JULY 2016

CYBERSECURITY BULLETIN

Borden Ladner Gervais

CYBER RISK MANAGEMENT – LEGAL PRIVILEGE STRATEGY – PART 1

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.

REPORTING AND DISCLOSURE OBLIGATIONS

Data Security Incident Reporting Obligations

Data security incident reporting obligations may be imposed by statute, contract or generally applicable common law or civil law, and may specify when, how and to whom notice of a data security incident must be given. Failure to give timely notice of a data security incident may result in serious adverse consequences, including statutory sanctions, liability for breach of contract or breach of a duty to warn and loss of insurance coverage.

For example, the Canadian federal *Personal Information Protection and Electronic Documents Act* will soon require an organization that suffers a breach of security safeguards that presents a "real risk of significant harm to an individual" to report the breach to the Privacy Commissioner, give notice of the breach to affected individuals and to certain organizations and government institutions, and keep and maintain prescribed records of the breach. The Alberta *Personal Information Protection Act* imposes similar data security breach notification obligations. Generally applicable common law and Québec's civil law may also require an organization that suffers a data security incident to warn individuals and other organizations if the warning would enable them to avoid or mitigate harm caused by the incident.

Commercial contracts often contain obligations to give notice of an unauthorized disclosure of confidential information and data. Cyber-insurance policies invariably require an insured organization to give the insurer prompt notice of any actual or reasonably suspected data incident suffered by the organization. The Payment Card Industry Data Security Standard, which is incorporated into contracts governing participation in payment card systems and applies to all organizations involved in payment card processing (including merchants who accept payment card transactions), imposes obligations to report incidents relating to the security of payment card data.

Other Disclosure Obligations

An organization's cyber risk management activities (including preparations for and responses to data security incidents) may be subject to contractual audits (e.g. by a business partner or service provider), regulatory investigations or proceedings (e.g. by a privacy commissioner or industry regulator) or civil lawsuits (e.g. by customers, business partners or shareholders). In those circumstances, the organization might be legally obligated to disclose all relevant documents and information, including documents that the organization's personnel expected would remain confidential.

For example, a party to a Canadian civil lawsuit is required to disclose to the other parties all documents in the party's possession, power or control that are relevant to the issues in the lawsuit. Similarly, Canadian privacy commissioners are authorized to conduct investigations and to compel organizations to disclose relevant documents and information. In each of those situations, the fact that a document was expected to remain confidential is generally not a lawful basis for refusing disclosure.

LEGAL PRIVILEGE – GENERAL PRINCIPLES

In limited circumstances, an organization might be able to assert a legal right – called "legal privilege" – to refuse to disclose certain kinds of communications and documents. There are two kinds of legal privilege under Canadian law that might be applicable – "legal advice" privilege and "litigation" privilege. Each kind of privilege is different in purpose, scope and duration. Communications and documents might be protected by either or both kinds of privilege, depending on the circumstances. An organization that asserts legal privilege over a communication or document has the burden of proving that the privilege applies.

Legal Advice Privilege

Legal advice privilege (also known as "solicitor-client privilege") is a fundamental principle of justice and a substantive legal principle that is almost absolute. The privilege applies to confidential communications (written and oral) between a lawyer and client for the purpose of seeking or giving legal advice. The purpose of the privilege is to protect the lawyer-client relationship so that clients are able to confide in their lawyers to obtain proper legal advice. The privilege applies to communications between a lawyer and client, and usually not to communications with other persons. The privilege applies any time a client seeks legal advice from the lawyer, regardless of whether or not litigation is ongoing or anticipated. The privilege lasts unless and until it is waived by the client.

Litigation Privilege

Litigation privilege (also known as "work product privilege" or "lawyer's brief privilege") is a procedural rule of evidence that is not absolute. The privilege applies to communications and documents created for the dominant purpose of use in connection with ongoing or reasonably anticipated litigation. The purpose of the privilege is to provide a litigating party and its lawyers with a "zone of privacy" necessary for the proper functioning of the adversarial litigation process, so that lawyers may prepare for litigation without risking disclosure of their legal opinions, strategies and other work product. The privilege applies to communications and documents between a lawyer and client and to certain kinds of communications and documents between a lawyer and third parties (e.g. technical experts). The privilege applies only if a communication or document was made for the "dominant purpose" (but not the sole purpose) of use in connection with ongoing or reasonably anticipated litigation. The privilege lasts until the relevant litigation and any closely related litigation (i.e. the same or related parties and the same or related disputes) have ended or the privilege is waived by the client.

Waiver of Privilege

A client may waive the client's right to assert legal privilege over communications and documents. Waiver of privilege ordinarily requires the client to knowingly and voluntarily demonstrate, by words or conduct, an intention to waive privilege. Nevertheless, privilege can also be waived inadvertently or implicitly in circumstances where fairness and consistency require it. For example, legal privilege over a communication or document might be waived if some or all of the communication or document is disclosed to other persons.

LEGAL PRIVILEGE – SPECIFIC ISSUES

Investigation Reports

An internal investigation report might be protected from disclosure by either or both of legal advice privilege (to the extent that the report is a confidential communication between lawyer and client relating to the seeking or giving of legal advice) or litigation privilege (to the extent that the report was prepared for the dominant purpose of ongoing or reasonably anticipated litigation). The application of legal privilege to investigation reports can sometimes be complicated, because an investigation that begins with a business purpose (e.g. discovering the cause of an incident) might evolve into an investigation for a legal purpose (e.g. preparing for reasonably anticipated litigation relating to the incident). Also, in some situations, an investigation report might have discrete parts – some protected by legal privilege and others not protected.

In some situations, uncertainty regarding the application of legal privilege might be avoided by conducting two separate investigations of the same incident – an investigation for business purposes (resulting in communications and documents that are not privileged) and a separate investigation for legal purposes (resulting in communications and documents that are privileged).

In-house/External Lawyers

Legal advice privilege can apply equally to legal advice provided by an in-house lawyer or by an external lawyer, provided the advice is legal advice (as opposed to business advice) given by the lawyer in his or her capacity as a legal advisor (as opposed to as a business executive, investigator or other non-legal advisor). Similarly, litigation privilege can apply equally to communications and documents created by or at the request of an in-house lawyer or by an external lawyer, provided the communications and documents are for the dominant purpose of litigation (as opposed to another purpose). It is often easier to establish legal privilege over communications and documents created by external lawyers (who are usually retained to provide legal advice or to act as counsel in litigation) as opposed to communications and documents created by in-house lawyers (who often act as business executives or business advisors).

Disclosures to Government Agencies

An organization that suffers a data security incident might consider going beyond its legal disclosure obligations and voluntarily disclose investigation reports and related documents (e.g. expert consultant reports) to law enforcement, privacy commissioners and other government agencies. While there might be some practical benefit to those kinds of voluntary disclosures, it is important to bear in mind that the disclosures might result in a waiver of legal privilege over the disclosed documents. In addition, the recipient government agency might be subject to access to information laws that require the agency to make the disclosed documents and information available to a member of the public (including the media) who makes an access request.

LEGAL PRIVILEGE STRATEGY FOR CYBER RISK MANAGEMENT

Cyber risk management involves the creation of many kinds of sensitive communications and documents that might be protected 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. A legal privilege strategy is designed to enable an organization to establish legal privilege where appropriate. The second part of this bulletin provides practical recommendations for a legal privilege strategy for cyber risk management activities. ■

AUTHOR

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Scotia Plaza, 40 King St W, Toronto, ON, Canada M5H 3Y4
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com