").

[56] *See Cap. One*, 2020 WL 3470261, at 1; Wengui v. Clark Hill, PLC, 338 F.R.D. 7 (D.D.C. 2021).

[57] The *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." *Cap. One*, 2020 WL 3470261, at n.5 (emphasis added).

direction of external counsel.[58]

Courts typically, however, also look beyond the formal governing agreement to assess whether external counsel in fact managed all elements of a forensic firm's work.[59] Courts are particularly wary of parties naming counsel as a forensic firm's supervisor to immunize communications from discovery, when the realities of the parties' arrangement suggest that the breached firm is actually directing the forensic firm's work. 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.[60]

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 that the forensic firm has agreed to provide in its contract. In doing so, courts evaluate whether these services are associated with fundamentally business functions on the one hand, or with services that facilitate 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.[61] Services falling into the former category because they are business related include discovering how the breach occurred, remediating the consequences of breach, formulating public statements, and making recommendations to ensure a breach cannot happen again.[62] By contrast, services falling in the latter category include helping lawyers to respond to regulatory authorities, preparing for anticipated litigation, or understanding

[58] *See In re* Premera, 296 F.Supp.3d 1230, at 1244–46 (D. Or. 2017) (suggesting that a Statement of Work listing external counsel as the forensic firm's supervisor was relevant to the privilege analysis).

[59] *See Cap. One*, 2020 WL 2731238, at 4 ("The only significant evidence that Capital One has presented concerning the work Mandiant performed is that the work was at the direction of outside counsel….").

[60] *See, e.g.*, *Dominion*, 429 F.Supp.3d at 194 ("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.'"). *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).

[61] Sedona Report, *supra* note 22.

[62] *See Premera*, 329 F.R.D. at 666-67; *Wengui*, 338 F.R.D. at 11.

the scope of the breached firms' duties under state breach notification laws.[63] Meanwhile, some services, such as notifying customers regarding the scope of a breach, may frequently blend legal and non-legal 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 fundamentally altered the security firm's responsibilities.[64] If not, courts often conclude that the cybersecurity firm's work remains business related, and hence is discoverable.[65] 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 this work was really driven by legal or litigation-oriented purposes.[66]

Courts vary in the extent to which they look beyond formal contract language to assess whether that language accurately reflects the work that a forensic 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, even though there was evidence that this risk played a significant role in the firm being retained.[67] 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.[68] And in many cases, courts take seriously arguments that a

---

[63] *See 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).

[64] *See Cap. One*, 2020 WL 3470261, at 1; *Wengui*, 338 F.R.D. at 7.

[65] *See, e.g.*, *Dominion*, 429 F.Supp.3d at 194 (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'"); *Cap. One*, 2020 WL 2731238, at 1 (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").

[66] *See, e.g.*, *Dominion*, 429 F.Supp.3d at 193.

[67] *See In re* Rutter's Data Sec. Breach Litig., No. 1:20-CV-382, 2021 WL 3733137 (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).

[68] *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 Cap. One*, 2020 WL 3470261, at *4 (dismissing the relevance of a provision in the Statement of Work providing that "the work was done under the outside counsel's supervision").

contract purporting to hire a forensic firm to provide legal, rather than business, services, is a "sham," even if they do not always find such arguments convincing.[69]

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 forensic firm's services and how those payments were internally recorded. Recent cases have implied, without explicitly holding, that a breached firm's direct payment to a forensic investigator may indicate that its services were driven by business, rather than legal, considerations.[70] Similarly, the *Capital One* court highlighted that Capital One initially paid its forensic firm out of its "business critical" expense and cyber organization budgets, but subsequently paid it from its legal department budget after it was breached.[71]

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.[72] Other cases suggest that a cybersecurity firm that works closely with the breached firm's IT personnel in the aftermath of a breach is more likely to be deemed to be providing business, rather than legal or litigation-perpetration, services.[73]

---

[69] *See In re Marriott*, 2021 WL 2660180, at 1 (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).

[70] *See In re* Rutter's Data Sec. Breach Litig., No. 1:20-CV-382, 2021 WL 3733137, 1 (M.D. Pa. July 22, 2021) (noting that "[d]efendant paid [the firm] directly," but not clarifying the relevance of this fact, if any, to its analysis).

[71] *See Cap. One*, 2020 WL 3470261, at 1.

[72] *See Wengui*, 338 F.R.D. at 12-13.

[73] *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).

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.[74] With respect to attorney-client privilege, this trend reflects the broader principle that facts cannot be privileged.[75] 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.[76]

Courts are also reluctant to shield from discovery reports 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.'"[77] Other courts, however, do treat reports containing recommendations as privileged, though they are not often transparent about their reasoning for doing so.[78]

g. Disclosure of Materials Produced by Cybersecurity Firms

In addition to the substance of a forensic report, courts also consider the extent of that report's dissemination when making privilege and immunity determinations. The more individuals with access to a forensic report, the more likely courts will find the report serves a business, rather than a legal, purpose.[79] This logic played a key role in the *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."[80] This was especially true because Capital One could

[74] *Dominion*, 429 F.Supp.3d at n.4 ("[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.").

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

[76] *Cap. One*, 2020 WL 2731238, at *4 (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").

[77] *Wengui*, 338 F.R.D. at 13-14.

[78] *See In re Marriott*, 2021 WL 2660180, at *6 (acknowledging that the report included recommendations for the business's security systems, but nonetheless treating the report as privileged).

[79] *See, e.g.*, *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).

[80] *Cap. One*, 2020 WL 3470261, at 6.

provide no legal justification for the report's dissemination to its technical employees.[81]

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 they are transmitted directly to external counsel, even if external counsel then shares the report with the client. By contrast, some courts have expressed skepticism regarding the legal purpose of forensic firm's services when it shares its final report directly with the breached business's personnel.[82] This may be less true, however, if the report that is shared with the breached firm's personnel includes redacted materials that are relevant to legal strategy.[83]

h. Public Announcements 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 the *Dominion Dental* case, where the court latched on to the company's incident response talking points, 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.[84]

2. Balancing Competing Factors

In addition to evaluating the multitude of factors regarding whether a forensic 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

[81] *Id.* at 2.

[82] *Rutter's*, 2021 WL 3733137, at 3 (concluding that cybersecurity firm's direct disclosure of report to Rutter's demonstrated that the report lacked a primary legal purpose).

[83] *In re* Experian Data Breach Litig., No. SACV1501592AGDFMX, 2017 WL 4325583, 2 (C.D. Cal. May 18, 2017) (granting work product immunity when a redacted version of the report was provided to the business's internal incident response team).

[84] *See Dominion*, 429 F.Supp.3d at 192. The court in *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 Cap. One*, 2020 WL 3470261, at n.5. However, the *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.

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 the attorney-client privilege, on the one hand, and work product immunity, on the other.

With respect to the attorney-client privilege, many courts have suggested that the relevant factors must tilt almost entirely towards the provision of legal advice rather than business services in order 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 to be privileged.[85] Others go further, specifying that even limited evidence that a document was prepared by a cybersecurity firm "for a purpose other than *or in addition to* obtaining legal advice," will negate privilege.[86] However, the extent to which courts broadly embrace these formulations is varied, as the scope of the privilege varies significantly across different states and federal circuits.[87] 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.[88]

By contrast, most courts suggest that the balance between litigation-oriented and business purposes underlying breach investigations need only tilt moderately towards 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 rules on the federal rules.[89] 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

---

[85] *In re* County of Erie, 473 F.3d 413, 419-20 (2d Cir. 2007).

[86] *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 329 F.R.D. 656, 661 (D. Or. 2019); *cf. In re Marriott*, 2021 WL 2660180, at 6 (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").

[87] Glynn, *supra* note 43, at 60. To illustrate, the Sedona Report explains that one state, California, has a more liberal approach to the attorney-client privilege when communications have a mixed legal and non-legal purpose. *See* Sedona Report, *supra* note 22, at 17 (citing Costco Wholesale Corp. v. Super. Ct., 219 P.3d 736, 746 (Cal. 2009) (stating that a court must isolate "the dominant purpose of the relationship" to determine whether the associated communications are privileged)).

[88] *See* Sedona Report, *supra* note 22, at 110.

[89] *Cf.* Zachary D. Clopton, *Making State Civil Procedure*, 104 CORNELL L. REV. 1, 5 (2018) ("[S]tate rulemakers do more than simply mirror the federal rules.").

a primary or secondary motive behind the creation of a document,"[90] whereas courts in other federal circuits do indeed ask whether "the driving force behind the preparation of" a document was actual or anticipated litigation.[91] 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."[92] These courts often also require that a firm's "unilateral belief" that litigation might transpire be "objectively reasonable" for work product immunity to attach.[93]

***

In sum, the law governing when lawyers can successfully shield the breach-response efforts of forensic firms is complex, unpredictable, and variable. Indeed, *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. Pre-Incident Cybersecurity Efforts, Attorney-Client Privilege, and Work Product Immunity

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, 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.[94]

Unlike in the post-breach context, the law is relatively clear that

---

[90] *Experian*, 2017 WL 4325583, at 1 (quoting *In re* Grand Jury Subpoena (Mark Torf/Torf Envtl. Mgmt.), 357 F.3d 900, 907 (9th Cir. 2004)).

[91] *Cap. One*, 2020 WL 3470261, 3 (quoting Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co., 967 F.2d 980, 984 (4th Cir. 1992)); *Rutter's*, 2021 WL 3733137, at 2.

[92] *Experian*, 2017 WL 4325583, at 1; *Cap. One*, 2020 WL 3470261, at 3; *Rutter's*, 2021 WL 3733137, at 2.

[93] *Rutter's*, 2021 WL 3733137, at 2.

[94] *See* Sedona Report, *supra* note 22, at 28-33 (cataloging different types of pre-breach information that lawyers may be involved in developing).

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.[95] Attorney-client privilege will also infrequently apply to the pre-breach efforts of cybersecurity professionals, even when those efforts involve lawyers.[96] Recall that communications involving third-party experts like cybersecurity firms are only privileged if they principally operate to facilitate legal advice. 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.[97]

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 its role would not be to *support* the lawyer's work, but to provide non-legal services that are legally required. Yet the mere fact that non-legal services are legally required does not mean that they are privileged, even if a lawyer coordinates their delivery.[98]

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, and post-incident recovery."[99] 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.[100]

---

[95] 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) ("[A]ttorney work product doctrine . . . [requires] that litigation was fairly foreseeable at the time the materials were prepared.").

[96] Of course, privilege will be unavailable when a cybersecurity firm's work does not involve lawyers. *See* Sedona Report, *supra* note 22, at 34.

[97] *Id.* at 35-36.

[98] 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 id.* at 36.

[99] *CISA Tabletop Exercises Packages*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cisa-tabletop-exercises-packages (last visited July 24, 2022).

[100] *See* Sedona Report, *supra* note 22, at 37-38; Genesco Inc. v. Visa, Inc., No. 3:13-CV-00202, 2015 WL 13376284, at *1 (M.D. Tenn. Mar. 25, 2015) (holding that pre-breach communications between a technical consultant and counsel were privileged because the

Consistent with this analysis, relevant cases have largely rejected 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 2015 breach, it tried to shield its 2013 and 2014 technology audits from discovery on the grounds that they were privileged.[101] 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."[102] The mere fact that Premera delegated supervision of these business operations to counsel did not, the court emphasized, cloak them with confidentiality.[103]

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. With respect to the attorney-client privilege, disclosure of privileged information to any third party can constitute waiver of privilege.[104] 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 not need to know the information for purposes of managing the firm's legal affairs.[105] By contrast, disclosure of materials protected by work product may not result in waiver unless those disclosures are made to adverse parties.[106] With respect to both attorney-client privilege and work product doctrines, courts differ as to whether disclosure to law enforcement or regulatory authorities of otherwise confidential information results in waiver of those protections as to private litigants.[107]

---

consultant was hired solely to aid the lawyer's analysis of Arby's compliance with the PCI DSS).

[101] *See Premera*, 329 F.R.D. at 666-67.

[102] *Id.* at 665.

[103] *Id.* at 667. The ruling did acknowledge if "an attorney took the information from these documents and drafted a different document in preparation for litigation, that document would be protected." It also noted that a "draft report sent to counsel seeking legal advice and input on the draft also would be privileged." *Id.*

[104] *See, e.g.*, United States v. Deloitte LLP, 610 F.3d 129, 140 (D.C. Cir. 2010). *See generally* Principles of the Law, Compliance and Enforcement for Organizations § 6.06 TD No 2, cmt. c (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.").

[105] *See* Sedona Report, *supra* note 22, at 22-23 (citing Verschoth v. Time Warner, Inc., No. 00CIV1339AGSJCF, 2001 WL 286763 at *3 (S.D.N.Y. Mar. 22, 2001)).

[106] *See Deloitte*, 610 F.3d at 140.

[107] *See* Sedona Report, *supra* note 22, 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.,

These general rules, however, are subject to a host of important exceptions. For instance, the Cybersecurity Information Sharing Act (CISA) of 2015 provides that disclosing information to certain Information Sharing and Analysis Organizations (ISAOs) does not result in waiver of otherwise applicable attorney-client privilege or work product protections.[108] Similarly, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022 requires "critical infrastructure companies" 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.[109] 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.[110]

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,[111] 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.[112] In both settings, insurers not only fund the underlying legal activities about which disclosure is made, but also oversee the lawyers that coordinate these legal processes for the insured.[113]

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.[114] And there are several potential distinctions between the cyber-insurance 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

9 F.3d 230, 236 (2d Cir. 1993).

[108] Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

[109] The Cyber Incident Reporting for Critical Infrastructure Act of 2022.

[110] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 76(a).

[111] *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).

[112] RESTATEMENT OF THE LAW OF LIABILITY INSURANCE § 11; 1-10 Professional Responsibilities of Ins. Def. Counsel § 10.06 (2017).

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

[114] 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.

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.[115] 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.[116]

II. 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.[117] 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 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-

---

[115] *See* Romanosky et al, *supra* note 111, at 5-6.

[116] Of course, divergent interests among liability insurers, policyholders, and insurance defense counsel are hardly uncommon. *See* 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).

[117] *See* Sedona Report, *supra* note 22, at 79-93; Kosseff, *supra* note 7, at 261-62.

party forensic 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.[118] Because no prior work had investigated this issue empirically, we conducted in-depth, semi-structured interviews of a broad range of actors across the cybersecurity ecosystem.[119] Such qualitative techniques are particularly appropriate when it comes to understanding complex interactions between legal rules and practice that have not previously been empirically studied.[120] 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 offers multiple potential avenues for future quantitative inquiry.[121]

We conducted sixty-nine semi-structured interviews lasting between thirty and sixty minutes each from 2020 to 2022.[122] We recruited participants for the interviews 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.[123] Additionally, we contacted representatives from law firms, insurers, and forensic investigations firms known for their expertise in cybersecurity incident response, as well as other

---

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

[119] 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, 1541 (2017); Tom Baker & Sean J. Griffith, *Predicting Corporate Governance Risk: Evidence from the Directors' & Officers' Liability Insurance Market*, 74 U. CHI. L. REV. 487 (2007); Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J LEGAL STUD. 115 (1992).

[120] *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.").

[121] *See* Baker & Griffith, *supra* note 119, at 492.

[122] 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.

[123] Woods & Böhme, *supra* note 46.

professionals recommended to us by our interview subjects.[124] We ultimately 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 IT forensic firms with similar cyberinsurance relationships. In addition, we interviewed lawyers from many of the leading "Big Law" firms that have substantial practice areas in cybersecurity. We are thus confident that our study covered a significant portion of the incident response ecosystem.

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. 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 interviewee responses to these questions.

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 resulted in positive feedback, while also producing several small 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. These data are reported in an Appendix. Doing so allowed us to confirm our broad impressions regarding the results as well as to 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

[124] We identified law firms that focused on providing cybersecurity services but that were not on insurance panels by consulting public lists of top firms specializing in such areas. *See, e.g.*, Cyber Law Recommendations, Legal 500 https://www.legal500.com/c/united-states/media-technology-and-telecoms/cyber-law-including-data-privacy-and-data-protection/ (last visited July 24, 2022). 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.

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-one lawyers we interviewed said they did not always encourage forensic firms to produce a final, written report detailing the findings of their breach investigations. And about half of the lawyers we interviewed indicated that their standard practice was to direct the forensic firm not to author such a report. Lawyers that centered their practice on breach-response and received a significant amount of their work from insurers were particularly likely to insist that forensic firms should typically not produce any final written report.[125]

The forensic investigators we interviewed also identified that their production of final reports had become less common in recent years.[126]

[125] 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. The basic division was between smaller firms that 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, versus larger firms that practiced in a number of different areas, typically charged rates too high to be listed on insurance panels, and investigated a smaller number of breaches for clients with whom they already had long-standing relationships.

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 $1500 hourly rates. 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 was designed to maximize protections of privilege, such as by always hiring a new forensic firm with whom the law firm had a good relationship, and often involved minimal documentation.

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. "There's no specialized attention, it's routine and formulaic," one lawyer said of how breach-focused firms approach incident response, adding, "those firms are too mechanical and that's ok if it's not overly complex." 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.

[126] 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

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."

Lawyers generally explained their reluctance to direct forensic 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 *Capital One* and *Rutter's* cases.[127] Although many of the lawyers opined that these cases were wrongly decided, they also indicated that these cases injected substantial uncertainty into predicting when courts would treat forensic reports as privileged or otherwise non-discoverable.

Even in instances when lawyers instructed a forensic 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 forensic firms, with lawyers instructing forensic firms to redraft language that they believed could be taken out of context to support liability.[128] A repeated concern from lawyers was that the report only contain factual information.[129] 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.[130]

---

used to be. Only the most sophisticated clients are asking for reports these days and only for the most complicated incidents."

[127] See *supra* Part I.A(discussing *Capital One* and *Rutter's*). One attorney interviewed 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.'" Another said of the *Capital One* ruling: "[the courts] have jumped the fence [in the Capital One case] and are no longer respect privilege on the report, therefore we're not creating the report." A third lawyer echoed this sentiment, saying "since 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." A fourth attorney said, "I've started to advise against written report. It was not our practice before [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."

[128] 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." Another said, "we try to give guidelines like: no adjectives, no adverbs."

[129] One lawyer noted, "I prefer not to have editorializing … about all things that could have gone better." Another attorney said he tries to avoid "gratuitous language like 'these are the best practices in information security.'"

[130] A former investigator 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

Some lawyers identified various situations in which they might ask a forensic firm to produce a final report notwithstanding their general inclination to avoid this result. For instance, an investigation describing a "clean bill of health" 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.[131] Additionally, some lawyers explained that they might ask for a final report for clients subject to expansive regulatory scrutiny as a way of satisfying those regulators by showing that the firm had acted appropriately in response to a breach.[132] Such nuance was more common among lawyers who worked for more high-profile law firms that were not included on insurance panels.[133]

Other lawyers explained that they would occasionally instruct forensic 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.[134] Another approach is for external counsel to receive a final report, and then to 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.[135]

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

---

me to say that a specific server was vulnerable." What some law firms viewed as "editorializing," in other words, seemed to forensic investigators to be plain statements of the facts around vulnerabilities in a system.

[131] According to one lawyer, "there are times when the findings are just so bad that you don't want to reduce that to writing." 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."

[132] One lawyer interviewed said "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."

[133] *See supra* note 125.

[134] One lawyer said there were three categories of report formats: "(1) only oral, (2) stripped-down Powerpoint, and (3) full reports."

[135] One lawyer who took this further justified summarizing forensic reports in their own memos by claiming that doing this was necessary to make otherwise "incomprehensible" forensic reports understandable.

recommended control.[136] Additionally, lawyers expressed 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.[137]

Stakeholders expressed a broad variety of views on the impacts of instructing a forensic 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 re-constructing the incident for purposes of assessing the long-term effectiveness of cybersecurity processes, facilitating a regulatory inquiry, or simply reconstructing the incident for internal purposes after time had passed.

The forensic experts we interviewed were particularly concerned about the cybersecurity consequences of foregoing a final report. First, a number of forensic experts suggested that the lack of a final report could have immediate negative consequences on the effectiveness of incident response efforts.[138] Some of these consequences involved the ability of a forensic 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.

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.[139] Forensic investigators said

---

[136] 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." Another lawyer explained, "when I become concerned is when the forensics team is producing a paper trail. Because then plaintiff 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."

[137] *See supra* Part I.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." Another echoed these concerns, saying, "for some firms, the recommendations are boilerplate long list that may not make sense in a particular context."

[138] One investigator noted, "there's a lot of information you can convey verbally but when you have larger companies with bigger teams when you have that report and it's disseminated out to those teams it gives them such a better understanding of the weaknesses in their systems."

[139] One forensic investigator explained: "Those opinions [*Rutter's* and *Capital One*] are

it was often difficult to explain recommendations verbally, given how complicated and nuanced they might be and the likelihood of employee turnover.[140] 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.[141]

Second, most of the forensic investigators we interviewed opined that 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 towards meeting those recommendations. Investigators also said they believed that the lack of documentation means that 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.[142] Such advocacy is much more difficult when recommendations are not included in a final report or even formalized in writing.[143] 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 most essential they improve their security.

Lawyers expressed more limited concerns about the cybersecurity consequences to their clients of foregoing a final report. Most notably, many lawyers argued that communicating forensic firms' security

---

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."

[140] 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."

[141] One attorney said he asked for written reports "not always, but more often than not." The attorney explained, "some 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 IOCs [Indicators of Compromise}."

[142] 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 … by the time it makes it to customers, it's probably not doing any good at that point."

[143] 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. 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.

recommendations orally, rather than in writing, was sufficient to ensure that clients received appropriate guidance. However, several lawyers indicated that they did not believe oral briefings of security recommendations were sufficient.[144] 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. 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."

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, pen testing, and tabletop exercises. Consistent with the caselaw discussed in Part I, most lawyers said documentation resulting from such activities was difficult to shield from discovery in subsequent lawsuits.[145] Even the lawyers who indicated that they do try to protect privilege for pre-breach materials also said that they were uncertain of their ability to do so.[146]

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.[147] These lawyers said they explicitly tried to prevent risk assessment reports that showed significant or glaring vulnerabilities (e.g., color-coded with red labels or dramatic "high-risk" warnings).[148] They noted that such

[144] 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."

[145] *See supra* Part I.B (concluding that courts will rarely treat pre-breach cybersecurity efforts as privileged or covered by work product immunity).

[146] One attorney said, "We try [to protect confidentiality of pre-breach materials] but we also are candid that our ability to privilege this is unclear." 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."

[147] 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]." Another said that security assessments were often "toned down" and particularly negative reports were never passed on to the client.

[148] One lawyer said of pre-breach assessments: "They're like RED RED RED RED. You

assessments were often exaggerated in their severity and could be used against firms in the event of a later security incident that led to litigation. 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. 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." 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 generally 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 when they occurred dramatically outweighed the potential costs that documents produced during this process could be used against firms in subsequent litigation, in their view.[149] Some attorneys, however, expressed concerns that the lack of privilege might deter some clients from engaging in robust pre-breach security screening.[150] These concerns provide some support to the concern, expressed by others, that the privilege framework creates a "perverse incentive system" whereby "assisting attorneys in litigation receives more protection from discovery than developing technical

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.' "

[149] 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." On the importance of proactive rather than reactive cybersecurity efforts, see CYBERRISK ALLIANCE, CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX, 1 (2020), https://www.cyberriskalliance.com/wp-content/uploads/2020/08/CRAE-Index.pdf (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 (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).

[150] The absence of privilege "is a disincentive and also a concern for candor," one lawyer said, adding, "you 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."

remediation measures that are separate from legal strategies."[151]

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 used to hire and direct cybersecurity firms, and in the protocols that control communications among personnel at the cybersecurity firm, breached firm, and their lawyers.

1. Hiring Forensic Firms to Conduct Cyber-Incident Response

Almost every lawyer we interviewed routinely advised their clients to contract with a forensic firm in the aftermath of a breach through a tripartite agreement that included the external law firm as a contracting party. Doing so, lawyers noted, was crucial to establishing that the breach investigation was being done for the purpose of facilitating legal advice or in anticipation of litigation, such that attorney-client privilege or work product protections would potentially attach.[152] One attorney said the *Capital One* ruling had changed their practice so that in some cases, now, the law firm is the sole party to retain the forensic firm, rather than having a tripartite agreement. Additionally, that lawyer now recommends that payments to the forensic firm come from the client's legal, rather than IT, budget.[153]

Lawyers also typically played a significant role in selecting the forensic investigation firm. This was particularly common for law firms that specialized in breach-response services and relied on cyberinsurers for their business.[154] 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. They added that "privilege is one of the main ways that was sold." Another forensic investigator indicated that their firm now routinely directs breach victims that contact them to go through a lawyer rather than to work

---

[151] Kosseff, *supra* note 7, at 284.

[152] *See supra* Part I.A1.a. (suggesting that courts strongly weigh which party hired a forensic firm in their work product and privilege analysis).

[153] *See supra* Part I.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).

[154] *See supra* note 125.

with the forensic firm directly.

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 *Capital One* for this proposition.[155] 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. A number of lawyers also indicated that hiring a new forensic firm was preferable because it eliminated the risk that the firm would downplay its own failures in investigating the root cause of a breach.[156] These views were particularly common among lawyers who worked at firms that specialized in breach response.[157]

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 forensics investigator. 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, according to another forensics expert. 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.[158]

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,

---

[155] *See supra* Part I.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 Statement of Work is created in connection with the breach). One lawyer explained, "If you really wanted to preserve privilege, then the investigation firm would be separate from the firm who conduct IR or pre-breach activities."

[156] One lawyer said, "it's almost like an inherent conflict of interest to have the firm that did the security work investigate their own failure." Another lawyer added, "We work with companies that are doing incident response 24/7. They've got a very good formula for going through it, they don't turn over every single rock."

[157] *See supra* note 125.

[158] 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.

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.[159] In rare cases, the lawyer would pay the preexisting forensics vendor directly, and then bill the client for these expenses.[160]

In addition to selecting forensic firms and formally contracting with them, lawyers also typically defined the scope of the forensic firm's role in breach response. Several lawyers indicated that after *Capital One* they more carefully specified in the tripartite agreement the precise services that the forensic firm would provide to support the lawyer's work.[161] Forensic investigators indicated that they were wary of suggesting additional tests or investigations to clients beyond those that the lawyers who hired them requested.[162] These dynamics were particularly stark with respect to the specialized breach-focused law firms listed on insurance panels.[163] 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.[164] As a result, as one prominent lawyer at a firm focused on

[159] 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 Statement of Work (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* Part I.A.2. (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).

[160] 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., 2015 WL 6777384 (D. MN. 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 due to the fact that two different parties are potentially impacted by a breach and have an interest in understanding their exposure. 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* Part II.D.

[161] *See supra* Part I.A.1.f. (indicating the relevance of the services provided and content of Statement of Work to privilege and work product protections).

[162] 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. Another investigator said, "we say that the counsel is our client and the counsel has their client, which we call client's client."

[163] *See supra* note 125.

[164] One forensic investigator explained: "you are … working for the lawyers as much if

breach response noted "when we say jump, they [the forensic firms] say 'how high?'" Several forensic investigators also expressed concern that lawyers' primacy in defining the scope of their services could undermine cybersecurity.[165]

2. Communications During Cyber-Incident Response

Lawyers' importance in breach response extended well beyond the contracting process; lawyers also routinely coordinated communication flows among forensic firms and clients throughout the breach response process. Often they did so by establishing detailed communication protocols that they distributed at the outset of an incident response. Lawyers 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 external counsel.[166] Generally, though, most lawyers made some concessions when it came to vendors requesting access to the client's systems for investigative purposes or for other purely technical or coordination matters.[167] 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.[168] 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.[169] Forensic investigators

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." Another investigator said: "The more you upset [the law firms] the more devastating impact it will have on your business."

[165] One investigator said: "if we're hired by a law firm, then we're going to do the project according to their Statement of Work and scope of work. If it appears the scope is expanding, then we'll bring it to law firm, but we let them decide if the scope should expand."

[166] 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."

[167] 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."

[168] 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, we'll never get done with anything." Another said that micromanaging communications could slow down the investigation and have adverse consequences for the remediation process.

[169] 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."

also said they had learned to be careful about what kinds of findings they put in writing.[170]

Lawyers explained their efforts to control communication flows during the incident response in 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, was directing the efforts of the cybersecurity firm.[171] 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 incident often are not ultimately supported by the evidence as a whole.[172] 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.[173]

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.[174] Doing so, these lawyers explained, helped substantiate later assertions of privilege or work product immunity by helping to frame forensic firms' efforts as facilitating the provision of legal services rather than providing business

---

[170] One investigator said: "you 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 multi-factor 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."

[171] *See supra* Part I.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).

[172] For example, one lawyer reported how the IT director's machine had been compromised and the CEO immediately concluded that was the attack vector. Further investigation using timestamps revealed that the incident pre-dated the IT director's machine being compromised.

[173] One lawyer shared an anecdote in which a preliminary report stated the victim firm had "a pervasive culture of non-compliance," others stated that technical investigators were prone to "editorialize" and go beyond the bare facts. Limiting documentation preemptively addressed this problem.

[174] 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. 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.

services to the impacted firm.[175]

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.[176]

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 remediate their security postures. Various third-party stakeholders may also be interested in the results of an investigation, including insurers, auditors, supply chain partners, customers, law enforcement agencies, and regulators. Stakeholders from these third parties emphasized to us the importance of acquiring detailed information from compromised firms so that they could better understand the constantly evolving threat landscape. Yet virtually all 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 for fear that it could constitute a waiver of privilege or work product immunity.[177] 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.

1. Insurers

Insurers providing coverage for cybersecurity incidents have numerous potential reasons for requesting a forensic firm's investigative findings. Although some of these have only a tangential relationship to

---

[175] *See supra* Part I.A.1.g.(noting that courts evaluating privilege and work product immunity claims often consider the extent to which a forensic firms' conclusions were widely disseminated at the impacted firm).

[176] One investigator noted that attorney-client privilege "slows communications at every level" during an investigation. Another echoed that sentiment, explaining "if 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." That investigator added that these delays can be critical because "all 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."

[177] *See* 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.").

cybersecurity,[178] others have potentially significant cybersecurity implications. Most importantly, access to forensic firms' breach reports or related materials could help cyberinsurers to limit the risk of breach through improved underwriting, targeted discounts, and various other insurer loss prevention strategies.[179] Indeed, the prospect of such insurer-driven enhancements to cybersecurity has been much touted by the insurance industry and commentators,[180] even though evidence of this effect is quite limited.[181] Access to post-breach forensic materials could also help cyberinsurers to 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.[182]

In reality, insurers virtually never receive any written materials from the forensic firms that investigate covered breaches. Both lawyers and insurers

---

[178] 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 113, at 11-36. Information from forensic firms could also potentially be useful in administering claims.

[179] *See* ERIN KENNEALLY, HIDING IN PLAIN SIGHT: TOWARDS NOW-GEN CYBER RISK UNDERWRITING, GUIDEWIRE WHITE PAPER 2 (2021), at https://www.the-digital-insurer.com/wp-content/uploads/securepdfs/2021/09/1834-GuidewireCyenceRiskHidingInPlainSight.pdf (arguing that post-incident digitial forensic reports offer important data for improving cyberinsurance underwriting that cyberinsurers have ignored). *See generally* Abraham & Schwarcz, *supra* note 24, at 20-35 (cataloguing potential 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).

[180] *See, e.g.*, Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191 (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. INQ. 417 (2018); Kyle Logue & Adam Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, 28 CONN. INS. L. J 247 (2021); Baker & Shortland, *supra* note 13; Jan Martin Lemnitzer, *Why Cybersecurity Insurance Should be Regulated and Compulsory*, 6 J. CYBER POL'Y 118 (2021).

[181] JOSEPHINE WOLFF, CYBERINSURANCE POLICY: RETHINKING RISK IN AN AGE OF RANSOMWARE, COMPUTER FRAUD, DATA BREACHES, AND CYBERATTACKS (forthcoming 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); JAMIE MACCOLL, JASON R. C. NURSE & JAMES SULLIVAN, CYBER INSURANCE AND THE CYBER SECURITY CHALLENGE vii (2021), https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge.

[182] *See* Abraham & Schwarcz, *supra* note 24, at 20-35 (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).

said in interviews that lawyers routinely limit the information from forensic firms regarding a cyber-incident that is shared with insurers. 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. 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.[183]

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 waiver of privilege under the common interest doctrine,[184] 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 well depend on which jurisdiction adjudicated the matter.[185] Some lawyers also suggested that they resisted providing documents regarding a cybersecurity intrusion because an insurer could use these materials to deny coverage.[186]

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.[187] 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 resistant to demanding information produced by forensic firms because they could lose business as a result.

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

---

[183] One insurance broker said that insurers often received information from lawyers via PowerPoint slides that the lawyers were unwilling to provide a copy of to the insurers, or even allow them to take photos of screenshots while they were being shared.

[184] *See supra* Part I.C (suggesting that disclosure to a cyberinsurer of a forensic firm's breach report would likely not constitute waiver, but that the law on this point remains unclear).

[185] *See supra* Part I.C.

[186] 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, PROFESSIONAL RESPONSIBILITIES OF INSURANCE DEFENSE COUNSEL § 4.04 (2015).

[187] *See* Romanosky et al., *supra* note 111.

efforts. In many cases, the information that is conveyed on these calls is inaccurate, in part because it is not being communicated directly by the forensic firm that did the underlying work and has the necessary technical expertise, insurers said.[188] 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.

While most respondents believed insurers could learn from detailed written information produced by forensic firms, very few had experience of them doing so. Insurance personnel we interviewed often expressed interest in being able to access forensic reports and learn from them.[189] This was particularly true for interviewees that working in underwriting; by contrast, insurance employees who worked on claims indicated less of an interest in acquiring these materials.[190] 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.[191] "In most cases [insurers] don't know how to read a forensics report and how to react to it," one insurer explained. "Insurers aren't clamoring for it because they don't know what to do with it." 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."[192] One lawyer expressed a similar sentiment, noting that the risk models used by insurers were improving and that studying forensics reports was a part of this process.

Given the potential value to insurers of forensic reports and the legal

---

[188] One insurer said, "there 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."

[189] *See* KENNEALLY, *supra* note 179, 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.").

[190] 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 178-182 (describing these potential uses of information from forensic firms).

[191] As one insurer put it, "every carrier is dying for data, they just don't know what data they need."

[192] 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.

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.[193] And one insurance underwriter shared with us that an insurer had drafted new language for its insurance policy that required insureds to provide the insurer with all reports produced by vendors. 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. Several interviewees also said that the current hard market for cyberinsurance is changing insurers' calculations on these issues,[194] especially since insureds who resist sharing information from forensic firms may be relatively risky.[195] Yet another underwriter noted that one insurer is even considering cutting out lawyers from the initial breach-response process altogether in order to reduce costs; doing so, of course, would completely eliminate any claim of privilege and hence that barrier to sharing information.[196]

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 claims denial. However, these efforts, the underwriter suggested, often failed to result in clients or the lawyers being forthcoming, even though this can (and often did) result in the insurer non-renewing the policy.

Several stakeholders noted that lawyers often faced significant conflicts of interest in navigating these insurance-related issues. Lawyers who do not depend on insurers to refer cases to them had some freedom to push back against insurers' requests for information from forensic firms.[197] Other lawyers who derive a substantial amount of their work from insurers often felt less freedom to push back against insurer demands for information or

---

[193] For instance, we heard one anecdote in which a foreign insurer refused to pay a claim unless the forensics report was shared. Under this threat, the lawyer and client shared the forensic report. Another lawyer reported that insurers requested the report for claims in the millions of dollars but not for smaller claims.

[194] *See* Tom Johansmeyer, *The Cyber Insurance Market Needs More Money*, HARV. BUS. REV. (March 10, 2022).

[195] 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?"

[196] *See supra* Part I.A.

[197] *See supra* note 125.

resistance to paying for certain services.[198]

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.[199]

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 client must deal with them in other contexts and so the risk of waiving privilege was outweighed by the harms from damaging that relationship. Similarly, another lawyer indicated that sharing information with regulators of firms in the healthcare industry, where privacy is heavily regulated, was particularly important.[200] In contrast, many lawyers stated it was not worth complying with the Federal Trade Commission (FTC) requests because that agency is either under-staffed and not able to prosecute, or they decide to prosecute and hammer firms regardless of their level of cooperation.[201]

Consistent with these regulator-specific approaches taken by lawyers, the government regulators we interviewed expressed varying levels of confidence in their ability to obtain information about cybersecurity incidents from breached firms. One said they were usually able to 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 in order to answer questions about the specifics of the breach. 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.[202] Another

[198] *See supra* note 121.

[199] Another lawyer, who said he was unique among the partners of his own firm even, instead prioritized communicating with regulators. 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, and the benefits from doing so outweighed the risk in terms of waiving privilege. However, he said this advice was specific to regulated industries.

[200] *See* 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 (2015).

[201] Various academics have also criticized the FTC's approach to cybersecurity on similar grounds. *See, e.g.*, Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955 (2016); Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008).

[202] This regulator explained, "the executive summary is fine for our purposes. We sort

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.[203] By contrast, a prominent state insurance regulator reported that they were typically able to compel firms to share documentation, including any reports that were produced, because they could credibly threaten to revoke an insurer's license to do business or otherwise impose significant consequences if it refused to comply.

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 oral updates. 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. 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 as compared with the other third-party stakeholders identified in this section, emphasizing the potential that doing so could result in waiver.[204] 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.[205]

Different results obtained for breaches involving credit card data, where

---

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."

[203] The regulator 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.

[204] *See* Ricardo Colón, *Caution: Disclosures of Attorney Work Product to Independent Auditors May Waive the Privilege*, 52 LOY. L. REV. 115, 116 (2006); R. Alexander Swider, *Toeing the Line: The Delicate Balance Attorneys Must Maintain When Responding to Auditor Inquiry Request Letters*, 50 IND. L. REV. 969, 983-88 (2017) (reviewing caselaw showing that courts are split on whether disclosure to auditors of documents result in waiver of attorney-client or work product protections).

[205] For instance, one lawyer described how he would ask the auditors "what do you want to know?", he then received a question about whether the system containing financial records was compromised, and he said no without providing further evidence.

firms were contractually required to permit an investigation resembling an audit. The Payment Card Industry (PCI) data security standard requires an investigation conducted by a PCI certified vendor, which must then be shared with the payment cards council.[206] Interestingly, this consideration was the motivation for the dual-track investigation structure that was infamously used by Target following its 2013 breach.[207] In particular, the defense accepted that the PCI investigation was discoverable by plaintiffs, but successfully argued a second independent investigation conducted under the supervision of counsel was protected by privilege.[208] However, no participants endorsed dual-track investigations as a strategy to improve confidentiality protections.

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 that firm's clients and customers.[209] For this reason, firms' commercial partners sometimes request information about a breach. 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 what is known about the incident at that point in time, acknowledging that the investigation is ongoing. To the extent that such updates were documented rather than provided orally, respondents acknowledged that those documents would not be privileged. Providing these updates on a request-by-request basis could still limit the risk that they would be shared more widely. Some respondents received requests for forensic reports from supply chain partners, which they rebuffed.

III. ALIGNING CONFIDENTIALITY PROTECTIONS AND CYBERSECURITY

[206] *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).

[207] *See supra* note 160.

[208] A respondent with knowledge of the case suggested this was widely misinterpreted as a viable strategy independent of a PCI investigation. As noted above, outside of similarly unusual circumstances, none of the lawyers we interviewed ran a dual-track investigation primarily because it was viewed as too costly and unnecessary for purposes of protecting privilege. *See supra* note 160.

[209] JOSEPHINE WOLFF, YOU'LL SEE THIS MESSAGE WHEN IT IS TOO LATE: THE LEGAL AND ECONOMIC AFTERMATH OF CYBERSECURITY BREACHES (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).

Lawyers' efforts to preserve the confidentiality of incident response are driven principally by the stated goal of limiting litigation risk to breached firms.[210] Yet empirical studies show that the vast majority of cyber-incidents are not litigated,[211] a trend that is likely to continue given the rise of ransomware attacks that may not result in the release of private information.[212] 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 face involving issues like establishing standing.[213] And, as Part I suggests, judges overseeing these cases often refuse to treat materials generated during incident response as privileged or otherwise exempt from discovery.[214] 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,[215] their cases typically involve relatively small incidents that are less likely to result in significant litigation costs.[216] Given that a small number of law firms dominate this space,[217] 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

---

[210] *See supra* Part II.B.

[211] *See* Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL L. STUD. 74, 85 (2013); 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. 123, 130-57 (2021). Both the prospect of litigation and its potential costs, moreover, are well understood to depend on several factors that can be observed 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 125.

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

[213] *See* McGeveran, *supra* note 3, at 110-11; Romanosky et al., *supra* note 211, at 76; Kesan & Zhang, *supra* note 211, at 159 (noting that overall dismissal rate of cybersecurity suits is high). *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018) (discussing standing issues associated with data breach litigation).

[214] *See supra* Part I.A..

[215] *See supra* Part II.B.

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

[217] Prior work has shown that just four law firms have the majority of relationships with cyberinsurers; notably one firm is on 80 percent of the panels in the study's sample. *See* Woods & Böhme, *supra* note 46.

governing confidentiality allows these lawyers to preserve their business model notwithstanding their limited technical sophistication.[218]

Irrespective of the potential benefits of these efforts to preserve the confidentiality of breach response, Part II demonstrated that they have large costs. Lawyers' focus on confidentiality is holding back the formal evidence base about the causes of cyber-incidents, limiting the understanding of key third parties in the cybersecurity ecosystem like insurers and regulators, and perhaps most perversely, denying internal IT teams the knowledge and information that 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 towards 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 when it comes to addressing the central problems described in Part II. 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, both in the form of an enhanced privilege and altered evidentiary rules. At the same time, it 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 II. 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

[218] 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 disclosing cybersecurity information to specific federal actors. Although both approaches have merit, they also have significant limitations in addressing the particular 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.[219] In each case, the goal of these privileges is to encourage honest and frank communication between individuals and trusted advisors or loved ones.[220]

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."[221] Both proposals envision a broad-ranging privilege that would extend to communications between cybersecurity professionals and their clients regarding preparing for or responding to cybersecurity threats to the client's networks or communication systems.[222] Moreover, both proposals employ a "functional" definition of who would qualify as a cybersecurity professional.[223]

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.[224] Additionally, the Sedona Report suggests that parties claiming the privilege should be required to sufficiently document their

---

[219] *See* Amanda H. Frost, *Updating the Marital Privileges: A Witness-Centered Rationale*, 14 WIS. WOMEN'S L.J. 1, 6-10 (1999).

[220] *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 cmt. c (2000).

[221] *See* Kosseff, *supra* note 22, at 285-303; Sedona Report, *supra* note 22, at 99-100.

[222] *See* Kosseff, *supra* note 22, at 285-303; Sedona Report, *supra* note 22, at 99-100.

[223] 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 22, at 300. *See also* Sedona Report, *supra* note 22, at 99-100 (proposing a privilege that would apply whenever "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").

[224] Sedona Report, *supra* note 22, at 97-100.

reasons for doing so to allow opposing parties to challenge that claim.[225] Perhaps most notably, the Sedona Report suggests a no-waiver rule when firms disclose privileged information to criminal law enforcement authorities investigating an attack.[226]

Both of these proposals have substantial 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.[227] And they would also provide companies with enhanced certainty that any efforts to document their incident response would not be discoverable in subsequent litigation.[228] As suggested in Part II, 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.[229]

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 remediate the risk of a cybersecurity incident. Yet our findings in Part II do not, we believe, provide sufficient support for concluding that confidentiality concerns significantly impair firms' pre-breach cybersecurity efforts.[230] 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.[231] Even in the isolated counter-examples we heard, the effects were generally limited to occasional routing of these efforts through attorneys and

---

[225] *See id.* at 100-01. The Sedona Report also suggests that its proposed privileged be implemented via legislation rather than common law to enhance certainty and uniformity. *See id.* at 107-08.

[226] *See id.* at 114-18.

[227] *See id.* at 105.

[228] *See* Kosseff, *supra* note 22, at 284.

[229] *See supra* Part II.A.

[230] 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 22, at 96. This, it notes, is ultimately an "empirical question." *Id.*

[231] *See supra* Part II.A.1.

editing of cybersecurity professionals' work product.[232]

For this reason, the overinclusivity 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.[233] 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.[234] Even worse, these cybersecurity proposals could have the perverse 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.

Not only are prior cybersecurity privilege proposals overinclusive, they are underinclusive as well. In particular, neither proposal would address prevailing concerns about breached firms or their lawyers sharing breach-related information with third parties.[235] To the contrary, both proposals seem to envision that ordinary rules of waiver would apply to their proposed cybersecurity privileges. The only exception is that the Sedona Report would create a limited no-waiver rule for information sharing with criminal law enforcement officials.[236] Ironically, however, Part II suggested that many lawyers and firms feel comfortable sharing oral information with law enforcement in the status quo, and that this information is typically sufficient for these officials to do their job.[237] Meanwhile, Part II 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.

---

[232] *See supra* Part II.A.1.

[233] *See* McGeveran, *supra* note 3; SOLOVE & HARTZOG, *supra* note 1, at 190-98; Hurwitz, *supra* note 12, at 1520 (explaining that "[l]aw, when working well, can create powerful incentives that align individual conduct with socially-optimal goals" when it comes to cybersecurity).

[234] *See* Sedona Report, *supra* note 22, at 98 (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.

[235] *See supra* Part II.C.

[236] Sedona Report, *supra* note 22, at 114-18.

[237] *See supra* Part II.C.

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 risk to firms of sharing information about cybersecurity incidents with the federal government. The most important example is The Cybersecurity Information Sharing Act of 2015 (CISA).[238] Under CISA, firms enjoy certain protections when they share "cyber threat indicators" and "defensive measures" for a "cybersecurity purpose."[239] These include protections from liability and waiver of any privileges for sharing such information.[240] However, these protections are subject to a host of limitations and caveats.[241] For instance, liability protections under CISA generally[242] only apply when firms share information with the federal government through a specific Department of Homeland Security (DHS) process.[243] Similarly, CISA only limits waiver of privilege when firms disclose information though this federal DHS process.[244] 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.[245]

In addition to CISA, Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). 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.[246] As with CISA, CIRCIA includes assurances that

[238] 6 U.S.C. §§ 1501-10 (2018). *See generally* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, Harv L. School Forum on Corporate Governance, (Thursday, March 3, 2016).

[239] CISA §104(c)(1).

[240] *See id.* §§106(b)(1) & 105(d)(1).

[241] *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).

[242] 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." CISA §105(c)(1)(B)(ii).

[243] CISA § 105(c).

[244] *Id.* § 105(d)(1).

[245] *Id*. §§104(d).

[246] CIRCIA § 103(a)(2), adding § 2240 to the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) (adopting the definition of Critical Infrastructure used in Presidential Policy Directive 21); Presidential Policy Directive – Critical Infrastructure Security and Resilience (2013), at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. 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.

disclosures made under the law will not result in liability or waiver of otherwise applicable privileges.[247]

Although these provisions in CISA and CIRCIA may encourage breached firms to share information about incidents with the federal government,[248] they do little to address most of the broader problems described in Part II. The scope of these laws is narrow, applying only to specific types of threat intelligence, certain classes of cybersecurity incidents, and specific government offices. By contrast, they do nothing to promote information sharing between breached firms and private actors—including insurers, auditors, and supply-chain partners.[249] Nor do they even do much to promote information sharing with firms' state and federal regulators.[250] 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. 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 remediate cybersecurity incidents;[251] instead, by focusing solely on disclosure of breach information rather than the production of this information, they seem to assume that breach response documentation functions work reasonably well. Yet to the extent that breached firms avoid documenting and fully 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

---

[247] CIRCIA § 103(a)(2), adding § 2245(b) to the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.).

[248] 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 241, at 585; Kristin N. Johnson, *Managing Cyber Risks*, 50 GA. L. REV. 547, 580 (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).

[249] *See supra* Part II.D.

[250] As noted above, some of CISA's protections do extend to certain communications to federal regulators. *See* note 242, *supra*.

[251] *See supra* Part II.B & C.

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 Part 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, Subsection One focuses on reforms that could provide firms with assurances that robust breach response documentation, communication, and information sharing would not meaningfully increase their litigation, regulatory, or reputational risks. Meanwhile, Subsection Two 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 towards providing breached firms with the assurances they need to prioritize their own cybersecurity and that of society more broadly in breach response. In particular, we propose that state and federal lawmakers create a non-waivable, 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,[252] as well as the potential unintended consequences such a privilege could create.[253] Instead, as its name suggests, the Cyber-incident Response privilege would only shield from discovery firms' incident response efforts.

Our proposed Cyber-incident Response privilege would thus be narrower than prior proposals in crucial ways; at the same time, it would also be stronger than prior proposals. First, building on the non-waiver 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

[252] *See supra* Part II.B.2.
[253] *See supra* Part II.A.1.

chain partners, or auditors.[254] This provision, of course, 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, our proposed Cyber-incident Response privilege would extend beyond communications between breached firms and cybersecurity professionals to cover internal communications within a breached firm. In doing so, the privilege would depart from the structure of conventional privileges, which all require communications between firms and outside professionals. This departure is, in our view, sensible because a major cybersecurity goal should not only be to encourage full and frank communication between firm personnel and outside parties like lawyers or forensic firms, but also to encourage full and frank internal communication within breached firms. Moreover, as Part II 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 parties involved in responding to this event 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, and most notably, 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, when appropriate, to commission the production of full incident response reports by cybersecurity firms.

Finally, and perhaps most notably, a Cyber-Incident Response privilege would enable insurers and regulators to demand access to documentation

---

[254] Under the law of some states, disclosure of privileged information to certain government actors does not operate as a waiver of privilege with respect 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 It All*, 30 SEATTLE U. L. REV. 155, 156 (2006)

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 data sets about cybersecurity controls and countermeasures and improve 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 not just theoretical: our interviews with insurers suggest that at least some carriers might be interested in stepping into that role.[255]

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 efforts that firms take in breach response. Such a rule could be patterned on Federal Rule of Evidence 407, which substantially limits the admissibility of "measures taken that would have made an earlier injury or harm less likely to occur."[256] The goal of that rule is to encourage, or at least not discourage, firms from taking remedial measures in furtherance of physical safety, such as repairs, installation of safety devices, and changes in company rules.[257] Under the rule, such efforts cannot permissibly be used to support an inference that the firm acted improperly in connection with an initial harm. 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 is that it can potentially be applied more broadly to materials like entire incident reports than the proposed evidentiary rule. Incident reports may, for instance, include descriptions of measures that the breached firm did not ultimately take following a breach and those may not be protected by the evidentiary rule. So the evidentiary rule on its own, without the privilege, might lead to further constraints on what can be included in reports, especially long-term recommendations that firms may not implement in the immediate aftermath of an incident and may therefore not fall under the protection of the proposed evidentiary rule.

By contrast, the advantage of the evidentiary rule would be that it applies

---

[255] Insurers also noted that their ability to do this would depend on their market power and whether other insurers were taking similar steps.

[256] *See* Fed. R. Evid. 407. *See generally* Bernard Chao, Kylie Santos, *How Evidence of Subsequent Remedial Measures Matters*, 84 MO. L. REV. 609, 613 (2019).

[257] *See* Comment to Fed. R. Evid. 407.

to certain facts that the cyber-incident 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 multi-factor authentication or password requirements would be factual information. 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 both 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 well impair accountability for breached firms. In particular, shielding firms' breach response efforts from discovery or introduction into evidence would mean that regulators and plaintiffs would have less capacity to hold firms accountable for their failure to take reasonably cybersecurity precautions. We take this concern seriously, notwithstanding the fact that most breaches do not in fact result in litigation or regulatory action.[258] In part, this is 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. And in part this is because even limited legal and regulatory actions in the past have produced important principles about firms' cybersecurity obligations that can have a broader positive effect.[259]

One way to accomplish this 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.[260] Extending these reporting obligations[261] to all severe

[258] *See supra* Part III..

[259] *See* McGeveran, *supra* note 3; Solove & Hartzog, *supra* note 12; Christopher Bradley, *Privacy for Sale* (draft, 2022). By contrast, it is quite clear that data breach notification laws do not result in significant information. *See* Paul Vaaler & Brad Greenwood, *Do Us State Breach Notification Laws Decrease Firm Data Breaches?* (Draft, 2022).

[260] *See supra* Part III.A.2.

[261] CIRCIA requires reporting of cybersecurity incidents by certain critical infrastructure operators to DHS including:

(i) A description of the covered cybersecurity incident, including identification of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident, and the estimated date range of such incident.

cybersecurity incidents, not just those affecting critical infrastructure, would be a significant step towards 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 (PCIDSS) requires that a certified investigator conducts an investigation to establish facts.

A second, and more ambitious, model might build on the PCIDSS to establish a mandatory forensic evidence collection pipeline that was entirely distinct from incident response. Private firms could coordinate this process or the obligation could be placed on independent technology providers.[262] 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 inconsistently collected.

Another variant of this more ambitious model would require firms that experience a sufficiently serious breach 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 build in analytical capabilities that produce (semi) automated reports. For example, one forensic provider demonstrated a tool that produced investigative reports for compromised Office 365 inboxes. 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 primarily that certain types of

---

(ii) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures relevant to such incident.

(iii) Where applicable, any identifying information related to the actor reasonably believed to be responsible for such incident.

(iv) Where applicable, identification of the category or categories of information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

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

incidents, such as the breach of personal identifying information, be reported, but not requiring the inclusion of many details about how they those incidents were perpetrated or what steps were taken to remediate them.[263]

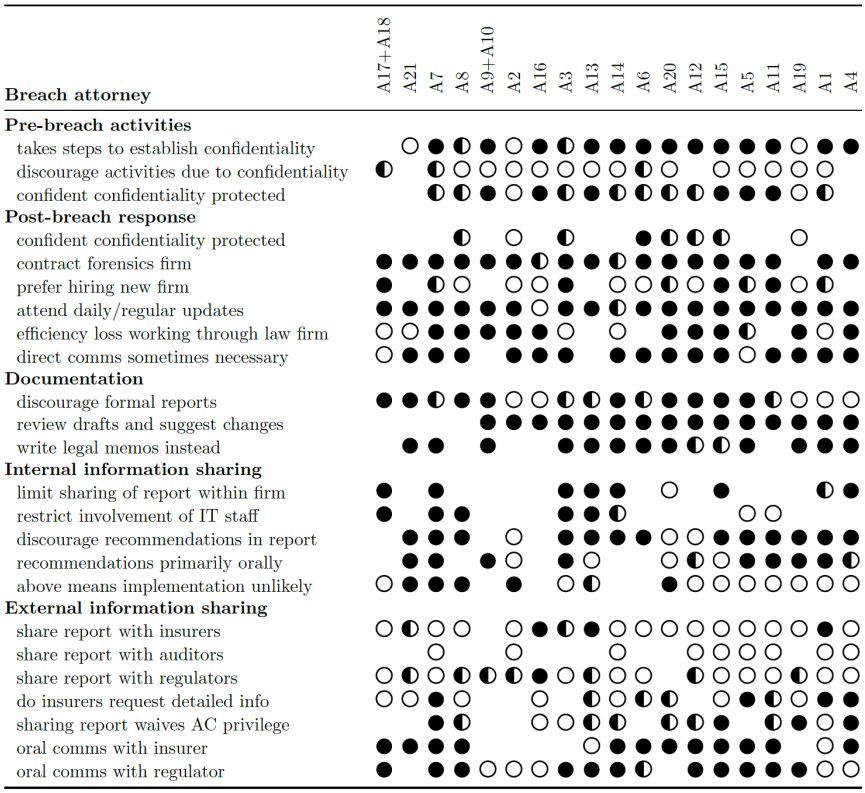
CONCLUSION

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 immediate 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 when cybersecurity investigation materials and pre-breach assessments are protected by attorney-client privilege or work product doctrine has exacerbated many of 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." Addressing these significant obstacles to both short-term and long-term cybersecurity necessitates greater clarification and tailoring of the confidentiality protections that apply to cybersecurity. To accomplish this, we suggest expanding the confidentiality protections that apply to incident response so as 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.

[263] *See* Vaaler & Greenwood, *supra* note 259.

Appendix

Table 1: Strategies employed by each breach attorney (A1–A21) 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 visually related similar response patterns.