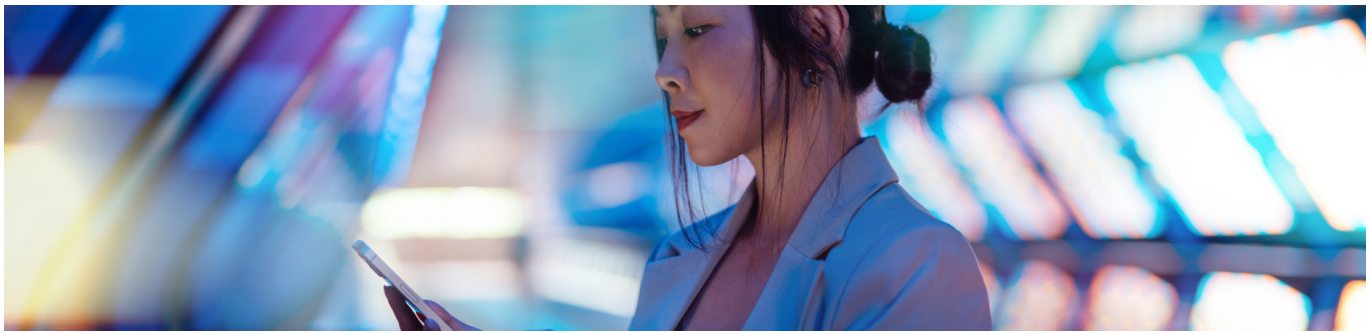
SQUIRE PATTON BOGGS

Defending the Privilege of a Forensic Report

Colin Jennings, Steven Delchin and Gicel Tomimbang[1]

US – August 1, 2024



This is our Global Data Breach Response Team's client alert regarding defending the work-product status and attorney-client privilege of forensic reports. For information about how the Global Data Breach Response Team responds to, handles and assists clients in addressing cyber incidents, please visit our website. You can also subscribe to Privacy World, your one-stop shop for fast-breaking news and views on the high¬speed developments surrounding data privacy, security and innovation, brought to you by lawyers who practice in this space every day.

The Forensic Report

When a company experiences a cybersecurity incident, standard practice is to hire an independent cybersecurity firm to assist with investigating, and assessing the nature and scope of the cybersecurity incident. A forensic report is typically provided at the conclusion of the cybersecurity firm's investigation, which records details pertaining to the response efforts and investigation findings, including:

- The identity of the (suspected) threat actor group that perpetrated the cyberattack
- The attack vector, the initial access point and the vulnerabilities the threat actor exploited to gain access to the target's IT environment
- The date the threat actor gained access to the target's IT environment (date of intrusion) and the date the threat actor deployed the cyberattack (date of compromise)
- The systems that were impacted by the cybersecurity incident and the threat actor's activities within those systems (i.e., lateral movement, access and exfiltration), and the categories of personal information affected

Legal Counsel and the Forensic Report

As a best practice, key regulators, including the US Federal Trade Commission, recommend first hiring outside legal counsel with privacy and cybersecurity expertise when responding to a cybersecurity incident. Legal counsel with cybersecurity and breach experience can advise businesses on legal obligations necessary for cybersecurity incident response, as well as data breach notification obligations across jurisdictions.

Counsel will typically retain a cybersecurity firm to gather information about the incident. The cybersecurity firm will prepare a forensic report that includes a technical assessment of the incident, its likely causes and potential impacts. Counsel will use this information to determine legal obligations across jurisdictions and develop an incident response and legal strategy to mitigate risks associated with the incident. Counsel will also rely on the forensic report to anticipate and defend the business against potential future claims.

Where counsel commissions the forensic report for the express purpose of informing the legal advice they provide to the affected business, forensic reports have historically been treated as attorney work-product, and therefore privileged and not discoverable in litigation. Further, the attorney-client privilege can attach to reports of other third-parties made at the request of the lawyer or the client, where the primary purpose of the report was to put in usable form information obtained from the client.

Protecting the Forensic Report from Litigation Discovery

The discoverability of a forensic report in litigation is a significant issue, as the forensic report generally details the critical vulnerabilities in a company's information technology environment that enabled the cyberattack. The report often identifies areas in which a company's IT defense fell short or was noncompliant with best practices and regulatory or industry standards. Accordingly, the forensic report contains information that could be potential evidence of the company's negligence or recklessness in safeguarding the privacy and security of its consumers' personal information.

In data breach litigation, plaintiffs will typically plead a variety of statutory and common claims in pursuit of liquidated statutory damages or file class actions and seek to negotiate a settlement relying upon the defendant's insurance coverage. Plaintiffs typically also seek to discover any forensic reports as evidence to substantiate their claims.

1 We extend our sincere gratitude and appreciation to Yiannis Vandris, 2024 Summer Associate, for his contributions to this publication.

No Privilege if the Forensic Report is Prepared for Business vs. for Litigation/ Legal Purposes

The attorney work-product privilege has limits. For the privilege to attach to the forensic report, so it is not discoverable in litigation, companies must demonstrate that the forensic report was prepared in anticipation of litigation. Documents that are routinely prepared in the ordinary course of business, or that are produced for some other purpose and then subsequently prove helpful in litigation are not protected by the work-product privilege. Some courts have even held that where a document would have been created in a substantially similar form regardless of the litigation, the work-product privilege does not apply.

Likewise, to maintain the attorney-client privilege, companies must demonstrate the primary purpose of the report was to seek legal advice. While the attorney-client privilege does not ordinarily protect communications between attorneys and third-parties, privilege can attach to reports intended to put information obtained from the client into a usable form. If a forensic report goes beyond simply translating the technical aspects of the breach for counsel's understanding, it may fall outside the scope of the attorney-client privilege.

Part of the standard cybersecurity compliance and risk mitigation efforts companies often take include agreements with cybersecurity firms for a comprehensive suite of cybersecurity compliance services. These agreements include both proactive data security services (e.g., security and risk assessments) and future incident response services (e.g., forensic investigation with a forensic report when a breach occurs) to ensure that the company can quickly respond to a cybersecurity incident. Directly engaging a cybersecurity firm for both proactive and incident response services prior to a cybersecurity incident occurring seems practical from a data security and risk mitigation perspective. However, doing so risks potentially conflating documents that are prepared for ordinary business purposes and those prepared specifically in anticipation of litigation, such that neither the work product nor attorney-client privilege would apply.

Best Practices for Defending Privilege of a Forensic Report

Courts evaluate the totality of the circumstances when determining whether a forensic report is privileged and will generally construe evidentiary privileges narrowly. Therefore, companies must start defending the privilege of the forensic report early, well before it is drafted and finalized. To maximize the chances of successfully asserting privilege over a forensic report, it is important to adhere to best practices elucidated by recent case law, including:

1. Engage an Independent Cybersecurity Firm Through Outside Counsel

Recent case law pertaining to the discoverability of forensic reports has determined that to truly anticipate litigation, the scope of the forensic services must be determined after the cyberattack has occurred. Accordingly, where reasonable and appropriate, it is advisable to retain a cybersecurity firm, through outside counsel, with which your company has no preexisting relationship for incident response services. Proceeding in this manner would, among other things, make it easier to demonstrate that the cybersecurity firm was retained as part of the overall legal and incident response strategy.

2. Consider a Two-track Investigation, Tighten Up Your Statements of Work (SOWs)

It may not be feasible to engage a cybersecurity firm with no preexisting relationship.

As a practical matter, a company may opt instead to proceed with a two-track investigation wherein the company leverages its existing cybersecurity firm to conduct an investigation for business purposes, while retaining a separate independent cybersecurity firm at the direction of outside counsel to conduct an investigation in anticipation of litigation. The investigation for business purposes would not be privileged, and its findings would be focused on matters that contribute to business considerations – such as determining profit and liability projections, identifying software or hardware upgrades, as well as liaising with the FBI for attribution purposes. The investigation in anticipation of litigation, on the other hand, would be privileged and focused on matters that would assist counsel in advising the company on its incident response-related legal obligations.

However, if the company opts to use the same cybersecurity firm for its proactive and incident response efforts, the company should (a) make sure that the existing cybersecurity firm is separately engaged by outside counsel for incident response activities; and (b) isolate the litigation-related services that the cybersecurity firm provides in a detailed and separate SOW that makes clear how the scope and purpose of the litigation-related work differs from any preexisting SOWs.

The SOW should clarify, for example, that counsel is directing the work for the purpose of providing legal advice and guidance to the company in anticipation of litigation. It should not include any unrelated work such as remediation that may be covered under preexisting SOWs. Additionally, courts generally have not found nominal statements regarding an investigation's legal purpose to be particularly persuasive. In order to defend privilege, a forensic report must actually be used by counsel to provide legal advice.

3. Use the Forensic Report Only for Litigation Purposes, and Limit Its Disclosure Only to Necessary Individuals

The company should use the forensic report prepared at the direction of counsel solely for litigation purposes. The full forensic report should only be shared with in-house counsel. In-house counsel may share, as necessary, a separate high-level summary of the forensic report with the board of directors, and third parties, such as auditors, law enforcement and regulators. Other members of the company's workforce, such as members of the leadership and IT teams, may refer to the report resulting from the non-privileged business-focused investigation if their duties require them to understand the scope of the cybersecurity incident and the vulnerabilities identified.

4. Exercise Caution in Public Statements

Companies should also avoid publicly leveraging the report or their retention of a cybersecurity firm for non-litigation purposes. In a recent case, a company eager to mitigate concerns after a breach mentioned the retention of a cybersecurity firm in its breach notification letters to customers, and in a list of internally circulated talking points for customer-facing employees. The court found that reassuring customers and shaping communications strategies are non-litigation, business purposes and rejected the company's claim that the forensic report prepared by the cybersecurity firm was protected by the work-product doctrine.

5. Just the Facts, Please

The forensic report should detail only the facts, as supported by forensic findings and should not include recommendations for further investigation and remediation; information that is speculative; or opinions (i.e., no severity rating, compliance scoring, etc.). Such content may be interpreted as evidence that the forensic report was created for business considerations and not in anticipation of litigation or for the primary purpose of obtaining legal advice. The forensic report should also clearly indicate that the purpose of the report was to assist counsel in providing legal advice to counsel's client in anticipation of litigation.

6. Charge From Your Legal Budget

A company should pay for incident response services out of its litigation or legal budget to show that a forensic firm's services were provided in anticipation of litigation and for the provision of legal advice. This will help differentiate the incident response services from the traditional IT and cybersecurity services paid for with operational business accounts. Companies should pay close attention to how they pay and account for cybersecurity and incident response services to clearly differentiate business and legal functions. When appropriate, retainers or similar payments should be allocated to a legal function and accounting entries should be written to demonstrate the legal purpose of the work to be undertaken. In any event, before incurring the expenses, companies should consider designating the costs of incident response services to their legal budgets to show that such services are provided in anticipation of litigation.

How We Can Help

Our Global Data Breach Response team combines experienced cybersecurity, privacy, litigation, government investigations, insurance and labor and employment specialists working together to provide the technical, legal, regulatory, as well as procedural advice and support that you need to protect your company and your data.

How we can assist:

- Conduct cybersecurity threat risk assessments
- Develop and/or review company-specific cybersecurity incident response plans
- Build cybersecurity compliance programs and procedures
- Design and conduct training, including desktop exercises and simulations
- Provide legal support 24/7 to assist clients in responding to ransomware attacks, data breaches, phishing emails, etc.
- Coordinate and draft breach notifications to data subjects and regulators
- Handle legal claims from data subjects
- Conduct internal investigations
- Liaise with law enforcement and national security agencies
- Respond to enforcement actions
- Advise on insurance coverage and recovery
- Coordinate with IT professionals and technical consultants on the recovery of data, and network remediation
- Supervise forensic investigations and support on litigation strategy
- Litigate cybersecurity and data privacy matters
- Work with public relations and marketing professionals on crisis management messaging

Our Global Data Breach Response team is well-equipped to advise and assist your business on all aspects of ransomware response. Our experienced team includes seasoned data protection and litigation experts in the US, the EU and across key markets, who will coordinate national and international preparation for, and responses to, cybersecurity and personal data breach threats of all types, including ransomware attacks.

For further information, please contact

Colin Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squirepb.com

Steven A. Delchin
Senior Attorney, Cleveland
T +1 216 479 8278
E steven.delchin@squirepb.com

Gicel Tomimbang
Associate, Los Angeles
T +1 213 689 6543
E gicel.tomimbang@squirepb.com