FEBRUARY 17, 2022 • 7 MIN READ

Challenges to privilege over cybersecurity investigations: Cross-border litigation trends

AUTHORS


Julie Himo


Molly Reynolds


Alina Butt

As cybersecurity incidents have increased dramatically in recent years, so have regulatory investigations and litigation. Regulators and plaintiffs regularly ask for production of forensic reports and other documents relating to internal investigations of data breaches, ransomware and other incidents, and the limits of legal privilege over these materials are being tested on both sides of the border. As businesses continue to develop their incident response plans, boards and management should be aware of recent cross-border trends questioning the scope of lawyer-client, work product and litigation privilege over cybersecurity investigations.

Legal landscape in Canada

Cybersecurity incidents are usually closely managed by in-house or external counsel, given that the cause, consequences and response to the breach ties closely to the organization's legal and regulatory risks. Correspondence, internal reports and expert assessments of incidents are routinely labelled privileged because they are requested by counsel or created to support the analysis of the company's legal exposure. However, courts are just starting to test the strength and breadth of those privilege claims in Canada.

The Ontario Superior Court considered this issue in *Kaplan v. Casino Rama Services Inc.*, a proposed class action relating to a cyberattack on a casino. The plaintiffs sought production of a third-party investigative report, communications, and security audit records[1]. Casino Rama claimed privilege over the records. The court declined to rule on the privilege claim itself, but instead focused on waiver of privilege and relevance. Casino Rama had to disclose portions of the records it referred to in its certification materials (thereby waiving any valid privilege) and which were relevant to class size and scope (as opposed to broader issues of relevance to the merit of the claim if certified)[2].

A more common scenario involves a regulator's request for a forensic report about a data breach in the course of an investigation. Typically, the forensic firm was hired and instructed by counsel and the report is marked privileged on the basis that it supports counsel's legal advice to the client. But the report also includes detailed factual information about the evidence relating to the security compromise.

Join us for our webinar series "Leveraging the data life cycle: data strategies for business leaders". The first session on March 3 will explore tools and strategies to protect your "digital crown jewels". Register here.

This issue came before the Ontario Information and Privacy Commissioner (IPC) following a cybersecurity attack on LifeLabs. In 2019, LifeLabs notified the IPC that it had suffered a compromise of personal and health information of approximately 15 million customers[3]. The IPC requested documents from LifeLabs relating to the incident and its internal investigation[4].

LifeLabs claimed litigation and solicitor-client privilege over various documents, including security testing and communications with hackers by its incident response advisors, as well as correspondence with third parties involved in its concurrent litigation defence[5]. Unless explicitly authorized by statute, Canadian regulators cannot compel production of privileged information to decide the validity of privilege claims. As a result, a privilege dispute between an organization and a regulator must be reviewed by the courts, or decided by the regulator on the basis of a description of the records only[6].

To address the privilege objections, the IPC demanded the production of an itemized list of responsive documents describing "what documents exist and the basis for each claim"[7]. Unsatisfied with LifeLabs' response listing broad categories of documents, the IPC ordered production of third-party documents including forensic reports and internal analyses of changes made by LifeLabs in response to the breach[8]. Importantly, the IPC's reasoning turned on the lack of evidence provided by LifeLabs to justify its claims of privilege rather than a specific finding that the documents were not privileged.

The Commissioner noted that it is not enough for a party to have been subject to concurrent litigation for incident response documents to be litigation privileged[9]. LifeLabs needed to rebut a presumed inference that "the third party documents were necessarily also created in response to the operational needs of the company as it dealt with the breach"[10]. As well, the mere communication of third-party reports in LifeLabs' control to in-house or outside counsel did not necessarily give rise to solicitor-client privilege according to the IPC[11]. While LifeLabs indicated that it was seeking judicial review of this order, no public decision has yet been released.

Legal landscape in the United States

The law is relatively more developed in the United States, with a fact-specific body of cases leading to the recent decision in *In re Capital One*.

Capital One had a standing retainer with Mandiant, a well-known cybersecurity advisory and incident response firm. After Capital One suffered a cybersecurity incident, external counsel engaged Mandiant, under the umbrella of the existing business retainer, to report on the "technical factors" leading to the breach[12]. Capital One relied on the work product doctrine (which is similar to litigation privilege in Canada) to resist production of this report in a consumer class action[13]. The court found that re-purposing a standing business retainer into a legal retainer was insufficient to establish privilege because Mandiant offered Capital One the same services before the cyber incident as afterwards. Put another way, the existing business advisory services could not be re-papered by counsel to protect them from production in litigation.

Notably, the court compared Capital One's relationship with Mandiant to that of Experian and Mandiant in an earlier case[14]. In contrast to Capital One's standing retainer, Experian had first retained outside counsel who then engaged the services of Mandiant[15]. In contrast to Capital One's internal distribution of the forensic report, Mandiant sent its report to Experian's outside and internal legal counsel, but not its internal incident response team, which supported the claim it was prepared for litigation rather than business advice[16].

The result is that while the report in *Experian* was protected, the report in *Capital One* had to be produced because the court was not convinced that the report would have been substantially different than if the company was not facing litigation relating to the data breach.

More recently, the Pennsylvania Federal Court required production of a forensic report in the *Rutter's* data security breach litigation. The court found that the third-party investigative report generally focused on whether there had been a breach and its scope—factual information relevant to the business well before litigation was contemplated[17].

Implications for business

While the law on this issue is still developing across North America, organizations must consider privilege early in the investigation of cybersecurity incidents. Boards, management and incident response team members should consider:

- explicit privilege protocols as part of incident response plans, which address:
  - internal and external communications about cybersecurity readiness, internal investigations, external investigations and litigation;
  - retention of operational and crisis-response advisors;
  - determining if legal counsel to be retained to oversee the investigation will be in-house or external;
  - documenting when litigation is anticipated; and
  - stakeholders who need access to various factual information for their respective business and legal roles;
- clearly identifying the scope and purpose of incident investigations, and separating retainers (and reports) for incident preparedness; incident response; and regulatory or litigation fact gathering;
- having legal counsel incorporate forensic findings relevant to their legal analysis into separate analysis by counsel on the application of law, regulatory regimes and contractual obligations to the facts of the incident in order to assess risk and provide strategic advice;
- sources of evidence used in defending litigation, to ensure reports prepared for counsel are not co-mingled with prevention or remediation advice to the business or disclosed in a manner that waives privilege; and
- rigorous documentation of privileged and non-privileged correspondence and reports, to facilitate compliance with regulatory investigations.

FOOTNOTES

1. 2018 ONSC 3545 at para 2 [*Casino Rama*].
2. *Casino Rama* at paras 11, 18.
3. PHIPA Decision 114 at para 3 [*LifeLabs*].
4. *Ibid* at para 5. The IPC's first request was pursuant to section 38(1)(b) of the *Personal Information Protection Act*. The IPC later made a further demand for production pursuant to section 40 of the *Personal Health Information Protection Act, 2004*.
5. *Ibid* at paras 6, 13.
6. The Supreme Court of Canada made this distinction in *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, 2008 SCC 44 at paras 22, 29. In this case, a former employee was denied access to her personnel file by her employer despite her suspicions that it contained inaccurate and improperly collected information. The federal Privacy Commissioner ordered production of documents over which the employer claimed solicitor-client privilege. This order was initially granted but denied on subsequent appeals.
7. *Ibid* at paras 12-13, 18.
8. *Ibid* at paras 31-32.
9. *Ibid* at para 36.
10. *Ibid* at para 43.
11. *Ibid* at paras 65, 67.

12. *In re Capital One Consumer Data Security Breach Litigation*, 2020 U.S. Dist. LEXIS 91736 (E.D. Va. May 26, 2020) at *5 [*In re Capital One*]; see also this incident addressed in a proposed Canadian class action, *Del Giudice v. Thompson*, 2021 ONSC 5379.

13. *In re Capital One* at *9.

14. *In re Capital One* at *14-16; *In re Experian Data Breach Litigation*, 2017 U.S. Dist. LEXIS 162891 (C.D. Cal. May 18, 2017).

15. There are several other cases that have considered the same factors as those discussed in *Capital One* and *Experian*. In *In re Dominion Dental Servs. United States*, 2019 U.S. Dist. LEXIS 225275 (E.D. Va. 2019), a report by Mandiant was considered non-privileged because the defendants and Mandiant had been in a relationship prior to the incident, and because most of Mandiant's work served business purposes such as prevention and remediation. As well, in *In re Premera Blue Cross Customer Data Security Breach Litigation*, 2019 U.S. Dist. LEXIS 20279 (D. Or. 2019) at *668, the shifting of an existing work agreement to outside counsel did not necessarily result in a change in the scope of work and therefore the application of privilege.

16. The widespread sharing of an investigation report has also led to conclusions that privilege did not apply in other cases, such as *Wengui v. Clark Hill, PLC*, 2021 U.S. Dist. LEXIS 5395 (D.D.C. 2021) at *12.

17. *In re Rutter's Data Security Breach Litigation*, 2021 U.S. Dist. LEXIS 67031 (M.D. Pa. July 22, 2021) at *6, 12

To discuss these issues, please contact the author(s).