Focusing on the primary purpose: Protecting the attorney–client privilege and work product doctrine in incident response

Received (in revised form): 29th December, 2021

Ashley Taylor
Partner, Troutman Pepper, USA

Ashley L. Taylor, Jr. is a Partner at Troutman Pepper who focuses his practice on federal and state government regulatory and enforcement matters involving state Attorneys General, the Consumer Financial Protection Bureau and the Federal Trade Commission. Ashley has in-depth experience handling consumer protection issues and defends companies against a variety of enforcement actions brought by state and federal regulators, and in claims including marketing and advertising representations, statutory disclosures, unfair or deceptive acts or practices and data security breach response.

Troutman Pepper, 1001 Haxall Point, 15th Floor, Richmond, VA 23219, USA
Tel: +1 804-697-1286; E-mail: Ashley.taylor@troutman.com

Ron Raether
Partner, Troutman Pepper, USA

Ron Raether leads the Cybersecurity, Information Governance and Privacy group and is a Partner in the Consumer Financial Services practice group at Troutman Pepper. Ron is known as the interpreter between businesses and information technology and has assisted companies in navigating federal and state privacy laws for over 20 years. Ron's understanding of technology leads him to be involved in legal issues that cross normal law firm boundaries, including experience with data security, data privacy, patent, antitrust, and licensing and contracts. This experience allows Ron to bring a fresh and creative perspective to data compliance issues with the knowledge and historical perspective of an industry veteran.

Troutman Pepper, 5 Park Plaza, Suite 1400, Irvine, CA 92614, USA
Tel: +1 949-622-2722; E-mail: ron.raether@troutman.com

Sadia Mirza
Associate, Troutman Pepper, USA

Sadia Mirza is a member of the Cybersecurity, Information Governance, and Privacy team at Troutman Pepper and dedicates her practice to counselling clients on cutting-edge privacy and cyber security issues. Clients turn to her for compliance counselling, pre-incident response planning and preparedness, and also call her when the first sign of a security incident/data breach appears. Given her years of experience coaching clients through security incidents, Sadia is heavily involved with data breach regulatory and litigation matters, which gives her a 360-view and understanding of the issues most important and relevant to her clients.

Troutman Pepper, 5 Park Plaza, Suite 1400, Irvine, CA 92614, USA
Tel: +1 949-622-2786; E-mail: sadia.mirza@troutman.com

Sam Hatcher
Associate, Troutman Pepper, USA

Sam Hatcher is an Associate in Troutman Pepper's Business Litigation practice. He completed his Juris Doctor cum laude from University of Georgia School of Law, where he served as senior articles editor for the *Georgia Journal of International and Comparative Law*. Sam also competed in the Philip C. Jessup International Law Moot Court Competition and was a member of the E. Wycliffe Orr Inn of Court.

Troutman Pepper, 600 Peachtree Street, N.E., Suite 3000, Atlanta, GA 30308, USA
Tel: +1 404-885-3025; E-mail: sam.hatcher@troutman.com

Bonnie Gill
Associate, Troutman Pepper, USA

Bonnie Gill is an Associate in Troutman Pepper's White Collar and Government Investigations practice. She represents clients facing state and federal regulatory investigations and enforcement actions, as well as related civil litigation. She also advises clients on internal investigations and corporate compliance.

Troutman Pepper, 1001 Haxall Point, 15th Floor, Richmond, VA 23219, USA
Tel: +1 804-697-1210; E-mail: bonnie.gill@troutman.com

Abstract Organisations responding to cyber security incidents must manage their incident response efforts while maintaining two critical legal protections: the attorney–client privilege and the work product doctrine. This paper analyses how the attorney–client privilege and the work product doctrine, when properly maintained, prevent information regarding an organisation's thoughts and discussions from being disclosed or used in subsequent proceedings. It discusses how recent judicial decisions analysing the application of these two doctrines have emphasised the importance of seemingly minor details that may be overlooked during incident response efforts that can have significant consequences in subsequent legal actions when asserting protections. In particular, courts will focus on the stated purpose for any step in the incident response process (eg business versus legal), and any discrepancies between the stated purpose and conduct can have disastrous effects on future claims of protection in legal proceedings. This paper puts forward that organisations should craft incident response plans with the maintenance of these protections in mind. Practical steps organisations can take include carefully scrutinising the language in retainer agreements, involving in-house or outside counsel at the earliest opportunity, limiting the disclosure of privileged materials, and exercising caution when documenting during incident response. After-the-fact attempts to shield the results of any investigation from opposing parties in litigation are rarely successful, so organisations should take affirmative steps to ensure the vitality of these two critical legal protections from the earliest stages of incident response, which start with the planning and preparation.

KEYWORDS: attorney–client privilege, work product doctrine, privacy, disclosure, incident response, protection

INTRODUCTION

'In anticipation of litigation' — a phrase of only four words — is a term of art that can have pivotal consequences for companies dealing with overlapping investigations and potential litigation actions. The phrase is not only meaningful in its own right, but in the cyber security field it is also emblematic

of a growing trend. Minute details that can get lost in the chaotic shuffle following a cyber security incident can re-emerge years later to have profound effects. A few words in a retainer agreement can factor into whether investigatory findings can be limited to internal consideration — and thus shielded from being used against the target by opponents in the courtroom — and permitting candid conversations without fear that third parties will second-guess every choice or word used as parties work to defend against criminal hackers.

During a cyber security incident, companies must handle internal and external pressure to quickly answer fundamental questions, such as how the attack happened, is the incident contained, what information was affected and is notice required? While breach notification laws are structured to allow companies a reasonable time to investigate the incident, businesses often want to inform external parties of the incident immediately, without fully knowing what is at stake. This desire increases when the incident is detected by a third party (as opposed to the company itself), and the media and customers are already aware that an event occurred or is taking place.

These necessities often result in a perceived need for instant action and external communication. But this understandable need to move quickly can obfuscate and often conflict with critical, long-term considerations. One of these long-term concerns is protection of the attorney–client privilege and the work product doctrine. The pitfalls of failing to consider these protections can be drastic, but they are often slow to emerge, sometimes taking years to fully develop. By the time it is apparent that steps were not taken to preserve protections, it is often far too late to rectify the situation.

In most courts, whether protections apply depends on the court's assessment of the 'primary purpose' of the investigation.[1] For example, is the primary purpose to determine whether a threat is active, which may not be considered legal advice, or is the purpose to determine the root cause of the incident to assist counsel in defending against legal claims? In incident response, the practical reality is that an investigation may have overlapping purposes, but only an investigation with a predominantly legal purpose will receive protections. Companies affected by cyber security incidents, however, can take steps to shape how a court will assess the primary purpose of its incident response (IR) efforts, and companies should be mindful that preserving the vitality of these protections starts even before the incident occurs.

AN OVERVIEW OF THE ATTORNEY–CLIENT PRIVILEGE AND THE WORK PRODUCT DOCTRINE

The attorney–client privilege and the work product doctrine are two related but distinct doctrines to protect information that is shared with legal counsel from future disclosure. The attorney–client privilege protects communications to and from one's attorney(s) (and their delegates) *for the purpose of seeking legal advice*, while the work product doctrine protects materials prepared by an attorney — or the agents of an attorney — *in anticipation of litigation*. In the context of cyber security investigations, these two protections often overlap. Some people tend to group them together and treat them interchangeably, but the distinct purposes, origins and tests for these two protections inform the unique methods that must be employed to assert them during the life of cyber investigations and any subsequent litigation.

Attorney–client privilege

'The attorney–client privilege is the oldest of the privileges from confidential communication known to the common law.'[2] The privilege protects communications made to one's attorney *for the purpose of*

seeking or obtaining legal advice, but it does not automatically attach to every communication between an attorney and a client. The Supreme Court noted the limitations of the privilege in *Fisher v. United States*:

> '[S]ince the privilege has the effect of withholding relevant information from the factfinder, it applies only where necessary to achieve its purpose. Accordingly[,] it protects only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege.'[3]

To determine whether the attorney–client privilege applies to a given communication, courts will examine the motivation and purpose underlying the communication. In practical terms, however, courts will look beyond the confines of a single communication and examine the predominant purpose of the relationship that led to the communication.[4] Communications — even those to an attorney — that take place in the context of seeking business or technical advice likely will not fall under the privilege's protections, even if potential legal implications are discussed. And documents are not privileged merely because they are transmitted to an attorney. If that were the case, companies could withhold communications on the basis of attorney–client privilege simply by including their attorney on the communication.[5]

Work product doctrine

While the attorney–client privilege protects communications between a client and its attorneys, the work product doctrine protects documents produced by an attorney in preparation for litigation.

> 'At its core, the work product doctrine shelters the mental processes of the attorney, providing a privileged area within which the attorney can analyse and prepare his client's case.'[6]

The doctrine protects not just materials prepared by the attorney, but those prepared by 'investigators and other agents' for the attorney's use.[7] This may include the attorney's notes, research files, or other information collected or prepared in anticipation of litigation.

The phrase 'in anticipation of litigation' is the critical determinant of whether the work product doctrine protects information developed.[8] This is effectively a 'because of' test. The doctrine only protects documents or information that would not have been developed but for the good-faith belief that it was necessary to do so because of pending or threatened litigation.[9] This inquiry has objective and subjective elements. Objectively, the party asserting the doctrine's protection must demonstrate that it had a reasonable belief a specific litigation threat existed. A general fear of litigation, not tied to a specific claim, is not enough.[10] But litigation need not be ongoing at the time of a document's creation for it to be made 'because of' litigation. For instance, while a government investigation itself is not litigation, courts have generally found that a government investigation gives a company a reasonable basis to anticipate litigation. Subpoenas, requests for mediation, or even the nature and severity of the incident itself can all create a reasonable basis to anticipate litigation.[11] Courts will also examine a company's efforts to preserve potentially relevant documents — a duty also triggered by a reasonable anticipation of litigation — as evidence of whether a reasonable basis to anticipate litigation existed for work product purposes.[12] A company that plans to rely on work product protections for elements of its IR plan should plan to issue litigation holds simultaneously, both to comply with the duty to preserve evidence and to reinforce the existence of a reasonable basis to anticipate litigation.

Subjectively, the anticipated litigation must motivate the production of the document or information. Even with a reasonable and

specific threat of litigation, a document that would have been prepared regardless of the threatened litigation will not receive work product protections.[13] Investigations conducted pursuant to regulatory requirement or internal policy are not created 'because of' litigation, even where litigation is anticipated. The party asserting work product protection over a particular document has the burden of showing that the protection applies, including demonstrating that the material was prepared in anticipation of litigation.[14]

The attorney–client privilege and the work product doctrine are valuable tools that can protect information which, if shared, may be harmful to a company's defence should a regulatory investigation or lawsuit ensue. In practice, courts examine similar factors in applying both the attorney–client privilege and the work product doctrine. The focus is always on the primary purpose and motive of the communication. If the court finds that the primary purpose is driven from a legal necessity (as opposed to a business need), it is more likely to find the material to be protected.

BOLSTERING AN ARGUMENT THAT PROTECTIONS APPLY

Recent judicial decisions have reaffirmed that establishing protections involves a highly fact-sensitive inquiry. What is clear, however, is that whether a document or communication can be shielded from prying eyes depends on its purpose, and whether the actions that follow align with the declared purpose. While seemingly straightforward, the practical reality is that actions taken as part of incident response efforts often serve dual purposes (eg a business purpose and a legal purpose). Consider, for example, an organisation's need to identify potentially affected data following an incident. From a business perspective, this information may be needed to fix corrupted or altered data to support product functionality. From a legal perspective, this same information is needed as it informs an organisation's legal notice requirements. But only this latter (legal) purpose stands a chance of being protected by the attorney–client privilege. Similarly, an estimate of the number of affected users serves a business purpose to help craft a public relations strategy. Counsel may also request a similar estimate to predict the size of a class action lawsuit after litigation is threatened. But only documents created because of the threatened litigation will receive work product protection. Whether determining the primary purpose of a communication or if a document was created because of a litigation threat, courts will examine the stated purpose, conduct and result of any action to determine whether they align with the claimed protections.

No fixed formula will ensure protections apply. Rather, following proper procedure provides the best shot to establish the attorney–client privilege and work product doctrine, but companies would be wise to proceed with caution. Indeed, courts appear to be ruling, more often than not, that responding to an incident is primarily a business function. Despite this trend, some organisations have been successful in shielding IR documents. Drawing from these examples, the following are a few steps businesses can take to bolster an argument that protections apply.

At the first sign of an incident: Engage in-house counsel

Not all cyber security incidents require the same response or lead to the same outcomes. And of course, not all cyber security incidents will result in litigation. Businesses and incident response teams, however, have not historically been good at discerning which incidents will result in litigation and/or investigation, thus often resulting in organisations skipping steps that are critical to preserve protections. Thus, at the first sign of an incident, organisations

should engage in-house counsel immediately for two critical reasons. First, by involving in-house counsel, companies may be able to demonstrate that their IR efforts were driven from a legal necessity (eg a belief that litigation is reasonably anticipated and thus counsel should be involved). Secondly, in-house counsel may be in a better position to assess whether retaining outside counsel is necessary after assessing the potential magnitude and impact of the incident. Factors the legal team may take into consideration when determining an appropriate response to an incident and potential outcome include the number of consumers/customers affected, types of data at issue (eg personally identifiable information and protected health information), the likelihood of harm to individuals, type of intrusion, the privacy and data security laws/contractual obligations applicable to the organisation, and the amount of media attention the incident is receiving.

Of course, not every incident will warrant bringing in outside counsel. The in-house legal team, or counsel serving this function, however, is likely in the best position to make this determination. For organisations that do not have an in-house counsel legal team, or someone experienced to conduct this evaluation, it would be wise to have a plan in place to ensure this step is not overlooked. One option is to obtain cyber insurance so that in the event of an incident, the carrier can connect the company with counsel experienced in this area of the law.

When the situation warrants it: Hire outside counsel

Reliance on in-house counsel in the place of outside counsel in the context of IR can be dangerous. Indeed, in-house counsel often perform both legal and business functions, and a company that does not engage outside counsel during IR efforts may face difficulty establishing that their efforts stemmed from a predominantly legal purpose. If in-house counsel is providing advice that is not strictly legal in nature, or if in-house counsel serves multiple roles (which is often the case), the risks increase. Thus, the hiring of outside counsel is a factor courts take into consideration when assessing whether attorney–client privilege (and especially the work product doctrine) applies. Once outside counsel is retained, let outside counsel direct and supervise the incident response, including the hiring of any third-party firms that may be involved in the response (eg forensic companies, data mining vendors, etc.). With outside counsel in charge, companies will be in a better position to argue that their IR documents and communications stemmed from a legal need.

Pay close attention to language in existing retainer agreements and new statements of work

During incident response, relying on forensic companies that are on retainer to provide cyber security services to the company in its ordinary course of business has proven to be dangerous from the privilege perspective. While a company may have valid reasons to use a company already on retainer (eg the company is already familiar with the company's systems and environment; less contract negotiation during an incident), companies and outside counsel must take caution when taking this route. Courts often take the view that companies on retainer are providing services for a primary business purpose, as opposed to a legal need. Paying attention to the language used in a statement of work specific to a particular incident is critical, especially when an existing contract is in place. Among other things, the statement of work should: 1) clearly define the legal advice sought; 3) designate outside counsel as the one directing and supervising the investigation; and 3) make clear that all written reports and communications should

flow through counsel. Within the company itself, it will also be helpful to designate any forensic investigation expenses as legal expenses, as opposed to flowing through a business function, such as IT.

For example, in litigation following the 2015 Premera Blue Cross (Premera) cyber security incident, the District of Oregon closely scrutinised the wording of retainer agreements and statements of work to discern the purpose of the investigation undertaken by a forensic incident response company.[15] The court ultimately found that the results of the investigation were not protected by the attorney–client privilege or the work product doctrine, and relied on particular wording in the agreements to reach this conclusion.

Premera hired Mandiant in October 2014 to conduct routine reviews of its data management system.[16] On 20th February, 2015, Premera hired outside counsel in anticipation of litigation following the discovery of a cyber intrusion. The next day, Premera and Mandiant entered a revised statement of work that gave Premera's outside counsel supervisory authority over Mandiant's investigation.[17] The new statement did not otherwise change Mandiant's scope of work from the October 2014 statement, however.[18]

When the plaintiffs suing Premera sought to compel the disclosure of Mandiant's report, Premera argued that the report was protected by the attorney–client privilege and the work product doctrine. The court disagreed, noting that 'the only thing that changed' with respect to Mandiant's work was that 'Mandiant was now directed to report directly to outside counsel and to label all of Mandiant's communications as "privileged", "work-product", or "at the request of counsel"'. Because Premera could not show that 'Mandiant changed the nature of its investigation at the instruction of outside counsel and that Mandiant's scope of work and purpose became different in anticipation of litigation' versus the previous business purpose for its work, Premera could not demonstrate a predominantly legal purpose for the investigation.[19] Premera's failure to define a clear and distinct legal purpose in Mandiant's scope of work following the incident proved fatal to Premera's privilege and work product arguments, despite the fact that outside counsel assumed supervisory authority over Mandiant following the cyber security incident. Similarly, in litigation surrounding Rutter Inc.'s (Rutter's) data breach, the court forced the company to produce an investigative report prepared by Kroll Cybersecurity, LLC (Kroll) to plaintiffs.[20] Rutter's hired outside counsel the day of the suspected incident, and outside counsel hired Kroll.[21] But while outside counsel hired Kroll, Rutter's paid Kroll directly, and Rutter's personnel regularly communicated directly with Kroll.[22] Kroll's retention agreement also stated that it would 'work alongside Rutter's IT personnel to identify and remediate potential vulnerabilities' to determine 'whether unauthorised activity within the Rutter's systems environment resulted in the compromise of sensitive data'.[23] The court concluded that the purpose of the investigation was not to determine the proper legal response to the cyber security incident, but rather to determine if there had been a cyber security incident. Despite understanding between Rutter's and outside counsel that the investigation would be privileged, the judge was not convinced that the subsequent conduct demonstrated that intended purpose.

The foregoing cases demonstrate the importance of demonstrating to a court that legal advice was the predominate purpose, including paying close attention to the language used in contracts with forensic companies. Although not ideal from a business perspective, companies may be in a better position to argue IR-efforts are protected by using a third-party forensic company that does not have a previous relationship with the company. If the company wants to use a forensic company

already familiar with the company's environment, outside counsel should carefully review existing contracts and take steps to include language in the new statement of work that clearly demonstrates how the new services differ from what was provided for in the past. Further, the statement of work must show that outside counsel is supervising the work, interacting directly with the vendor and providing instruction and direction. In a close call on predominate purpose, these actions will make it easier for a court to find that the effort was protected by privilege.

Protections can be waived: Take caution when distributing or relying on privileged materials

Companies also need to be careful not to inadvertently waive the attorney–client privilege. 'As a general rule, the attorney–client privilege is waived by voluntary disclosure of private communications by an individual or corporation to third parties.' For example, if the target of a cyber incident e-mails in-house counsel about preliminary investigation results, but then subsequently forwards those results to an unrelated third party (eg law enforcement), the privilege over the results is likely waived.

This rule has exceptions, however. Parties may 'share privileged materials with one another to more effectively prosecute or defend their claims' where the parties' 'legal interests coincide'. But these exceptions — like the privilege itself — are complicated, and subject to often strict interpretations. Particularly applicable in the incident response, a common interest in understanding factually what happened does not mean that parties share a common legal interest in the resolution of any claims. An agreement to share investigation results or conduct a joint inquiry is not an agreement to pursue a joint legal strategy. Privileged information shared under such an arrangement is subject to waiver of the attorney–client privilege. Put simply, for any protection to survive disclosure to a third party, there must be a clearly defined joint legal purpose before the disclosure. Attempts to define a common legal purpose after the fact are rarely successful.

Less stringent rules on disclosure apply to attorney work product than attorney–client privileged communications. Unlike privileged communications, work product can be shared outside the attorney–client relationship without necessarily resulting in a waiver of the doctrine's protection. But the use of documents protected by the work product doctrine for non-litigation purposes — such as diagnosing security weaknesses or evaluating the extent of a cyber security incident for business purposes — may lead a court to conclude that the document in question was not created 'because of' pending or threatened litigation. As a practical reality, companies should avoid the disclosure of work product protected documents to persons not necessary for litigation purposes (eg broader incident response team, law enforcement, other employees, etc.) to avoid the risk of losing the doctrine's protections.

Dual-track investigation

Privilege and work product doctrine claims are often challenged based on arguments that IR reports/materials were prepared for business purposes, as opposed to for obtaining legal advice or in anticipation of litigation. Some organisations have been successful in establishing protections by setting up dual-track investigations with separate teams, where one team investigates in the ordinary course of business (a non-privileged investigation) and the other team conducts a privileged investigation aimed towards providing the organisation with legal advice. When following this approach, companies should gather sufficient documentation to evidence that two separate investigations have been set up and maintain a clear demarcation of roles and

workflow. Companies should also consider the consequences of relying on material they are claiming privilege or work product over for other non-legal purposes (eg responding to regulators, improving the IR function, general cyber security improvements). From a forensic report perspective, any information that would likely only serve a business function (eg general recommendations on how to improve a company's information security programme) should be omitted from privileged reports, as that may blur the lines as to the purpose of the investigation.

In *Wengui v. Clark Hill, PLC*, for example, the District Court for the District of Columbia found that Clark Hill had waived the protections of the attorney–client privilege and the work product doctrine, despite setting up clearly separated investigations for litigation and non-litigation purposes.[24] Following a cyberattack resulting in a breach of client information, Clark Hill engaged outside counsel to manage potential litigation while also mounting a separate forensic investigation to determine the extent and origins of the breach. Immediately following the breach, Clark Hill engaged outside counsel, while also hiring a separate company — eSentire — to conduct an internal investigation into the breach. The outside law company in turn hired its own forensic investigators, Duff & Phelps, to investigate the breach to develop information for future litigation. When the plaintiff moved to compel Clark Hill to produce the Duff & Phelps report, Clark Hill argued that the report was protected because it was created in anticipation of litigation. Clark Hill pointed to the separate eSentire investigation as the investigation being performed for business continuity reasons.[25]

But Clark Hill's argument was unpersuasive. The court found the Duff & Phelps report — ostensibly created purely for litigation purposes — was 'shared not just with outside and in-house counsel, but also with "select members of Clark Hill's leadership and IT team"'.[26] The court found that 'the fact that the report was used for a range of non-litigation purposes reinforces the notion that it cannot be fairly described as prepared in anticipation of litigation'.[27] Clark Hill also argued the report was protected by the attorney–client privilege, but this too was rejected: '[T]he Court concludes that Clark Hill's true objective was gleaning Duff & Phelps's expertise in cybersecurity, not in "obtaining *legal* advice *from its lawyer*".'[28]

Put simply, Clark Hill's actions did not match the stated intent of the investigation. Clark Hill, with the assistance of counsel, articulated a clear legal purpose for the Duff & Phelps investigation. But when Clark Hill relied on that report for other purposes and shared that report with people outside that purpose, Clark Hill's actions no longer aligned with the intended purpose stated at the outset of the incident response plan. When actions do not align with purposes, courts may be quick to strip protections.

Exercise caution when documenting during incident response

Given that courts are increasingly finding incident response efforts to be a business (and not a legal) function, IR teams must be trained to document investigation efforts carefully, as if they expect the documentation and communications to be part of litigation, or even worse, make their way into the press. Indeed, an organisation is only as strong as its people — all personnel should be informed that their communications are potentially discoverable. A good rule of thumb is to educate personnel to document facts, not opinions. Personnel should also be taught to avoid any unnecessary written communications and avoid speculating on the reason for, or impact of, an incident. Communications hypothesising about a company's fault as it relates to an incident or referring to an incident as a 'breach', which is a legally defined term, can affect an

organisation's legal position and create risks during litigation and enforcement actions.

REMEMBER, FOCUS ON THE PURPOSE AND ENSURING ACTS FOLLOW THE INTENDED PURPOSE

These recent decisions, when viewed holistically, follow a common theme. Courts, in determining the applicability of the attorney–client privilege or work product doctrine to investigatory materials, will assess the investigation's underlying purpose and motivation. Simply having outside counsel nominally hire the forensic company is not enough. Recent cases have made it clear that establishing protections involves a highly fact-sensitive inquiry, and after-the-fact attempts to shield an investigation from opposing parties will not pass judicial scrutiny. Companies — with the assistance of counsel — must clearly delineate the purpose of an investigation at the outset of the response and outline a plan for conduct that demonstrates that purpose.

Successfully maintaining attorney–client privilege and work product doctrine protections throughout the incident response process requires careful consideration and affirmative action well before a cyber security incident is detected. There is no fixed formula to ensure the protections apply, and courts will examine the detailed factual circumstances surrounding any asserted protection. In the often chaotic aftermath of a cyber security incident, companies face a daunting proposition to manage these considerations while simultaneously responding to the incident itself. But armed with the advance knowledge of the factors courts will examine to determine whether attorney–client privilege or work product doctrine protections apply, companies can take proactive steps *before* an incident to ensure their incident response plans are positioned to maintain these critical protections throughout the life cycle of a cyber security incident response.

By proactively creating an IR plan that emphasises the primary purpose of each action with future judicial analysis in mind, companies can place themselves in the best position to demonstrate a clear purpose for each step of the IR process — and consequently, be better prepared to ensure that the most sensitive aspects of the response to a given incident remain well protected behind the attorney–client privilege or work product doctrine.

References

1. See for example in *Target Corp. Customer Data Security Breach Litig.*, MDL No.14-2522 (PAM/JJK), 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015) (finding protections apply where 'Target has demonstrated … that the work of the Data Breach Task Force was focused not on remediation of the breach, as Plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company [in litigation].'); *Nat. Union Fire Ins. Co. of Pittsburg, Pa. v. Murray Sheet Metal Co., Inc.*, 967 F.2d 980, 984 (4th Cir. 1992) ('Determining the driving force behind the preparation of each requested document is therefore required in resolving a work product immunity question.').
2. *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).
3. 425 U.S. 391, 403 (1976).
4. See, for example in *Rutter's Data Security Breach Litig.*, C.A. No. 1:20-cv-382, 2021 WL 3733137, at *2-4 (M.D. Pa. July 22, 2021) (examining totality of relationship between company and outside investigator, and not just individual documents, in both work product doctrine and attorney–client privilege analysis).
5. Courts have uniformly held that any documents transmitted to an attorney for the purpose of seeking legal advice, which could have been obtained by court process directly from the client, can be obtained directly from the attorney. *Upjohn*, 425 U.S. at 403-04 ('This Court and the lower courts have thus uniformly held that pre-existing documents which could have been obtained by court process from the client when he was in possession may also be obtained from the attorney by similar process following transfer by the client in order to obtain more informed legal advice.').
6. *United States v. Nobles*, 422 U.S. 225, 238 (1975).
7. *Ibid.*
8. Fed. R. Civ. P. 26(b).
9. *Paice, LLC v. Hyundai Motor Co.*, 302 F.R.D. 128, 133 (D. Md. 2014) ('Materials prepared in the ordinary course of business, pursuant to regulatory

requirements, or for other non-litigation purposes are not prepared in anticipation of litigation.').

10. In *Grand Jury Subpoena*, 220 F.R.D. 130, 147 (D. Mass. 2004) ('[A]nticipation requires something more than a mere remote possibility of litigation.').
11. In *Grand Jury Proceedings*, No. M-11-189, 2001 WL 1167497, at *17-18 (S.D.N.Y. Oct. 3, 2001) (government subpoena gives rise to reasonable anticipation of litigation); *Cal. Earthquake Auth. v. Metro W. Sec., LLC*, 285 F.R.D. 585, 590 (E.D. Cal. 2012) (request for mediation creates threat of litigation); *Kan. City S. Ry. v. Nichols Constr. Co.*, C.A. No. 05-1182, 2007 WL 2127820, at *5 (E.D. La. July 25, 2007) (particularly severe nature of incident creates reasonable anticipation of litigation).
12. See *Johnson v. Air Liquide Large Indus. U.S. L.P.*, Case No. 2:18-CV-259, 2019 WL 4256962, at *5 (E.D. Tex. Sept. 9, 2019) (finding intent to preserve evidence relevant to determining whether reasonable anticipation of litigation existed for work product protection).
13. *United States v. Aldman*, 134 F.3d 1194, 1202 (2d Cir. 1998) ('[T]he "because of" formulation that we adopt here withholds protection from documents… that would have been created in essentially similar form irrespective of the litigation.').
14. *Paice*, 302 F.R.D. at 133.
15. In re *Premera Blue Cross Customer Data Security Breach Litig.*, 296 F.Supp.3d 1230 (D. Or. 2017).
16. *Ibid*., at 1245.
17. *Ibid*., at 1245.
18. *Ibid*., at 1245.
19. *Ibid*., at 1245.
20. In re *Rutter's Data Security Breach Litig.*, 2021 WL 3733137, at *1.
21. *Ibid*.
22. *Ibid*.
23. *Ibid*., at *2-3.
24. 338 F.R.D. 7, 9 (D.D.C. 2021).
25. *Ibid*. at 11.
26. *Ibid*.
27. *Ibid*.
28. *Ibid*. at 13 (citations omitted) (emphasis in original).