I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

The Cybersecurity Privilege

JEFF KOSSEFF[1]

Cybersecurity threats – such as denial of service attacks, data theft, website defacement, and other incidents – cost U.S. companies billions of dollars a year in lost business, remediation, and other expenses. Cyberattacks also compromise individuals' privacy and reduce public confidence in the Internet and networked computing. Companies recognize these threats, and are increasingly relying on cybersecurity professionals to protect their networks and systems from hackers, and mitigate damage after data security incidents.

Unfortunately, U.S. evidentiary law discourages companies from hiring cybersecurity professionals to protect their networks and remediate security incidents. The work of cybersecurity professionals – unlike that of attorneys, accountants, and therapists – is not directly covered by a privilege under federal or state law. Accordingly, cybersecurity professionals' work product and communications is, by default, discoverable in litigation or regulatory proceedings. Cybersecurity work often relies on highly confidential information about a company's network vulnerabilities, and therefore the disclosure of the work product or communications could be useful to plaintiff's lawyers or regulators after a data security incident. To protect against this risk, companies attempt to cover their cybersecurity professionals' communications and work product under an existing evidentiary privilege, such as the attorney-client privilege or work product doctrine. However, such privileges are an uneasy fit for some cybersecurity work, particularly prophylactic measures that are not directly tied to ongoing or potential litigation. In other words,

---

[1] Assistant Professor of Cybersecurity Law, United States Naval Academy. B.A., M.P.P., University of Michigan; J.D., Georgetown University Law Center. The views expressed are only those of the author. I'd like to thank Professor Peter Shane, Trenton Weaver, and the staff of I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY for their excellent comments and edits.

current evidentiary law discourages companies from investing in the services necessary to prevent cyberattacks from occurring.

In this Article, I propose the creation of a stand-alone privilege for cybersecurity work. Courts should recognize a common-law cybersecurity privilege under Federal Rule of Evidence 501, just as they have recognized the attorney-client privilege, psychotherapist privilege, and priest-penitent privilege. There is a significant public interest in encouraging companies to hire professionals to assess cybersecurity and close potential gaps. Companies will be more likely to make such investments if they have some assurance that the cybersecurity professionals' communications and work product will not later be discovered in court. Although courts are hesitant to create new privileges, the strong societal interest in promoting cybersecurity justifies the creation of a new common-law privilege. Alternatively, legislators should consider creating a statutory privilege for cybersecurity professionals, as they have for journalists, accountants, and others whose work serves the public interest.

INTRODUCTION

Large-scale data security breaches, such as the late 2014 hack of Sony,[2] have upended companies' operations, exposed the personal information of millions of individuals, and caused widespread political and economic disruption. In addition to high-profile breaches, companies of all sizes and industries experience data security incidents that do not receive as much attention, but threaten their business secrets and consumers' personal information.[3]

Recognizing these significant threats, companies increasingly are hiring cybersecurity professionals to prevent and remediate data security incidents. Cybersecurity professionals play a preventative role by ensuring that computer systems, networks, hardware, and service providers are equipped with effective safeguards from attack, and they also help companies develop internal use policies and train employees.[4] Cybersecurity professionals also remediate harm after a

---

[2] *See, e.g.*, Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 4, 2015).

[3] *See, e.g.*, Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015).

[4] *See M-Trends 2015: A View from the Front Lines*, MANDIANT, at 23 ("As cyber security goes mainstream, organizations should consider data breaches in a new light – not a source of fear and shame but a business reality.").

data security incident by investigating the cause of the breach and securing the information assets from further attack.[5]

Unfortunately, cybersecurity professionals' work product – and their direct communications with clients – are not, by default, protected by discovery through an evidentiary privilege.[6] Although the common law provides privileges to a number of professions that deliver critical services, such as attorneys and therapists,[7] no such privilege directly applies to cybersecurity professionals.

The lack of a privilege for cybersecurity work product and communications creates significant legal exposure for companies that seek to protect their systems and repair vulnerabilities. Data security incidents are increasingly the cause of multi-million-dollar class action lawsuits under a variety of state common law claims and statutes. Moreover, state and federal regulators are increasingly bringing enforcement actions and lawsuits against companies that they believe failed to take proper steps to protect consumers' personal information.[8] Cybersecurity professionals' work product often contains candid assessments of vulnerabilities, and therefore could be very damaging evidence against the client in litigation or a regulatory enforcement action.[9] This creates a disincentive to hire cybersecurity professionals to assess and remediate vulnerabilities in companies' information technology infrastructure. Ultimately, this results in more cybersecurity vulnerabilities throughout the private sector, an outcome that clearly is not in the public interest.

In recent years, companies have attempted to solve this problem by engaging cybersecurity professionals through attorneys, providing some coverage of the work product through the attorney client

---

[5] *Id.*

[6] *See* Section II, *infra*.

[7] *See generally* Jaffee v. Redmond, 518 U.S. 1 (1996).

[8] *See, e.g.*, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

[9] Cybersecurity consultants frequently offer candid, in-depth assessments of potential clients' vulnerabilities, see, e.g., *Is your Web site fully protected?*, ZENEDGE, https://www.zenedge.com/cybersecurity-vulnerability-and-threat-assessment (last visited Mar. 7, 2016) ("Leveraging industry-standard threat assessment techniques to analyze risks and vulnerabilities, our ZENEDGE Vulnerability and Threat Assessment process evaluates the potential vulnerabilities facing your web properties and web applications to deliver an objective third-party threat assessment, complete with in-depth analysis and recommendations for hardening cybersecurity.").

privilege and the work product doctrine.[10] However, this is only a partial solution, as the scope of the privilege for attorneys often does not fully encompass the work of cybersecurity professionals. Litigants are increasingly challenging companies' attempts to cover the work product and communications of cybersecurity professionals under the attorney-client privilege. Moreover, tying the privilege to attorney-related matters discourages companies from taking proactive cybersecurity measures *before* they face significant legal risk.

In this article, I argue for the creation of a standalone privilege – either through common law or by statute – for the work and communications of cybersecurity professionals. Courts are understandably hesitant to create new common-law privileges.[11] However, this is an extraordinary case in which a new privilege is justified, due to the sensitive nature of data gathered, produced, and created by cybersecurity professionals, as well as the crucial role that they play in protecting businesses and consumers.

Part I of this article outlines the challenges that companies face in securing their networks and systems, the roles that cybersecurity professionals play in helping companies prepare for and respond to cybersecurity events, and the types of work product and communications that cybersecurity professionals produce. Part II provides an overview of the current evidentiary protections for cybersecurity work product and communications through the attorney-client privilege and work client doctrine. It also examines the results in recent cases in which companies have attempted to prevent the disclosure of cybersecurity communications and work product in litigation, and argues that these cases demonstrate the inadequacy of the attorney-client privilege for cybersecurity. Part III examines the Supreme Court's standard for creating a common-law privilege under Federal Rule of Evidence 501, and explains why a cybersecurity privilege would satisfy that standard. Alternatively, I argue, there is sufficient public interest to justify Congress and state legislatures enacting a statutory cybersecurity privilege. Part IV suggests legal rules and standards to ensure balanced and fair application of a cybersecurity privilege, including methods by which

---

[10] *See* Section II.A, *infra*.

[11] *See* United States v. Bryan, 339 U.S. 323, 331 (1950) ("[W]e start with the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctly exceptional, being so many derogations from a positive general rule.").

courts could identify cybersecurity professionals who would be covered by the privilege.

I. THE GROWING IMPORTANCE OF CYBERSECURITY PROFESSIONALS

Before exploring the reasons that courts should protect the confidentiality of cybersecurity work and communications, it is important to understand what cybersecurity is, and why cybersecurity has become increasingly important to businesses in recent years.

Cybersecurity is a relatively new concept for courts. Indeed, few U.S. courts have used the term, and none have articulated a common definition for cybersecurity.[12] The Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies (NICCS) offers a fairly comprehensive definition of cybersecurity: "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[13] That definition, which is based on various documents and policies issued by Department of Homeland Security, National Institutes of Standards and Technology, and the White House, makes clear that cybersecurity includes the protection of both systems *and* information. This definition also correctly makes clear that cybersecurity is different from privacy, which NICCS defines as the "assurance that the confidentiality of, and access to, certain information about an entity is protected."[14] Although cybersecurity can help to protect individuals' privacy, the terms are not interchangeable. Privacy involves assuring individuals that their personal data is protected, while cybersecurity more broadly encompasses the steps that a company takes to protect its systems *and* the information that is stored on those systems. If a company does not enact the necessary cybersecurity safeguards, then its consumers' and employees' privacy may be more likely to be at risk. Accordingly, companies are increasingly focusing on cybersecurity.

---

[12] The first published U.S. court opinion to use the term "cybersecurity" was *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007), which, in a footnote, cited an article noting "the propriety of the analogy between toxic torts and cybersecurity breaches."

[13] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, http://niccs.us-cert.gov/glossary (last visited Mar. 7, 2016).

[14] *Id.*

To demonstrate businesses' increased need for cybersecurity, Part A of this Section provides an overview of the scope of the cybersecurity challenges that businesses face, and the economic harm that data breaches and other incidents can cause. Part B of this Section explains the work that cybersecurity professionals do to prevent incidents from occurring and remediate damage after incidents have taken place.

A. *Increase in Cybersecurity Incidents*

It is rare for a week to go by without a headline about data breaches at large companies or government agencies. In a 2014 survey by the Ponemon Institute, 43 percent of companies reported data breaches in the previous year, up from 33 in 2013.[15] According to the Identity Theft Resource Center, the number of U.S. data breaches rose by 27.5 percent between 2013 and 2014.[16]

Data breaches can be incredibly costly for companies. In its annual report about data security, the Ponemon Institute found that the average total cost of a single U.S. data breach was $6.53 million in 2014, up from $5.85 million in 2013.[17] The average cost per compromised U.S. record was $217, up from $201 a year earlier.[18] Ponemon estimates that approximately 26 percent of the costs are attributed to detection and escalation services, such as forensics, audits, and crisis management.[19] Approximately 28 percent of the costs are associated with ex-post response, such as help desk, remediation, and legal expenses. Less than 5 percent are attributed to the costs of notifying individuals and regulators of the breaches.[20] The

---

[15] *Is Your Company Ready for a Big Data Breach?: The Second Annual Study on Data Breach Preparedness*, PONEMON INSTITUTE RESEARCH REPORT, Sept. 2014.

[16] *Identity Theft Resource Center Breach Report Hits Record High in 2014*, IDENTITY THEFT RESOURCE CENTER (Jan. 12, 2015), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

[17] *2015 Cost of Data Breach Study: Global Analysis*, PONEMON INSTITUTE RESEARCH REPORT, May 2015, at 7.

[18] *Id.* at 5.

[19] *Id.* at 17.

[20] *Id.*

remainder -- more than 41 percent -- comes from business that was lost due to the breach.[21]

Indeed, the litigation costs after data breaches are unpredictable and can reach many millions of dollars in attorney fees and settlements. For instance, after more than 77 million PlayStation user records were hacked in 2011, Sony settled a class action lawsuit for $15 million.[22] Similarly, after a 2009 data breach involving 460,000 consumers, healthcare company AvMed settled a class action lawsuit for $3.1 million.[23]

To fully understand the cost of data breaches, consider the 2013 attack on the payment systems of Target. During the holiday shopping season, hackers installed malware on Target's internal sales network by logging in with credentials used by one of Target's heating, ventilation, and cooling contractors.[24] This led to the exposure of tens of millions of customers' personal information, including credit card numbers.[25] The company's holiday sales fell below expectations, and the company attributed the decline to the data breach.[26] The next

---

[21] *Id.*

[22] Timothy J. Seppala, *The Claim Process for Sony's $15 Million PSN Breach Lawsuit Starts Now*, ENGADGET (Jan. 24, 2015), https://www.engadget.com/2015/01/24/psn-breach-payment-form/.

[23] Marianne Kolbasuk McGee, *Settlement in AvMed Breach Suit: Class Action Settlement Offers Payments for Lack of Security*, DATA BREACH TODAY (Oct. 31, 2013), http://www.databreachtoday.com/settlement-in-avmed-breach-suit-a-6188.

[24] Jaikumar Vijayan, *Target Breach Happened Because of a Basic Network Segmentation Error*, COMPUTERWORLD (Feb. 6, 2014), http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html; *see also* Mary A. Chaput, *Calculating the Colossal Cost of a Data Breach*, CFO (Mar. 24, 2015), http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/ ("The asking price in health-care data breach lawsuits has typically been in the $1,000 per victim range, but few have come to fruition due to the courts' reluctance to confer standing on the potential of future harm — until now. In the Adobe Systems breach case, the U.S. District Court recently found that such potential future harm is sufficient to allow a putative class of plaintiffs to proceed in federal court.").

[25] Meagan Clark, *Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer*, INTERNATIONAL BUSINESS TIMES (May 5, 2014), http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

[26] *Id.*

month, Target laid off nearly 500 headquarters employees.[27] Congress held hearings about the breach. Through the end of 2014, Target accumulated $252 million in expenses related to the breach, though those costs were partly offset by $90 million in insurance payments.[28] Those expenses did not include potential judgments or settlements in the numerous class action lawsuits that customers and others filed against Target as a result of the breach.[29]

Some companies are forced to shutter operations entirely after data breaches. According to the House Small Business Subcommittee on Health and Technology, nearly 60 percent of small businesses are forced to shut down within six months of a data security incident.[30] For instance, in 2014, hackers deleted a great deal of sensitive data from the servers of Code Spaces, a software-as-a-service provider, forcing the small company to go out of business within a week.[31] And in 2015, Altegrity, a background investigations firm, filed for bankruptcy in 2015 after a state-sponsored cyberattack.[32]

Cybersecurity also is a significant problem for government agencies, as seen in the 2015 breach of millions of employees' data at the Office of Personnel Management. According to a report from the Government Accountability Office, 67,168 cyber incidents harmed federal government computer systems in 2014, an increase of more than 1,000 percent in eight years.[33]

---

[27] *Id.*

[28] Ingrid Lunden, *Target Says Credit Card Data Breach Cost It $162M in 2013-14*, TECHCRUNCH (Feb. 25, 2015), https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/.

[29] *Id.*

[30] Press Release, Collins Subcommittee Examines Small Business Cyber-Security Challenges With New Technologies, House Small Business Subcommittee on Health and Technology Chairman (Mar. 21, 2013), http://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=325034#sthash.bKjrBI5W.dpuf.

[31] Adam Greenberg, *Code Spaces Shuts Down Following DDoS Extortion, Deletion of Sensitive Data*, SC MAGAZINE (Jun. 19, 2014), http://www.scmagazine.com/code-spaces-shuts-down-following-ddos-extortion-deletion-of-sensitive-data/article/356774/.

[32] Linda Sandler and Andrea Tan, *Altegrity Files Bankruptcy After 'State-Sponsored' Breach*, BLOOMBERG (Feb. 8, 2015), http://www.bloomberg.com/news/articles/2015-02-09/altegrity-files-for-bankruptcy-after-losing-vetting-contracts.

[33] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-290, HIGH RISK SERIES: AN UPDATE, 241 (Feb. 2015), *available at* http://www.gao.gov/assets/670/668415.pdf.

These statistics demonstrate that cybersecurity is a real and growing problem for organizations large and small, public and private. For good reason, President Barack Obama identified cyber threats as "one of the most serious economic national security challenges that we face as a nation."[34]

B. *Emergence of the Cybersecurity Profession*

Recognizing the huge threats that security incidents can pose for businesses, a cybersecurity industry has quickly emerged. The global cybersecurity industry is estimated to generate $75.4 billion in 2015, and is projected to grow to $170 billion in 2020.[35] Although the Bureau of Labor Statistics does not track the number of cybersecurity professionals, the demand for skilled cybersecurity labor reportedly has surged in recent years.[36]

Companies use cybersecurity forensics firms for two general purposes: (1) preventing cybersecurity incidents; and (2) remediating and mitigating harm after a data security incident already has occurred. Both tasks can be costly and time-consuming, and require companies to provide cybersecurity consultants with broad access to information about data processing and storage. This data is highly sensitive and could be damaging to the company, particularly during a regulatory investigation or litigation arising from an alleged data security incident.

Among the most common steps that companies take to prevent cybersecurity incidents is developing an incident response plan.[37] The

---

[34] Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015) ("When companies get hacked, Americans' personal information, including their financial information, gets stolen. Identity theft can ruin your credit rating and turn your life upside down.").

[35] Tara Seals, *Cybersecurity Spending to Hit $170Bn by 2020*, INFOSECURITY MAGAZINE (July 13, 2015).

[36] Martin C. Libicki et al., *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, RAND CORPORATION ("There is a general perception that there is a shortage of cybersecurity professionals within the United States, and a particular shortage of these professionals within the federal government, working on national security as well as intelligence. Shortages of this nature complicate securing the nation's networks and may leave the United States ill-prepared to carry out conflict in cyberspace.").

[37] Tucker Bailey et al., *How Good is Your Cyberincident Response Plan?*, MCKINSEY & CO. (Dec. 2013), http://www.mckinsey.com/insights/business_technology/how_good_is_your_cyberincident_response_plan.

main goal of such plans is to minimize the damage caused by a data security incident and build confidence among the public and regulators.[38] To develop an incident response plan, cybersecurity professionals must first conduct interviews and review information technology functions throughout the company to understand the systems and data flows and identify the information and systems that are most vulnerable to a cyberattack.[39] Once companies have developed incident response plans, they run table-top exercises in which employees and managers throughout the company respond to a simulated data security incident. A cybersecurity professional typically oversees the process and provides feedback to help the company hone its response.[40]

Relatedly, companies engage cybersecurity professionals to develop information security policies. Like the incident response plan, the goal of security policies is to prepare a company for a cybersecurity incident.[41] Among the information security policies that companies consider adopting are policies that cover encryption, acceptable Internet use, password protection, remote access, vendor management, and monitoring.[42] To develop information security policies – and the programs to implement these policies – cybersecurity professionals first must comprehensively examine and understand a company's systems and networks, as well as the

---

[38] *Id.*

[39] *Id.*

[40] *See* Tucker Bailey and Josh Brandley, *Ten Steps to Planning and Effective Cyber-Incident Response*, HARV. BUS. REV. (July 1, 2013) ("The best-prepared organizations routinely conduct war games to stress-test their plans, increasing managers' awareness and fine-tuning their response capabilities."); Judy Selby and Lynn Sessions, *Building a Breach Response Team, Before You Have a Breach*, CSO (Oct. 3, 2014) ("Proactive retention of a breach response team provides the entity with the opportunity to engage in practice runs and fire drills to rehearse their response to a breach incident, which can help to identify communication, technical or other snags before a breach ever happens.").

[41] R. Daniel Lee, *Developing Effective Information System Security Policies*, SANS INSTITUTE, http://www.sans.org/reading-room/whitepapers/policyissues/developing-effective-information-systems-security-policies-491 ("Unfortunately, threats do exist and information systems security policies are necessary to provide a framework for selecting and implementing countermeasures against them. An enforceable written policy helps ensure that everyone within the organization coherently behaves in an acceptable manner with respect to information security.").

[42] *Information Security Policy Templates*, SANS INSTITUTE, https://www.sans.org/security-resources/policies (last visited Mar. 8, 2016).

potential technical and human vulnerabilities that could lead to a security incident.[43]

Companies also engage cybersecurity professionals to perform penetration tests, which "prove (or disprove) real-world attack vectors against an organization's IT assets, data, humans, and/or physical security."[44] The results of these tests can help a company reconfigure its systems, policies, and processes to guard against security threats.[45]

Cybersecurity professionals' second task – remediating and mitigating harm *after* a security incident – often carries more urgency and must begin immediately.[46] Cybersecurity professionals must immediately gain full access to a network to determine the extent of the intrusion, and the necessary steps to remediate any damage and prevent further unauthorized access.[47] The cybersecurity experts and lawyers must work together to determine whether they are legally required to notify state regulators or consumers of the breach under a state notification law.[48] Cybersecurity professionals also collaborate

---

[43] Natalie Timms, *Secure Networks: How to Develop an Information Security Policy*, INFORMATIONWEEK NETWORK COMPUTING (Jan. 23, 2014) ("It's critical to understand what you are trying to secure and why; if you don't understand the underlying network, how can you secure it? Network addressing schemes, choice of routing protocol, and correct mapping of physical connections, such as switch ports to logical configurations, are basic components that must be understood.").

[44] Eric Basu, *What Is a Penetration Test and Why Would I Need One for My Company?* FORBES (Oct. 12, 2013) ("A penetration test is designed to answer the question: 'What is the *real-world* effectiveness of my existing security controls against an active, human, skilled attacker?'").

[45] *Id.*

[46] *See* Karen Kent et al., *Guide to Integrating Forensic Techniques into Incident Response*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, at 2-3 ("Practically every organization needs to have some capability to perform computer and network forensics. Without such a capability, an organization will have difficulty determining what events have occurred within its systems and networks, such as exposures of protected, sensitive data.").

[47] Nate Lord, *Data Breach Experts Share the Most Important Next Step You Should Take After a Data Breach in 2014-15 & Beyond*, DIGITAL GUARDIAN (May 4, 2015) ("By bringing in an unbiased, third-party specialist, you can discover exactly what has been accessed and compromised, identify what vulnerabilities caused the data breach, and remediate so the issue doesn't happen again in the future.").

[48] Forty-seven states and the District of Columbia require companies to notify consumers or regulators of the breach of certain types of unencrypted personal information. State laws vary in terms of the categories of personal information that trigger the notification requirements. *See Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE

with public affairs departments and consultants to publicly explain the incident in a manner that is prompt, complete, and accurate.[49]

In short, the cybersecurity profession has quickly developed as companies have experienced an increase in the size, frequency, and cost of data security incidents. Cybersecurity professionals wear multiple hats, including auditor, technologist, policymaker, strategist, and spokesperson. To perform such wide-ranging duties, cybersecurity professionals must have broad and unfettered access to information that a company or organization may store in a variety of media and formats.[50] Such information may well be sensitive and highly confidential. Accordingly, a company will be more likely to provide such broad access if it has a reasonable assurance that the cybersecurity professional will not be forced to reveal that information in court or to a regulatory agency.

Why should a company care about the exposure of this information? Quite simply, it increases the risk of losing a civil lawsuit or being a target of a regulatory investigation. For example, if a company experiences a data breach that leads to customers' identity theft, it likely would face a wide range of lawsuits, including common-law negligence. The information communicated or created by its cybersecurity consultant – if not privileged – could be used by a plaintiff to establish that the company failed to exercise reasonable care.

LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Mar. 8, 2016).

[49] Natalie Burg, *Five Lessons for Every Business From Target's Data Breach*, FORBES (Jan. 17, 2014) ("[A] security crisis can very quickly turn into a crisis of trust and loyalty if swift communications and responsive customer service aren't employed — even if the fault lies with the same weak credit card security used by so many other businesses.").

[50] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *supra* note 46 at 3-2 ("The increasingly widespread use of digital technology for both professional and personal purposes has led to an abundance of data sources. The most obvious and common sources of data are desktop computers, servers, network storage devices, and laptops. These systems typically have internal drives that accept media, such as CDs and DVDs, and also have several types of ports (e.g., Universal Serial Bus [USB], Firewire, Personal Computer Memory Card International Association [PCMCIA]) to which external data storage media and devices can be attached.").

II. WHY EXISTING PROTECTIONS FOR CYBERSECURITY COMMUNICATIONS AND WORK PRODUCT ARE INADEQUATE

As described above, cybersecurity consultants often have access to incredibly sensitive information about their clients' data security practices and information technology infrastructure. Such information could be extremely damaging to the company in litigation or a regulatory investigation. Accordingly, companies have a great incentive to ensure that cybersecurity consultants' work product and communications are protected from disclosure under a privilege.[51]

Unfortunately, neither the common law nor statutes provide a privilege for the work product or communications of cybersecurity experts. Instead, companies that seek to maintain the confidentiality of their cybersecurity work and communications often retain consultants through their outside counsel, because their work is more likely to be privileged than if it were conducted directly for the company. For instance, the head of a large cyberinvestigations practice advises prospective clients that they should retain his firm through outside counsel. [52]

Although there are no statistics or empirical studies on the concerns that companies have about ensuring that cybersecurity work is privileged, anecdotally, it often is one of the first issues that they address after a data breach or other incident. As Adam Cohen, Managing Director at Berkley Research Group, aptly wrote recently, "[t]he more litigation we see in the cybersecurity realm, the more likely it is that joint legal-technical work in that realm is 'in anticipation of litigation' and for purposes of rendering legal advice."[53]

---

[51] *See, e.g.* Stuart A. Panensky, *The Use of Attorney Client Privilege for Cyber-Focused Risk Assessments*, INSURANCE COVERAGE AND PRACTICE (Dec. 2013) ("A significant concern of organizations is that the written reports generated at the culmination of such a risk assessment, whether conducted internally or by an external party, may provide a roadmap for an adversary. It is important for an organization to seek to protect such reports from unwanted discovery.").

[52] *See* Christopher M. Matthews, *Law Firms Tout Cybersecurity Cred*, WALL ST. J. (Apr. 1, 2013) ("While a forensics firm such as Kroll can detect malware, scour network-access logs or understand the modus operandi of a foreign hacking group, if Kroll is contracted directly by the company rather than by an outside lawyer, that work is unlikely to be protected by attorney-client privilege, he says.").

[53] Adam Cohen, *Bringing Cybersecurity Under a Protective Umbrella (of Privilege)*, INSIDECOUNSEL (Sept. 15, 2015).

Cohen stressed that it "is critical for lawyers to be involved in leading cybersecurity efforts."[54]

The attorney-client privilege and related protections, however, do not fully shield cybersecurity work and communications from discovery. As demonstrated below, the three most applicable protections – the attorney-client privilege, attorney work product doctrine, and non-testifying experts privilege – do not cover the full scope of cybersecurity professionals' work product.

A. *Attorney-Client Privilege*

The attorney-client privilege protects from discovery communications between attorneys and clients in the course of seeking and providing legal advice.[55] The privilege is nearly absolute and only contains a few limited exceptions, such as instances in which the attorney helped the client perpetrate crime or fraud,[56] or if the client disputes the attorney's competence or job performance.[57]

This broad privilege is intended "to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[58] The privilege "exists to protect not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice."[59]

---

[54] *Id.*

[55] Upjohn Co. v. Unites States, 449 U.S. 383, 388 (1981).

[56] United States v. Zolin, 491 U.S. 554, 563 (1989) ("It is the purpose of the crime-fraud exception to the attorney-client privilege to assure that the seal of secrecy between lawyer and client does not extend to communications made for the purpose of getting advice for the commission of a fraud or crime.") (citation omitted) (internal quotation marks omitted).

[57] United States v. Pinson, 584 F.3d 972 (10th Cir. 2009) ("The theoretical basis for the assertion that raising an ineffective-assistance claim waives attorney-client privilege is the exception to the privilege that applies when a litigant chooses to place privileged communications directly in issue.").

[58] *Upjohn*, 449 U.S. at 388.

[59] *Id.* at 384.

Although the attorney-client privilege is absolute, it only covers certain types of communications.[60] The specific elements of the privilege vary slightly by jurisdiction, but the following Ninth Circuit summary generally is an accurate illustration of the privilege's scope of coverage:

> (1) When legal advice of any kind is sought (2) from a professional legal adviser in his or her capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are, at the client's instance, permanently protected (7) from disclosure by the client or by the legal adviser (8) unless the protection be waived.[61]

The privilege, therefore, protects communications from the client to the attorney – or from the attorney to the client – that are exchanged for the purpose of rendering legal advice. The privilege protects *communications*, and does not protect the evidence underlying the communications. For instance, suppose a company is reviewing its server logs and discovers an apparent breach. The company's CIO immediately emails a description of the apparent breach to the company's outside counsel. Although the CIO's email to the attorney may be privileged, the server's logs would not be privileged.

Additionally, the attorney-client privilege only applies to communications that seek or provide *legal* advice. For instance, if a company's lawyers advise on *and* help implement a business transaction, only the legal advice that they provide will be privileged. Any "business advice" likely will fall outside of the scope of the privilege, though courts may disagree as to whether a specific communication is legal or business advice. [62] Applying this

---

[60] *See generally* Mohawk Indus., Inc. v. Carpenter, 130 S. Ct. 599 (2009).

[61] United States v. Martin, 278 F.3d 988, 999 (9th Cir. 2002).

[62] United States v. ChevronTexaco, 241 F. Supp. 2d 1065, 1069 (N.D. Cal. 2003) ("Because the purported privileged communications involve attorneys who apparently performed the dual role of legal and business advisor, assessing whether a particular communication was made for the purpose of securing legal advice (as opposed to business advice) becomes a difficult task."); Cuno, Inc. v. Pall Corp., 121 F.R.D. 198, 204 (E.D.N.Y. 1988) ("[w]here a lawyer mixes legal and business advice the communication is not privileged 'unless the communication is designed to meet problems which can fairly be characterized as predominantly legal'").

framework, if a company emails a cybersecurity consultant with a question about network protection and merely CC's the company's lawyer, a court may find that the communication was unrelated to *legal* advice, and therefore not protected by the attorney-client privilege.

Moreover, if a third party receives the communication, a court may find that the attorney-client privilege does not apply in that situation.[63] However, communications may still be protected if they include non-lawyers who are assisting the lawyer in the representation. For instance, the communications of an accountant or translator working for a law firm may be protected by the privilege. As Judge Friendly wrote a half-century ago, "[w]hat is vital to the privilege is that the communication be made in confidence for the purpose of obtaining legal advice from the lawyer."[64] Similarly, the attorney-client privilege covers consultants who perform work under the supervision of attorneys, if that work is conducted as part of the attorney's representation of clients.[65]

Accordingly, if a cybersecurity professional helps an attorney provide legal advice to a client, those communications may be covered by the attorney-client privilege. However, the attorney-client privilege is of limited use for a good deal of the work that cybersecurity professionals perform. Perhaps the largest obstacle for the purposes of cybersecurity consulting is the requirement that the communications relate to legal advice.[66] For instance, an email that describes the result of a network vulnerability test, for example, likely would not qualify as legal advice. Even if a cybersecurity professional is supervised by an attorney, there is no guarantee that the professional's communications with the attorney or client would be protected under the attorney-client privilege.

---

[63] *See* Cavallaro v. United States, 284 F.3d 236, 237 (1st Cir. 2002) ("The presence of third parties during an attorney-client communication is often sufficient to undermine the 'made in confidence' requirement, or to waive the privilege[.]") (internal citations omitted).

[64] United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961).

[65] *See* Fed. Trade Comm'n v. TRW, Inc., 628 F.2d 207, 212 (D.C. Cir. 1980) ("[T]he attorney-client privilege can attach to reports of third parties made at the request of the attorney or the client where the purpose of the report was to put in usable form information obtained from the client.").

[66] *See Kovel*, 296 F.2d at 922 ("If what is sought is not legal advice but only accounting service . . ., or if the advice sought is the accountant's rather than the lawyer's, no privilege exists.").

B. *Work Product Doctrine*

The work product doctrine is more likely to cover some cybersecurity work that is performed at the direction of attorneys, but the doctrine, unlike the attorney-client privilege, is not absolute.

The doctrine was first articulated in 1947, when the Supreme Court ruled in *Hickman v. Taylor*[67] that an attorney's notes and reports based on witness interviews could not later be discovered in litigation involving the attorney's client. Although the Court concluded that the attorney-client privilege does not protect the documents,[68] it nonetheless denied discovery, reasoning that the request was "an attempt to secure the production of written statements and mental impressions contained in the files and the mind of the attorney . . .without any showing of necessity or any indication or claim that denial of such production would unduly prejudice the preparation of petitioner's case or cause him any hardship or injustice."[69]

The *Hickman* work product doctrine was later codified in Federal Rule of Civil Procedure 26(b)(3).[70] That rule provides that "[o]rdinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)."[71] However, the rule is not absolute: it allows discovery if "the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means"[72] or if a court otherwise finds good cause to order the disclosure of relevant work product.[73] If the Court orders disclosure of work product, "it must protect against disclosure of the

---

[67] *Hickman*, 329 U.S. 495 (1947).

[68] *Id.* at 508.

[69] *Id.* at 509.

[70] *See* United States v. Adlman, 134 F.3d 1194, 1197 (2d Cir. 1998) ("Rule 26(b)(3) codifies the principles articulated in *Hickman*.").

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

[72] Fed. R. Civ. P. 26(b)(3)(A)(ii).

[73] Fed. R. Civ. P. 26(b)(3)(A)(i).

mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation."[74]

The work product doctrine covers more than just communications that are necessary for legal advice. The doctrine protects *work product* that is prepared in anticipation of litigation or trial. Moreover, Federal Rule of Civil Procedure 26 explicitly states that *consultants'* work product may be protected, provided that it is prepared in anticipation of litigation. Indeed, courts have held that the work product doctrine applies to materials prepared by environmental consultants,[75] medical device safety consultants,[76] and insurance claims investigators.[77] Similarly, a cybersecurity professional's report might be protected by the work product doctrine.[78]

However, the exceptions to the work product doctrine limit the extent of the protection that it provides to cybersecurity work. Perhaps most importantly, is the requirement that the work product be prepared in anticipation of litigation or trial. The Second Circuit, reflecting a common approach to the doctrine, interpreted work product to have been created "in anticipation of litigation" if "in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation."[79] Although this approach is relatively broad and could encompass large swaths of documents, the party asserting the work product doctrine would need

---

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

[75] Martin v. Bally's Park Place Hotel & Casino, 983 F.2d 1252, 1260-62 (3d Cir. 1993).

[76] Ebert v. C.R. Bard, Inc., 2014 WL 1632155, at *1 (E.D. Pa. Apr. 24, 2014).

[77] Carver v. Allstate Insurance Co., 94 F.R.D. 131 (S.D. Ga. 1982).

[78] *See* Benjamen C. Linden et al., *Use Outside Counsel to Control Data Breach Loss*, BLOOMBERG BNA (Mar. 21, 2014) ("The work product doctrine may be an additional means to shield findings from a post-breach investigation during subsequent litigation. Whereas the attorney-client privilege applies only to communications, work product applies broadly to 'documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent).' Thus, when investigative documents in the aftermath of a breach are prepared primarily in anticipation of litigation, the doctrine might protect them. However, when documents appear to be the product of a routine investigation and were not prepared primarily in anticipation of litigation, courts are much less likely to protect the work product doctrine.").

[79] *See* United States v. Adlman, *supra* note 70 at 1202 (citations omitted) (internal quotation marks omitted).

to demonstrate that the materials were created *because of* potential litigation. A consultant's report about the causes of a data breach likely would have a greater chance of being covered by the work product doctrine than the consultant's annual, routine assessment of a company's cybersecurity controls. The company would have a stronger argument that consultant prepared the data breach report in response to a real threat of actual litigation. The annual, routine assessment, in contrast, is less likely to be likened to a real prospect of litigation. This creates a perverse result: companies likely receive *less* protection for taking proactive measures to *protect* their networks from attacks than they do for taking remedial measures *after* breaches have occurred.

Moreover, even if work product was prepared in anticipation of litigation, a court *still* could require its disclosure if the court concludes that the party requesting the materials has demonstrated a substantial need or other good cause for the discovery.[80] Routine work product is less likely to receive protection under the work product doctrine unless it is "core" or "opinion" work product related to an attorney's conclusions or impressions about particular litigation.[81] In the cybersecurity context, this means that a forensics expert's initial evaluation of a data breach most likely could be discovered in subsequent litigation if the opposing party demonstrates substantial need or good cause. In contrast, that consultant's analysis of claims in a pending complaint arising from the data breach is more likely to be protected under the work product doctrine. Again, this dichotomy results in cybersecurity professionals' work receiving less protection if it is not related to ongoing litigation.

Although the work product doctrine has a broader scope than the attorney-client privilege, the work product doctrine is not absolute. Because litigants could successfully argue that a good deal of the work performed by cybersecurity consultants falls within one of the

---

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

[81] *In re* Cendant Corp. Securities Litigation, 343 F. 3d 658 (3d Cir. 2003) ("Stated differently, Rule 26(b)(3) establishes two tiers of protection: first, work prepared in anticipation of litigation by an attorney or his agent is discoverable only upon a showing of need and hardship; second, 'core' or 'opinion' work product that encompasses the mental impressions, conclusions, opinion, or legal theories of an attorney or other representative of a party concerning the litigation is generally afforded near absolute protection from discovery.") (internal quotation marks omitted); *In re* San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d 1007, 1015 (1st Cir. 1988) ("Courts typically afford ordinary work product only a qualified immunity, subject to a showing of substantial need and hardship, while requiring a hardier showing to justify the production of opinion work product.").

doctrine's exceptions, companies cannot rely on the work product doctrine to prevent the compelled disclosure of cybersecurity material.

C. *Non-Testifying Expert Privilege*

A third, narrower privilege prevents the compelled disclosure of certain non-testifying experts. Federal Rule of Civil Procedure 26(b)(4)(D) states that "a party may not, by interrogatories or depositions, discover facts known or opinions held by an expert retained or specially employed by another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial," unless the party can demonstrate "exceptional circumstances under which it is impracticable for the party to obtain facts or opinions on the same subject by other means."[82] The non-testifying expert privilege is "designed to promote fairness by precluding unreasonable access to an opposing party's diligent trial preparation."[83]

The non-testifying expert privilege is quite strong, and courts have interpreted the "exceptional circumstances" exception to be quite limited.[84] However, it has limited value for cybersecurity investigations. As the Ninth Circuit recently noted, the rule "shields only against disclosure through interrogatories and depositions[.]"[85] Accordingly, the rule would not prevent the disclosure of a report prepared by a cybersecurity expert; it would only prevent that expert from being subjected to interrogatories and depositions. Moreover, like the work-product doctrine, the non-testifying expert privilege only applies to anticipated litigation or trial preparation.[86] A routine cybersecurity investigation, therefore, likely would not be covered under this privilege. This privilege would, however, apply to an incident assessment that a cybersecurity professional prepares to assess the merits of pending litigation.

---

[82] Fed. R. Civ. P. 26(b)(4)(D).

[83] Durflinger v. Artiles, 727 F.2d 888, 891 (10th Cir. 1984).

[84] *In re* Shell Oil Refinery, 132 F.R.D. 437, 442 (E.D. La. 1990) ("The exceptional circumstances requirement has been interpreted by the courts to mean an inability to obtain equivalent information from other sources.").

[85] Ibrahim v. Department of Homeland Sec., 669 F. 3d 983, 999 (9th Cir. 2012).

[86] Fed. R. Civ. P. 26(b)(4)(D).

D. *Genesco v. Visa: Why the Privilege System is Flawed for Cybersecurity*

Few published opinions have directly addressed the application of the attorney-client privilege, work-product doctrine, and non-testifying expert privilege to the work of cybersecurity professionals. This is not surprising; discovery disputes often are settled orally in discussions between the parties and magistrate judges; therefore, there is not a written opinion documenting many of these disputes. The most extensive written discussion of the application of these privileges to cybersecurity was in *Genesco v. Visa*.[87]

In that case, hackers had accessed customer payment card information that was stored on the network of Genesco, a retail chain.[88] Genesco's general counsel, Roger Sisson retained Stroz Friedberg, a cybersecurity consulting firm.[89] Genesco's retention agreement with Stroz stated that the retention was "in anticipation of potential litigation and/or legal or regulatory proceedings."[90]

After consulting its own investigation, Visa assessed more than $13 million in fines and reimbursement assessments against two banks that processed Genesco's credit card purchases, claiming that Genesco's inadequate data security violated payment card data security standards and Visa's operating regulations.[91] Genesco, which had an indemnification agreement with the banks, sued Visa, asserting that the assessments lacked factual basis and violated various state laws.[92] In discovery, Visa subpoenaed Stroz for deposition testimony and its work product related to the investigation, and also requested to depose Sisson and that Sisson provide documents related to his investigation of the incident.[93]

The court largely denied Visa's discovery requests. The court first held that the requests for Stroz's deposition and work product is

---

[87] Genesco v. Visa U.S.A., 302 F.R.D. 168 (M.D. Tenn. 2014).

[88] *Id.* at 171.

[89] *Id.* at 180-81.

[90] *Id.* at 181.

[91] *Id.* at 170.

[92] *Id.*

[93] *Id.* at 181-82.

prohibited by the non-testifying expert privilege.[94] Visa argued that Stroz was a fact witness, but the court rejected this argument, concluding that "the Stroz representative would necessarily be applying his or her specialized knowledge," and that Visa had not established the "extraordinary circumstances" needed to overcome the non-expert witness privilege.[95]

The court also held that the attorney-client privilege and work product doctrine prevent the compelled disclosure of both the requests to Sisson and to Stroz.[96] The court held that "[a]ttorney's factual investigations 'fall comfortably within the protection of the attorney-client privilege,'"[97] and that the privilege "extends to the Stroz firm that assisted counsel in his investigation."[98] The court also recognized that the work product doctrine "attaches to an agent's work under counsel's direction."[99] The court held that the work product doctrine applies because "Genesco's affidavits satisfy that the Stroz firm was retained in contemplation of litigation, as reflected in the express language of the retainer agreement."[100]

In 2015, Visa subpoenaed IBM for work product regarding remedial security measures that IBM performed for Genesco after the breach.[101] In a brief order, the court rejected this request, concluding that because Genesco "retained IBM to provide consulting and technical services so as to assist counsel in rendering legal advice[,]" IBM's materials are protected by the attorney-client privilege and work product doctrine.[102]

---

[94] *Id.* at 189-90.

[95] *Id.* at 190 ("To accept that characterization would effectively eviscerate and undermine the core purpose of Fed. R. Civ. P. 26(b)(4)(D).").

[96] *Id.* at 195.

[97] *Id.* at 190 (quoting Santra T.E. v. South Berwyn School Dist. 100, 600 F.3d 612, 619 (7th Cir. 2010)).

[98] *Id.*

[99] *Id.*

[100] *Id.* at 193.

[101] Genesco, Inc. v. Visa U.S.A., Inc., 2015 U.S. Dist. LEXIS 52314 (M.D. Tenn. March 24, 2015).

[102] *Id.*

Commentators hailed the *Genesco* rulings as a demonstration that cybersecurity work could be privileged, provided that they are conducted under the supervision of an attorney. Lawyers at one large law firm hailed the opinion as "a roadmap for confidentiality protections" that "underscores legal counsel's critical role in today's digital economy where the question is not 'if' but 'when,' an organization will be breached."[103] Lawyers at another firm advised that the decision "demonstrates how important it is for you to designate experienced privacy counsel to lead cybersecurity initiatives, including determining proactive privacy and security measures, directing forensic investigations, and spearheading data breach response efforts."[104] A news article declared that, in light of the opinion, the "smart and most conservative proactive approach" to cybersecurity risk management is "to have the appropriate law firm take the lead, hire the required consultants, and have all reports, analysis, memos, plans and communications protected under the attorney-client and work product privileges."[105]

The commentators were correct, to an extent. The *Genesco* rulings extend the same protections to communications and work product of cybersecurity consultants as previous court opinions have extended to the work and communications of environmental consultants, product safety experts, and others retained and supervised by counsel for the purposes of providing legal advice or preparing for litigation. The 2015 order regarding IBM, in particular, is encouraging because IBM provided technical consulting to help remediate security flaws on Genesco's network. Although the court viewed these services as part of Genesco's legal strategy, remedial measures for a computer network could have longer lasting effects that help Genesco in the future, entirely unrelated to the Visa litigation.

---

[103] Aravind Swaminathan et al., *Court Says Cyber Forensics Covered by Legal Privilege*, ORRICK (Apr. 24, 2015), https://www.orrick.com/Events-and-Publications/Pages/Court-Says-Cyber-Forensics-Covered-by-Legal-Privilege.aspx.

[104] *Communications with your Cybersecurity Consultant and Forensic Reports May Now Be Protected*, MCDONALD HOPKINS (June 11, 2015), http://www.mcdonaldhopkins.com/alerts/data-privacy-and-cybersecurity-communications-with-your-cybersecurity-consultant-and-forensice-reports-may-now-be-protected.

[105] Denis Kleinfeld, *Your Computer Will be Hacked, It's Just a Question of When*, NEWSMAX (May 4, 2015), http://www.newsmax.com/Finance/Kleinfeld/Cybersecurity-Hack-Passcodes-Risk/2015/05/04/id/642323/.

That said, the *Genesco* case also illustrates the evidentiary privileges' limits for cybersecurity work. The gravamen of Genesco's argument throughout the discovery dispute was that Stroz and IBM were merely helping Genesco challenge the Visa fees or prepare for its defense in other claims related to the breach.[106] Genesco framed its arguments as such for good reason: had it not framed the IBM and Stroz work as part of a legal defense strategy, the communications and work product likely would have been discoverable, as reflected in the court's focus on the three attorney-related privileges.

The *Genesco* case reflects the perverse incentive system created by the current evidentiary privilege framework. Assisting attorneys in litigation receives more protection from discovery than developing technical remediation measures that are separate from legal strategies. Had Genesco's Chief Information Officer – rather than its General Counsel – independently retained cybersecurity experts to remediate the security breaches, the communications and work products of those experts likely would have been subject to discovery. Yet it is likely that Genesco's Chief Information Officer has a better understanding of the company's networks and systems, and is therefore more equipped than the General Counsel to oversee cybersecurity consultants who are investigating and remediating security incidents. However, as long as there is not a standalone privilege for cybersecurity work, companies will continue to be forced to delegate the supervision of cybersecurity work to their attorneys.

III. THE CASE FOR A CYBERSECURITY PRIVILEGE

The *Genesco* case illustrates the need for a privilege to directly protect the work product and communications of cybersecurity professionals. Such a privilege would allow companies to more quickly and flexibly respond to suspected cybersecurity threats without being forced to engage in formalistic – and time-consuming – routines to increase the chances of attorney-related privileges applying. A separate privilege for cybersecurity would allow faster responses to data security incidents, and also would provide companies with more certainty that their cybersecurity work will not be discoverable in subsequent litigation.

---

[106] Opp. Brief of Genesco, Genesco, Inc. v. Visa U.S.A., Inc., 2015 U.S. Dist. LEXIS 52314 (M.D. Tenn. March 24, 2015) ("Here, it is undisputed that IBM prepared the PCI Gap Assessment pursuant to an engagement by Genesco's General Counsel for the purpose of assisting Genesco's General Counsel in providing legal advice to Genesco regarding its *legal* obligation to be PCI DSS compliant.").

This section outlines the two avenues for creating a privilege – the common law or statute. I review many of the other evidentiary privileges, and argue that the rationale for creating these privileges applies equally to cybersecurity work and communications.

A. *Common Law Privilege*

Providing a common-law privilege for the work of cybersecurity professionals would be in line with the centuries-old tradition of recognizing a privilege based on public-interest considerations. In its 1934 opinion in *Wolfle v. United States*,[107] the Supreme Court wrote that evidentiary privileges are "governed by common law principles as interpreted and applied by the federal courts in the light of reason and experience."[108]

In 1972, the Chief Justice of the United States, based on recommendations from the Judicial Conference Advisory Committee on Rules of Evidence, attempted to override this flexible common-law approach by proposing nine exclusive, specific evidentiary privileges, such as the spousal testimonial privilege and the psychotherapist-patient privilege.[109] Congress ultimately rejected this proposal, and instead incorporated the *Wolfle* "reason and experience" approach into Federal Rule of Evidence 501. The rule states:

> The common law — as interpreted by United States courts in the light of reason and experience — governs a claim of privilege unless any of the following provides otherwise:
>
> the United States Constitution;
>
> a federal statute; or
>
> rules prescribed by the Supreme Court.

---

[107] *Wolfle*, 291 U.S. 7 (1934).

[108] *Id.* at 12.

[109] Proposed Rules of Evidence for United States Courts and Magistrates Order, 56 F.R.D. 183 (1972); *see* Paul Rothstein, *The Proposed Amendments to the Federal Rules of Evidence*, 62 GEO. L.J. 125, 128 (1973) ("The Rules as approved by the Supreme Court prescribe an exclusive list of carefully defined privileges for all federal court proceedings, civil and criminal, diversity and federal question.").

> But in a civil case, state law governs privilege regarding a claim or defense for which state law supplies the rule of decision.[110]

The Senate Judiciary Committee reasoned that its approach to evidentiary privileges "should be understood as reflecting the view that the recognition of a privilege based on a confidential relationship and other privileges should be determined on a case-by-case basis."[111] As Chief Justice Berger wrote six years later, Congress adopted Federal Rule of Evidence 501 to "leave the door open to change."[112] Federal Rule of Evidence 501 "did not freeze the law governing the privileges of witnesses in federal trials at a particular point in our history, but rather directed federal courts to continue the evolutionary development of testimonial privileges."[113]

In *Jaffee v. Redmond,*[114] in which the defendant in a civil suit successfully defeated the plaintiff's attempt to subpoena notes from her counseling sessions with a licensed clinical social worker, the Supreme Court articulated the analysis that courts employ when determining whether a common-law evidentiary privilege exists. The framework begins with "the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctively exceptional, being so many derogations from a positive general rule."[115] Exceptions to this general rule "may be justified, however, by a public good transcending the normally predominant principle of utilizing all rational means for ascertaining the truth."[116]

---

[110] Fed. R. Evid. 501.

[111] S. Rep. 93-1277 at 13 (1974); *see also* Mila Sohoni, *The Power to Privilege*, 163 U. PENN. L. REV. 487, 494 (2015) ("By thus letting common law decisionmaking by federal courts set the content of federal privilege law, Congress was able to avoid the difficult task of drafting a set of statutory privilege rules that would please the many powerful interest groups with a stake in the shape of federal privilege law.").

[112] Trammel v. United States, 445 U.S. 40, 47 (1980).

[113] Jaffee v. Redmond, 518 U.S. 1, 9 (1996) (internal quotation marks omitted).

[114] *Jaffee*, 518 U.S. 1 (1996).

[115] *Id.* at 9 (quoting United States v. Bryan, 339 U.S. 323, 331 (1950)).

[116] *Jaffee*, 518 U.S. at 9 (citations omitted) (internal quotation marks omitted).

The public good served by both proactive *and* remedial cybersecurity consulting outweighs the standard assumption in support of compelled testimony and document disclosure. As demonstrated in Part I of this Article, cybersecurity vulnerabilities are increasingly placing companies at significant risk of economic harm. Cybersecurity incidents also increasingly lead to identity theft, and can even lead to global political disruptions. Accordingly, there is an overwhelming public interest in creating a policy framework that provides companies with incentives to invest significantly in cybersecurity. Because cybersecurity professionals often uncover vulnerabilities that could be harmful to the companies in subsequent litigation or regulatory investigations, current evidentiary law provides them with a disincentive to engage cybersecurity consultants.

The use of the attorney-client privilege, work product doctrine, and non-testifying expert privilege, described in Part II of this Article, are occasionally effective – but imperfect – attempts to provide this protection. As seen in the *Genesco* case, cybersecurity work is protected only to the extent that it could be associated with legal advice or defense. To be sure, cybersecurity does involve legal considerations; however, cybersecurity should be driven by the ultimate desire to protect a company's networks and systems, and to remediate any damage caused by security incidents. Companies should feel certain that if they engage a cybersecurity consultant, that consultant's work product and communications will be confidential; companies should not feel obligated to limit the cybersecurity consultant's work so that it falls squarely under the attorney-related privileges. Such a legal framework ultimately discourages companies from fully investing in cybersecurity. This result clearly is contrary to the public interest.

The cybersecurity privilege finds support in the two leading jurisprudential theories that underlie privilege law: utilitarian theory and privacy theory.[117]

The utilitarian approach is most commonly associated with the four-prong test articulated by John Henry Wigmore in his treatise, *Wigmore on Evidence*:

---

[117] Daniel Northrop, *The Attorney Client Privilege and Information Disclosed to an Attorney with the Intention that the Attorney Draft a Document to be Released to Third Parties: Public Policy Calls for at Least the Strictest Application of the Attorney-Client Privilege*, 78 FORDHAM L. REV. 1481, 1492-93 (2009) ("Several theories have been proposed to justify the attorney-client privilege. The utilitarian rationale and the privacy rationale are two predominant theories that provide a logical explanation for why the attorney-client privilege should and does exist.").

1. The communications must originate in a confidence that they will not be disclosed;

2. This element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties;

3. This relation must be one which in the opinion of the community ought to be sedulously fostered;

4. The injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of the litigation.[118]

A cybersecurity privilege would satisfy all four requirements of Wigmore's utilitarian test. First, communications between companies and their cybersecurity experts are conducted in confidence; it is difficult to conceive of a company that would share its network vulnerabilities, suspected incidents, defense strategies, and related information unless it was assured confidentiality. Second, that confidentiality is essential to the relationship; without this information, a cybersecurity professional would have difficulty performing basic analysis. Third, the public has great interest in ensuring the security of the networks and systems in which individuals entrust some of their most sensitive information.

The privacy approach to privilege law "emphasizes that human autonomy, respect for relationships, and respect for the bonds and promises that protect shared information are important values that must be protected,"[119] and that compelled disclosure results in "(1) the embarrassment of having secrets revealed and (2) the forced revelation of confidential information."[120] The utilitarian approach, rather than the privacy approach, is more directly applicable to a cybersecurity privilege for corporations. The attorney-client privilege and work product doctrine, for instance, are typically justified for

---

[118] John Henry Wigmore, WIGMORE ON EVIDENCE § 2285 (1961).

[119] Northrop, *supra* note 117 at 1495.

[120] *Id.*

corporations under a utilitarian argument.[121] However, a common-law cybersecurity privilege finds some support in the privacy-based approach to privilege law. Cybersecurity professionals have access to a great deal of consumer personal information, such as customer purchasing data, employee web browsing histories, and, in some cases, employee disciplinary records. Accordingly, there is a great privacy interest in ensuring that the data that cybersecurity professionals access and receive is private.

Opponents of a cybersecurity privilege likely would argue that cybersecurity is a brand-new field that is not deserving of common-law evidentiary protection. To be sure, courts are very reluctant to create new evidentiary privileges, and there is a strong presumption in favor of presenting evidence to a court.[122] However, cybersecurity is not a passing fad. As our personal and professional lives are increasingly tied to the Internet and other computer networks and systems,[123] the concerns about the security of the information described in Part I of this Article will continue. Even if "cybersecurity" becomes replaced with a new term in the next few decades, it is difficult to conceive of a modern world in which courts and policymakers are not concerned about the security of data, systems, and networks. Under Federal Rule of Evidence 501, courts must determine whether the public good served by a cybersecurity privilege outweighs the standard presumption in favor of requiring testimony and evidence in court.

To illustrate why the cybersecurity privilege is justified under the common law, the remainder of this section describes some of the most directly applicable common-law privileges – for psychotherapists,

---

[121] Catherine T. Struve, *Attorney-Client and Work Product Protection in a Utilitarian World: An Argument for Recomparison*, 108 HARV. L. REV. 1697, 1703 (1995). ("Although scholars once used a rights-based analysis to justify the individual's attorney-client privilege, few attempted to do so for corporate clients. Critics of a corporate attorney-client privilege note that corporations have no claim to the personal rights that underpin the attorney-client privilege.").

[122] *See* University of Pennsylvania v. EEOC, 493 US 182, 189 (1990) ("We do not create and apply an evidentiary privilege unless it promotes sufficiently important interests to outweigh the need for probative evidence.") (citations omitted) (internal quotation marks omitted).

[123] Bill Wasik, *In the Programmable World, All of Our Objects Will Act as One*, WIRED (May 14, 2013) ("In our houses, cars, and factories, we're surrounded by tiny, intelligent devices that capture data about how we live and what we do. Now they are beginning to talk to one another. Soon we'll be able to choreograph them to respond to our needs, solve our problems, even save our lives.").

attorneys, and clergy[124] – and explains how the underlying rationale for these privileges applies to cybersecurity work.

1. *Psychotherapist Privilege*

In *Jaffee*, the Supreme Court recognized a common-law privilege for communications between psychotherapists and their patients.[125] The Court held that "confidential communications between a licensed psychotherapist and her patient in the course of diagnosis or treatment are protected from compelled disclosure under Rule 501 of the Federal Rules of Evidence."[126]

The Court recognized the "significant public and private interests" supporting such a privilege.[127] Without a psychotherapist privilege, the Court reasoned, "confidential conversations between psychotherapists and their patients would surely be chilled, particularly when it is obvious that the circumstances that give rise to the need for treatment will probably result in litigation."[128] The "mental health of our citizenry," the Court concluded, "is a public good of transcendent importance."[129]

The Court's reasoning in support of a psychotherapist privilege also counsels in favor of a cybersecurity privilege. In *Jaffee*, the Court's ultimate decision to recognize a privilege was based largely on an assessment of the public good that is served by encouraging confidential communications between patients and psychotherapists. The Court correctly concluded that effective psychotherapy "depends upon an atmosphere of confidence and trust in which the patient is

---

[124] This article does not focus on the spousal testimonial or marital communications common law privileges, see *Trammel v. United States*, 445 U.S. 40 (1980), as those privileges arise from a familial and personal bond that is not analogous to the relationship between a company and a cybersecurity professional. *See* Mikah K. Story, *Twenty-First Century Pillow-Talk: Applicability of the Marital Communications Privilege to Electronic Mail*, 58 S.C. L. REV. 275, 281 (2006) ("[U]nlike the other evidentiary privileges, there is no professional party in the marital relationship who can advise the communicating party of the existence of the privilege.").

[125] *Jaffee*, 518 U.S. at 11.

[126] *Id.* at 15.

[127] *Id.* at 11.

[128] *Id.* at 11-12.

[129] *Id.* at 11.

willing to make a frank and complete disclosure of facts, emotions, memories, and fears."[130] Although cybersecurity consulting is quite different from psychotherapy, both depend on an atmosphere of candor and trust. Cybersecurity professionals must have unfettered access to a company's confidential computer systems, and learn about vulnerabilities that could cause a company to go out of business. Companies and their employees are unlikely to provide cybersecurity professionals with such broad access if there is a chance that the information could later be used against them in court by plaintiffs or regulators.

Like cybersecurity, modern psychotherapy did not exist during the development of the common law. Indeed, in his dissent in *Jaffee*, Justice Scalia noted that "[f]or most of history, men and women have worked out their difficulties by talking to, *inter alios*, parents, siblings, best friends, and bartenders – none of whom was awarded a privilege against testifying in court."[131] Yet the majority in *Jaffee* focused not on the history of the use of psychotherapy. Instead, the Court recognized a privilege after analyzing the *current* public value of ensuring confidentiality during psychotherapy. Likewise, although the term "cybersecurity" did not exist at common law – and was not widely recognized until recent years – courts should evaluate the benefits of providing a privilege based on the *current* public interest in allowing confidentiality for cybersecurity professionals and their clients.

2. *Attorney-Client Privilege and Work Product Doctrine*

The rationale in support of the attorney-client privilege and work product doctrine, discussed above, also supports a stand-alone cybersecurity privilege.

According to Wigmore, the attorney-client privilege dates back to Eighteenth Century England: "In order to promote freedom of consultation of legal advisers by clients, the apprehension of compelled disclosure by the legal advisers must be removed; and hence the law must prohibit such disclosure except on the client's consent."[132] United States courts quickly adopted a strong privilege for attorney-client communications. In 1851, the New York Supreme

---

[130] *Id.* at 10.

[131] *Jaffee*, 518 U.S. at 22 (Scalia, J., dissenting).

[132] Wigmore on Evidence § 2291.

Court recognized the attorney-client privilege, reasoning that "[i]f the facts thus communicated were liable to be extorted from the attorney or counsel, suitors would hesitate to employ them, to the great inconvenience of the court."[133] The United States Supreme Court acknowledged the attorney-client privilege in 1888, when Chief Justice Fuller wrote that the privilege "is founded upon the necessity, in the interest and administration of justice, of the aid of persons having knowledge of the law and skilled in its practice, which assistance can only be safely and readily availed of when free from the consequences or the apprehension of disclosure."[134] The Court has continued to recognize a broad attorney-client privilege. In *Upjohn v. United States*, the Court stated that the privilege's purpose "is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[135]

In short, courts and commentators have focused on the public good that is served by promoting a close and confidential professional relationship between attorneys and their clients.[136] Courts have long recognized that without the privilege, attorneys could not fully meet their obligations to serve their clients. Attorneys might choose to avoid asking certain questions or researching certain aspects of the case; otherwise they could discover information that could later be used against their clients. Likewise, cybersecurity professionals must be able to conduct broad-based inquiries of their clients' systems and information processing practices in order to gain a full understanding of vulnerabilities or a suspected data security event. Discouraging a cybersecurity professional from conducting a comprehensive evaluation surely would not serve the public interest. It likely would lead to continued vulnerabilities.

---

[133] Rochester City Bank v. Suydam, Sage & Co., 5 How. Pr. 254 (N.Y. Sup. Ct. 1851).

[134] Hunt v. Blackburn, 128 U.S. 464, 470 (1888).

[135] *Upjohn*, 449 U.S. at 389 (1981); *see also* Trammel, 445 U.S. at 51 (1980) ("The lawyer-client privilege rests on the need for the advocate and counselor to know all that relates to the client's reasons for seeking representation if the professional mission is to be carried out.").

[136] Charles Fried, *The Lawyer as Friend: The Moral Foundations of the Lawyer-Client Relation*, 85 YALE L.J. 1060, 1073 (1976) ("When I say the lawyer is his client's legal friend, I mean the lawyer makes his client's interests his own insofar as this is necessary to preserve and foster the client's autonomy within the law.").

Likewise, the rationale for the work-product doctrine supports a cybersecurity privilege. In *Hickman*, the Supreme Court observed that, in order to prepare a client's case, an attorney must "assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan his strategy without undue and needless interference."[137] Attorneys' work, the Court wrote, "is reflected, of course, in interviews, statements, memoranda, correspondence, briefs, mental impressions, personal beliefs, and countless other tangible and intangible ways[.]"[138] Allowing opposing counsel to access such work product would result in "[i]nefficiency, unfairness, and sharp practices," and "the interests of the clients and the cause of justice would be poorly served."[139] Cybersecurity professionals, like attorneys, frequently conduct interviews, research facts, and document their thoughts in memoranda and reports. Just as the Court recognized that the work-product doctrine encourages attorneys to produce such sensitive work, a cybersecurity privilege would encourage cybersecurity professionals to produce reports without fear of those materials later being subject to discovery.

3. *Priest-Penitent Privilege*

Although clergy members and cybersecurity professionals play very different roles in society, the fundamental reasons for the priest-penitent privilege also support the creation of a cybersecurity privilege.

The first known United States court opinion to recognize the priest-penitent privilege was the 1813 case, *People v. Phillips*.[140] In that case, the New York Court of General Session refused to require a priest to testify about a congregant's statement in a confessional, holding that protecting communications with clergy is essential for free exercise of religion:

---

[137] *Hickman*, 329 U.S. at 511.

[138] *Id.*

[139] *Id.*

[140] People v. Phillips, N.Y.Ct.Gen.Sess. (1813), as reported in Privileged Communications To Clergymen, 1 Cath. Lawyer 199, 207 (1955).

> The sacraments of a religion are its most important elements. We have but two in the Protestant Church — Baptism and the Lord's Supper — and they are considered the seals of the covenant of grace. Suppose that a decision of this court, or a law of the state should prevent the administration of one or both of these sacraments, would not the constitution be violated, and the freedom of religion be infringed? Every man who hears me will answer in the affirmative. Will not the same result follow, if we deprive the Roman catholic of one of his ordinances? Secrecy is of the essence of penance. The sinner will not confess, nor will the priest receive his confession, if the veil of secrecy is removed: To decide that the minister shall promulgate what he receives in confession, is to declare that there shall be no penance; and this important branch of the Roman Catholic religion would be thus annihilated.[141]

The United States Supreme Court adopted this reasoning, recognizing a broad privilege for communications with clergy.[142] Chief Justice Burger wrote that the priest-penitent privilege is "rooted in the imperative need for confidence and trust" and "recognizes the human need to disclose to a spiritual counselor, in total and absolute confidence, what are believed to be flawed acts or thoughts and to receive priestly consolation and guidance in return."[143] The privilege is absolute and rarely subject to debate.[144]

To be sure, clergy and cybersecurity professionals receive very different types of information. A clergy member may receive an individual's most intimate, personal confessions, while cybersecurity professionals may learn of a company's network vulnerabilities, or incidents that have compromised consumers' personal information but were not required to be reported to regulators or individuals.

---

[141] *Id.*

[142] Totten v. United States, 92 U.S. 105, 107 (1875) ("[S]uits cannot be maintained which would require a disclosure of the confidences of the confessional[.]").

[143] Trammel, 445 U.S. at 51 (1980).

[144] *Developments In The Law — Privileged Communications*, 98 HARV. L. REV. 1450, 1556 (1985) ("Neither scholars nor courts question the legitimacy of the privilege, and attorneys rarely litigate the issue.").

Although the *type* of information is quite different, the need to protect both secrecies can be great. The clergy member may receive information that could upend an individual's personal life or even lead to a criminal conviction. The cybersecurity professional could learn information that could destroy a company's reputation, potentially driving it out of business. Just as Chief Justice Burger recognized that clergy must be able to guarantee "total and absolute confidence,"[145] so too must cybersecurity professionals.

B. *Statutory Privilege*

If courts decline to recognize a common-law privilege for cybersecurity professionals, state legislatures and Congress may ultimately choose to promulgate statutes or evidentiary rules that protect cybersecurity work product and communications.[146]

Among the most analogous statutory privileges is the accountant-client privilege. At the federal level, courts have not recognized a common-law privilege for accountant communications or work product.[147] However, the Internal Revenue Code provides a privilege to "communication between a taxpayer and any federally authorized tax practitioner to the extent the communication would be considered a privileged communication if it were between a taxpayer and an attorney."[148] However, this privilege only applies to noncriminal tax matters before the Internal Revenue Service or in federal court, and only applies to law-related accounting work.[149] Many state

---

[145] *Trammel*, 445 U.S. at 51.

[146] *See* Sohoni, *supra* note 111 at 499 ("Congress does, on occasion, involve itself in expressly articulating rules of privilege and . . . such privileges supplement those developed by the federal courts under Rule 501.").

[147] *See* Couch v. United States, 409 U.S. 322, 335 (1973) ("[W]e note that no confidential accountant-client privilege exists under federal law, and no state-created privilege has been recognized in federal cases[.]).

[148] 26 U.S.C. 7525(a)(1).

[149] *See* United States v. BDO Seidman, 337 F.3d 802 (7th Cir. 2003) ("Thus the § 7525 privilege is no broader than that of the attorney-client privilege, and nothing in § 7525 suggests that nonlawyer practitioners are entitled to privilege when they are doing other than lawyers' work. Because the scope of the tax practitioner-client privilege depends on the scope of the common law protections of confidential attorney-client communications, we must look to the body of common law interpreting the attorney-client privilege to interpret the § 7525 privilege.") (citations omitted) (internal quotation marks omitted).

legislatures have enacted even stronger statutory privileges that prevent accountant work product or communications from being disclosed in state court.[150] Accountants, like cybersecurity professionals, obtain broad access to their clients' information in order to assess potential problems and take the necessary remedial action. The accountant-client privilege serves the public interest by encouraging confidential and open information-sharing between the client and the accountant, and enabling the accountant to provide candid advice based on this information.[151] Accordingly, arguments that have convinced legislators to enact an accountant-client privilege could be equally persuasive for a cybersecurity privilege; in both instances, society as a whole benefits from a statute that promotes a close, trusting relationship between the professional and client.

Similarly, physician-patient privilege statutes have been enacted for many of the same reasons that legislators would enact a cybersecurity privilege. Although federal courts recognize a common-law privilege for communications between psychotherapists and their patients, they do not recognize a similar privilege for communications between physicians and patients.[152] However, most states have

---

[150] *See* Pilar Mata and Melissa J. Smith, *Demystifying Accountant-Client Privileges in State Tax Litigation*, TAX ANALYSTS (Apr. 4, 2012) ("Although Congress created a federal tax practitioner privilege that protects accountants' confidential tax advice when litigating against the Internal Revenue Service, the federal tax practitioner privilege will not protect communications between accountants and their clients when matters are litigated in state courts. It is thus critical for taxpayers to determine the existence and scope of state privileges that can be used to protect state-tax-related communications between taxpayers and their accountants."). *See, e.g.*, Calif. Revenue and Taxation Code 7099.1 ("With respect to tax advice, the protections of confidentiality that apply to a communication between a client and an attorney, as set forth in Article 3 (commencing with Section 950) of Chapter 4 of Division 8 of the Evidence Code, also shall apply to a communication between a taxpayer and any federally authorized tax practitioner to the extent the communication would be considered a privileged communication if it were between a client and an attorney.").

[151] Thomas J. Molony, *Is the Supreme Court Ready to Recognize Another Privilege? An Examination of the Accountant-Client Privilege in the Aftermath of* Jaffee v. Redmond, 55 WASH. & LEE L. REV. 247, 271-72 (1988) ("Perhaps the most compelling argument in favor of the accountant-client privilege is that it will encourage full disclosure and allow public accountants to better serve both their clients and the public. The thrust of this argument is that protection of accountant-client communications promotes an atmosphere of confidence and trust which motivates clients to reveal more information to their accountants. Accountants are then able to evaluate the information to determine if it requires disclosure.").

[152] *See* Whalen v. Roe, 429 U.S. 589, 602 (1977) ("The physician-patient evidentiary privilege is unknown to the common law."); United States v. Bek, 493 F.3d 790 (7th Cir. 2007) ("[W]e can find no circuit authority in support of a physician-patient privilege, even after *Jaffee*.").

enacted statutes that provide a physician-patient privilege.[153] Supporters of the physician-patient privilege argue that "trust is conducive to the patient's seeking and receiving treatment," and therefore "the patient must be assured that his confidences will be kept."[154] Just as the physician is the "trustee by necessity of the patient's secrets,"[155] the cybersecurity professional is entrusted with a company's secrets about its data security and other network and systems vulnerabilities.

Likewise, most states have enacted statutes that provide a qualified privilege that prevents journalists from being compelled to reveal the identities of their confidential sources.[156] Although some jurisdictions provide limited protection to journalists and their sources under the First Amendment or common law, that protection often is weak – or, in some jurisdictions, non-existent.[157] To fill those gaps, state legislatures have passed shield laws that strengthen these protections and provide journalists and their sources with more certainty as to whether the journalist could be subpoenaed to reveal the source's identity in open court.[158] States have enacted shield laws largely in recognition of the unique role that journalists play in

---

[153] *See* Laural C. Alexander, *Should Alabama Adopt a Physician-Patient Evidence Privilege?* 45 ALA. L. REV. 261, 266 (1994).

[154] Daniel W. Shuman, *Origins of the Physician-Patient Privilege and Professional Secret*, 39 S.W. L.J. 661, 682 (1985) ("A disclosure of confidential information would forfeit the patient's confidence in the physician, breach the physician's duty as trustee by necessity, and cause people with embarrassing diseases not to seek treatment.").

[155] *Id.*

[156] For a comprehensive list of state shield laws, see The Reporter's Privilege, Reporters Committee for Freedom of the Press, *available at* www.rcfp.org/reporters-privilege.

[157] *See* Anthony L. Fargo, *Analyzing Federal Shield Law Proposals: What Congress Can Learn from the States*, 11 COMM. L. & POL'Y 35, 39 (2006) ("Over the next thirty-plus years, most of the federal appellate courts at least tacitly supported journalists' rights to refuse to testify or provide other evidence if the information subpoenaed was not highly relevant, critical or unavailable elsewhere. Some federal appellate courts have even extended protection for journalists to include nonconfidential material – such as outtakes, unpublished photographs, and notes – that was not obtained through a promise of confidentiality.").

[158] *Id.* at 49 ("[W]hile a shield law may not be a panacea for problems between the press and the legal system, it can provide relatively consistent treatment within a jurisdiction.").

society, and the important role that confidentiality plays in the journalistic process.[159]

In short, even if courts decline to recognize a cybersecurity evidentiary privilege under federal or state common law, Congress and state legislatures have great discretion to codify a cybersecurity privilege in a statute. Indeed, legislators have a long history of recognizing important public policy reasons in support of the creation of a new privilege. The rapid growth of cybersecurity threats – and the harm that they cause to individuals, companies, and the government – provides legislators with a good reason to consider the creation of a standalone cybersecurity privilege. Such protection would help to build the trust and confidence necessary for cybersecurity professionals to remediate harm and prevent future incidents.

IV. THE CONTOURS OF A CYBERSECURITY PRIVILEGE

If courts or legislators decide to create a cybersecurity privilege, such a privilege should be broad enough to encourage companies to hire cybersecurity consultants both before *and* after data security incidents.

A. *Who is Covered by the Cybersecurity Privilege?*

Among the primary issues that arise with a cybersecurity privilege is how to define the professionals who are covered by the privilege. Unlike attorneys, who are certified by a single, government-authorized bar in each state, cybersecurity does not have a unitary certification. Granted, there are a number of cybersecurity certifications, many of which require rigorous training and examination. Perhaps the best-known certification is the Certified Information Systems Security Professional (CISSP), which requires at least five years of paid, full-

---

[159] *See* Stephanie B. Turner, *Protecting Citizen Journalists: Why Congress Should Adopt a Broad Federal Shield Law*, 30 YALE L. & POL'Y REV. 503, 507 (2012) ("Lawmakers generally cite two related rationales for enacting a reporter's privilege. First, without the privilege, journalists would write with a more restrained pen, and fear of exposure would cause dissidents to communicate less openly to trusted reporters. By encouraging sources to give and journalists to disseminate information freely, the privilege encourages the free flow of information to the public and ensures a robust marketplace of ideas. Second, without the privilege, journalists would be reduced to an investigative arm of the government. By allowing journalists to operate independently, the privilege creates a fourth institution outside the Government as an additional check on the three official branches.") (citations omitted) (internal quotation marks omitted).

time work experience in two or more of eight cybersecurity domains, and passage of a six-hour exam.[160] They also must meet certain criminal history requirements and enroll in continuing education.[161]

At first glance, it appears reasonable to apply a cybersecurity privilege only to CISSP holders. However, CISSP is not the only credential that is valuable for cybersecurity professionals.[162] For instance, the International Association of Privacy Professionals offers privacy-focused credentials including the Certified Information Privacy Professional ("CIPP"),[163] Certified Information Privacy Manager ("CIPM"),[164] and Certified Information Privacy Technologist ("CIPT").[165] ISACA offers the Certified Information Systems Auditor ("CISA") credential, which focuses on systems audit, control, and security.[166] And the EC-Council offers the Certified Ethical Hacker ("CEH") credential.[167] Moreover, many technology vendors, such as Cisco, offer vendor-specific security certifications.[168]

---

[160] *See How to Get Your CISSP Certification*, (ISC)², https://www.isc2.org/cissp-how-to-certify.aspx (last visited Mar. 8, 2016).

[161] *See* Woody Leonhard, *Is CISSP Certification Worth the Effort*, INFOWORLD (Aug. 1, 2012).

[162] *See id.* ("While CISSP is considered by many to be the premiere certification in the field, it's by no means the only one, and there's no rule that says you can hold only one.").

[163] *See* Certification Programs, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/certify/programs (last visited Mar. 8, 2016) ("The CIPP shows that you understand the laws, regulations and standards of privacy in your jurisdiction or discipline.").

[164] *See id.* ("The CIPM says that you understand how to use process and technology to manage privacy in an organization—regardless of the industry or jurisdiction.").

[165] *See id.* ("The CIPT shows that you know how to manage and build privacy requirements and controls into technology.").

[166] *How to Become CISA Certified*, ISACA, http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/How-to-Become-Certified/Pages/default.aspx (last visited Mar. 8, 2016).

[167] *CEH: Certified Ethical Hacking*, EC COUNCIL, http://www.eccouncil.org/Certification/certified-ethical-hacker ("The definition of an Ethical Hacker is very similar to a Penetration Tester. The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a Hacker.").

[168] *See* Carolyn Duffy Marsan, *How to Land a Cybersecurity Job*, NETWORK WORLD (May 3, 2012) ("Vendor-specific certifications from Cisco, RSA, Symantec and others are also in demand.").

All of these credentials have some value for cybersecurity. A CISSP could provide expeditious incident response after a data breach. A CIPP or CIPM could help set cybersecurity policies. A CISA could conduct routine cybersecurity audits. And a CEH could creatively determine a system's vulnerabilities. Moreover, a certification alone may not be sufficient to prepare an individual to provide cybersecurity services.[169] Limiting the cybersecurity privilege to one or some of these certifications could both exclude some professionals who provide cybersecurity services while unnecessarily *including* people who have certifications but do not provide relevant cybersecurity services.

Rather than focusing on credentials, as with the attorney-client privilege, the cybersecurity privilege should be functional. The privilege should apply to the work product and communications of professionals engaged in the protection of communications systems and networks, and the information contained therein. Such a functional definition would broadly encompass the work and communications of cybersecurity professionals. At the same time, the privilege would exclude the non-cybersecurity work of professionals who also happen to perform cybersecurity-related functions. For instance, assume an auditing firm conducts both a cybersecurity and financial audit of a corporate client. Under my proposed privilege, only the firm's cybersecurity-related audit work would be protected from discovery.

Courts have long taken a functional approach to evidentiary privileges. For instance, a common debate about shield laws and privileges for journalism focuses on the definition of "journalist."[170] Federal courts have long determined that the privilege applies to journalists who "obtained the information in the course of gathering news for publication."[171] State shield laws also apply broadly to journalists, but only in their capacity gathering information for

---

[169] *See* Amber Corrin, *Is Cybersecurity the Right Job for You*, FCW (Jan. 23, 2014) ("It's not something you can just get a certificate for and check that box on your resume.").

[170] Stephen Bates, *The Reporter's Privilege, Then and Now*, HARV. KENNEDY SCHOOL (Jan. 1, 2000), *available at* http://shorensteincenter.org/wp-content/uploads/2012/03/r23_bates.pdf ("The law has no trouble deciding who is an attorney or a doctor. Defining a journalist is dicier. Courts and legislatures have had to decide whether the privilege extends to freelancers, magazine reporters, book authors, pamphleteers, Internet journalists, and scholars.").

[171] Von Bulow by Auersperg v. Von Bulow, 811 F. 2d 136, 144 (2d Cir. 1987).

publication.[172] Likewise, the cybersecurity privilege should focus on the *task* being performed by the professional, rather than the professional's certification, education, job title, or other formal qualifications.

Indeed, the Supreme Court embraced such a functional approach in *Jaffee*, which involved communications with a social worker. The Court declined to limit the psychotherapist privilege to licensed psychiatrists and psychologists, concluding that the "reasons for recognizing a privilege for treatment by psychiatrists and psychologists apply with equal force to treatment by a clinical social worker."[173] The Court extended the privilege to a clinical social worker because she provided psychotherapy services. Similarly, a consultant or other professional should be subject to the cybersecurity privilege based on the nature of the services provided to the client.

B. *What is Covered by the Cybersecurity Privilege?*

I propose that, subject to narrow exceptions, the cybersecurity privilege provide absolute protection to *both* the communications and work product of cybersecurity professionals. Only broad protection would provide the necessary assurance to encourage companies to allow cybersecurity professionals to access and evaluate their systems and networks.

A privilege may either be absolute or qualified. A qualified privilege is triggered only after a court conducts a balancing test and determines that application of the privilege in that instance is in the public interest and outweighs the need for the evidence.[174] A qualified

---

[172] *See, e.g.,* Cal. Evid. Code § 1070(a) ("A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or by a press association or wire service, or any person who has been so connected or employed, cannot be adjudged in contempt by a judicial, legislative, administrative body, or any other body having the power to issue subpoenas, for refusing to disclose, in any proceeding as defined in Section 901, *the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication*, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public.") (emphasis added).

[173] *Jaffee*, 518 U.S. at 15.

[174] Eileen A. Scallen, *Relational and Informational Privileges and the Case of the Mysterious Mediation Privilege*, 38 LOY. L.A. L. REV. 537, 548 (2004). ("Moreover, the protection is qualified, and if there is, among other factors, a sufficient showing of relevance, need for information, or seriousness of the issues involved, the trial judge may order the production of the information.").

privilege does not provide the necessary assurances to encourage companies to hire cybersecurity consultants. For instance, in *Upjohn*, the Supreme Court rejected a lower court's qualified attorney-client privilege, concluding that only an absolute privilege provides the necessary confidentiality guarantees to clients and attorneys.[175] Likewise, the Court declined to adopt a qualified psychotherapist privilege, concluding that "[m]aking the promise of confidentiality contingent upon a trial judge's later evaluation of the relative importance of the patient's interest in privacy and the evidentiary need for disclosure would eviscerate the effectiveness of the privilege."[176]

I propose that cybersecurity professionals' work product – and not just their communications – be covered by an absolute privilege. Granted, the attorney work-product doctrine is a qualified privilege that can be overcome by a showing of need or hardship.[177] However, the work product of cybersecurity professionals differs from that of attorneys. Cybersecurity professionals often are hired to *uncover* vulnerabilities in a company's computer systems and networks. Their work may be entirely unrelated to pending or ongoing litigation. The end goal of a cybersecurity professional is not only to reduce a company's legal liability (though that is part of the goal); it is to protect the confidentiality, integrity, and availability of its client's computers, systems, networks, and information. In turn, part of the cybersecurity professional's goals is to protect the information of the company's consumers, employees, and others. Unlike an attorney, whose allegiance is clearly to the client, the cybersecurity professional's goals are much broader. There is a strong public interest in encouraging companies to hire cybersecurity professionals to engage in this work.

Of course, the cybersecurity privilege should not be a means to allow companies to conduct illegal activities, such as violating computer hacking laws.[178] Accordingly, I propose that, as with the

---

[175] Upjohn, 449 U.S. at 393 ("[I]f the purpose of the attorney-client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all.").

[176] Jaffee, 518 U.S. at 17-18.

[177] *See* Section II.B, *supra*.

[178] *See* 18 U.S.C. § 1030 (criminalizing the intentional access of computers without authorization or in excess of authorization).

attorney-client privilege,[179] the cybersecurity privilege should not protect communications or work product that are used to commit or further crime or fraud. If a cybersecurity professional helps a client "hack back" at an attacker, in violation of federal or state anti-hacking laws, the cybersecurity privilege should not prevent the cybersecurity professional's work product or communications from being discovered in court.

Moreover, it may very well be that an absolute privilege – at least initially – is not feasible due to resistance from courts or legislators. In that case, a qualified privilege would be an acceptable starting point. Although it would not provide the same broad range of protections as an absolute privilege, it would help to encourage companies to invest in cybersecurity work and increase the likelihood that the cybersecurity professionals' work product would be protected from discovery.

CONCLUSION

As cybersecurity has emerged as a vital and necessary service, companies have struggled to figure out how to prevent the work of cybersecurity professionals from being subject to discovery. The makeshift solution has been to create the illusion that cybersecurity work is done at the direction of attorneys, and therefore is subject to attorney-client privilege and the work product doctrine. This solution is inefficient, as it requires attorneys to be the middleman between companies and cybersecurity professionals. The solution also is illusory: it requires attorneys with little technical expertise to "supervise" the work of experienced cybersecurity professionals.

The cybersecurity privilege provides a more logical and efficient solution. And it is a solution that is grounded in strong public policy. Just as courts and legislatures have recognized privileges for attorneys, accountants, priests, and journalists, they have good reason to provide evidentiary protection that promotes the use of cybersecurity professionals. A cybersecurity privilege would allow companies to invest in cybersecurity without fear that the investments would lead to evidence that would later be used against them in court.

---

[179] United States v. Zolin, 491 US 554, 563 (1989) ("It is the purpose of the crime-fraud exception to the attorney-client privilege to assure that the seal of secrecy between lawyer and client does not extend to communications made for the purpose of getting advice for the commission of a fraud or crime.") (citations omitted) (internal quotation marks omitted).