Cyber Risk Management – Legal Privilege Strategy – Part 2

July 28, 2016

An organization's cyber risk management activities may result in sensitive communications and documents that the organization's personnel expect will remain confidential. Nevertheless, in many circumstances an organization may be legally obligated to disclose those communications and documents unless the organization is able to assert a legal right – called "legal privilege" – to not make the disclosure. This two-part bulletin discusses legal privilege and cyber risk management. The first part of this bulletin discusses cyber risk reporting and disclosure obligations and the basic rules for legal privilege. The second part of this bulletin provides practical recommendations for a legal privilege strategy for cyber risk management activities.

Sensitive Communications And Documents

Cyber risk management involves the creation of many kinds of sensitive communications and documents, including threat risk assessments, assessments of cyber risk prevention activities and incident response preparedness, legal/contractual compliance assessments, insurance coverage advice, cyber risk management advice to directors and officers and cyber incident investigation reports. Those communications and documents often identify gaps and deficiencies in an organization's cyber risk management plans and activities relative to industry best practices, regulatory guidance and legal obligations (including contractual, common law and statutory requirements) and recommendations for improvement.

Those communications and documents might be subject to legal disclosure obligations if they are relevant to a contractual audit, a regulatory investigation or proceeding or a civil lawsuit, even though the organization's personnel expected the communications and documents would remain confidential. However, many of those communications and documents might be protected from disclosure by legal privilege, depending on the purpose of the communication or document and the circumstances surrounding the creation and use of the communication or document. An organization that asserts legal privilege over a communication or document has the burden of proving the privilege applies. For those reasons, it is prudent for an organization to implement a reasonable legal privilege strategy to enable the organization to establish legal privilege where appropriate.

Legal Privilege Strategy

Overview

A legal privilege strategy should be designed to enable an organization to prove, where appropriate, that a communication or document was made for a privileged purpose and in circumstances that support a finding of legal privilege, and should help prevent inadvertent waiver of privilege.

A legal privilege strategy should be an integral part of an organization's overall cyber risk management planning and activities. The strategy should be carefully planned, thoroughly implemented (including as part of cyber incident response plans) and periodically reviewed and refreshed.

An organization's legal privilege strategy should be suitable for the organization in light of all relevant circumstances, including size and sophistication of the organization, the nature of the organization's business activities (including the applicable regulatory framework) and the organization's cyber risk profile. There is no one-size-fits-all strategy.

Recent U.S. court decisions – *Genesco Inc. v. Visa USA Inc.* and *Re Target Corporate Customer Data Security Breach Litigation* – demonstrate how a legal privilege strategy can be used to establish legal privilege over cyber incident investigation reports. Each of those lawsuits related to a cyber incident that was subject to two separate internal investigations by separate teams – a business investigation for business purposes, and a legal investigation (directed by an external lawyer) for legal advice and litigation purposes. The plaintiffs in the lawsuits sought disclosure of the internal investigation reports. In each lawsuit, the court held that the report resulting from the business investigation had to be disclosed, but the report resulting from the legal investigations was protected by legal privilege and did not have to be disclosed. Those cases are instructive, but they must be considered with caution by Canadian organizations because U.S. rules for legal privilege are different from Canadian rules.

Comments/Recommendations

Following are some comments and recommendations for preparing and implementing a legal privilege strategy:

- **Legal Counsel and Legal Purpose:** Engage a lawyer to provide legal advice (including providing overall management and coordination of certain cyber risk management activities) or to assist with litigation as soon as possible, before beginning the relevant cyber risk management activities, and document the purpose of the engagement to support legal privilege claims.
- **Education/Training:** Educate the organization's relevant personnel about confidentiality, disclosure obligations and legal privilege (including the requirements for, and limits of, legal privilege and the risks of inadvertent waiver of privilege), establish practices and procedures for establishing legal privilege over sensitive communications and documents and avoiding inadvertent waiver of privilege, and verify compliance with those practices and procedures through periodic training and exercises.

- **External Consultants:** Where appropriate, external consultants (including technical advisors, investigators, public relations advisors, accountants, potential litigation experts) should be engaged, directed and supervised by a lawyer, and the terms of engagement, correspondence and reports should be consistent with and support legal privilege protection for the documents created by the consultant.
- **Involvement of Legal Counsel:** Where appropriate, internal cyber risk management activities should be directed by a lawyer for expressly stated legal advice or litigation purposes, and the lawyer should be involved in all related correspondence (including email) and should receive all resulting reports.
- **Internal v. External Lawyers:** In-house lawyers should be mindful that legal advice privilege applies only to legal advice, and not to non-legal advice they provide as a business executive, investigator or other non-legal advisor. If there is a reasonable risk that a court will consider an in-house lawyer to be acting in a non-legal capacity giving non-legal advice, then an external lawyer should be engaged to perform legal functions required to establish privilege.
- **Incident Response Plans:** Incident response plans, including the engagement of the incident response team and the assignment of roles and responsibilities, should be consistent with the legal privilege strategy.
- **Marking/Explanations:** All internal and external documents (including correspondence and reports) and discussions (including interviews) relating to privileged activities should be clearly marked with appropriate confidentiality and legal privilege designations (e.g. "privileged and confidential – legal advice", "privileged and confidential – for litigation purposes" or "privileged and confidential – created for legal counsel"), and should include appropriate notations/explanations regarding the privileged purpose. Legal privilege markings should not be used where inappropriate, because doing so may dilute and undermine the effect of appropriate privilege markings.
- **Limited Disclosure/Distribution:** The internal and external disclosure and distribution of privileged communications and documents (including correspondence, documents and reports) should be limited to individuals who have a legitimate need to know that is consistent with the privilege claim, and who are properly informed of, and agree to protect, the confidential and privileged nature of the communications and documents.
- **Data Security Incident Reporting:** Data security incident reports and related notifications and disclosures, including disclosures to law enforcement and government regulators, should not include privileged communications and documents.
- **Separate Documents:** Where practicable, privileged and non-privileged communications and information should not be recorded in the same document, to avoid the need assert privilege over part of a document.
- **Separate Activities:** Where practicable, privileged and non-privileged activities should be undertaken by discrete teams. For example, if a cyber incident occurs, then one technical team could conduct a non-privileged business investigation focussed on remediation, while a separate technical team engaged by legal counsel could conduct a privileged investigation for the purpose of preparing for litigation relating to the incident and assisting legal counsel to provide legal advice.

Final Comment

Cyber risk management activities invariably result in sensitive communications and documents that may be subject to disclosure in connection with contractual audits, regulatory investigations and proceedings and civil lawsuits, unless the communications and documents are protected by legal privilege. A reasonable legal privilege strategy can help establish legal privilege over many of those kinds of communications and documents. For those reasons, a legal privilege strategy should be an integral part of an organization's overall cyber risk management planning and activities. The strategy should be carefully planned, thoroughly implemented and periodically reviewed and refreshed.

By:

Bradley Freedman

Services:

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749