OCTOBER 2015

CYBERSECURITY BULLETIN

Borden Ladner Gervais

CYBER-RISK MANAGEMENT – DATA INCIDENT NOTIFICATION OBLIGATIONS

Effective cyber-risk management requires that an organization have a comprehensive incident response plan, so that the organization can rapidly respond to a data incident. To prepare an incident response plan, an organization must understand its data incident notification obligations.

NOTIFICATION OBLIGATIONS – GENERAL

Data incident notification 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 incident must be given. Failure to give timely notice of a data 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.

NOTIFICATION OBLIGATIONS UNDER PERSONAL INFORMATION PROTECTION LAWS

- **Federal PIPEDA**

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) will soon impose reporting, notification and record keeping obligations in connection with a "breach of security safeguards" for personal information that creates a "real risk of significant harm" to an individual. Those obligations were added in June 2015 and are not yet in force, because required regulations have not been enacted.

PIPEDA provides that if a breach of security safeguards involving personal information under an organization's control creates a real risk of significant harm to an individual, then the organization must, as soon as feasible after the organization determines that the breach has occurred, give prescribed forms of notice to: (1) the Privacy Commissioner of Canada; (2) each affected individual; and (3) any other organization or government institution that the organization believes may be able to reduce or mitigate the harm resulting from the incident or if prescribed conditions are satisfied. In addition, the organization must create and maintain prescribed records of every breach of security safeguards involving personal information under the organization's control and provide copies of those records to the Privacy Commissioner on request.

PIPEDA broadly defines "breach of security safeguards" as the loss of, or unauthorized access to or disclosure of, personal information resulting from a breach of security safeguards required by PIPEDA (which includes safeguards for information that an organization has transferred to another organization for processing or storage) or from a failure to establish those safeguards. PIPEDA broadly and non-exhaustively defines "significant harm" as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record and damage to or loss of property, each determined in light of the relevant circumstances (e.g. the sensitivity of the information and the probability that the information has been, is being or will be misused).

The security breach reporting, notification and record keeping obligations can be enforced by regulatory proceedings and through court proceedings by affected individuals. A knowing contravention of those obligations is an offence punishable by a fine of up to $100,000.

- **Alberta PIPA**

The Alberta *Personal Information Protection Act* (PIPA) provides that an organization that has personal information under its control must, without unreasonable delay, give notice to the Alberta Privacy Commissioner of any incident involving the loss of, or unauthorized access to or disclosure of, the personal information if a reasonable person would consider the incident to present a real risk of significant harm to an individual. The prescribed form of notice includes details of the incident, an assessment of the resulting risk of harm to affected individuals, and information about the steps taken by the organization to reduce the risk of harm and to notify affected individuals. The Privacy Commissioner may require an organization to give notice to affected individuals. An organization's failure to timely report a data incident is an offence punishable by a fine of not more than $100,000, and exposes the organization to liability for damages to affected individuals.

- **British Columbia and Québec**

The British Columbia and Québec personal information protection statutes currently do not impose a data incident notification obligation, but the B.C. and Québec Privacy Commissioners have recommended that their respective statutes be amended to add those obligations. The B.C. and Québec Privacy Commissioners have also issued data incident response guidance that includes giving notice to affected individuals, the Privacy Commissioners and other organizations.

NOTIFICATION OBLIGATIONS UNDER OTHER STATUTES

An organization that operates in a regulated industry or has custody of regulated data may be subject to specific statutory data incident notice obligations. For example, public companies must comply with continuous disclosure obligations, which may require disclosures about data incidents and other cyber-risk issues in press releases, annual information forms, financial

statements (MD&A) and offering documents (e.g. a prospectus). As another example, personal health information protection statutes may require a health information custodian that has custody or control of an individual's personal health information to promptly notify the individual if the information is stolen, lost or accessed by unauthorized persons. Breach of a statutory data incident notification obligation may result in statutory sanctions (including administrative monetary penalties) and civil liabilities.

CONTRACTUAL NOTIFICATION OBLIGATIONS

An organization that suffers a data incident may be contractually obligated to give notice of the incident to contract counter-parties or affected third parties. Commercial contracts usually contain confidentiality obligations that apply to data disclosed by the contracting parties, and those obligations often include an express requirement that a party give the other party notice of any unauthorized use or disclosure of the other party's data. A data incident notification obligation may also be express or implied in an organization's customer-facing privacy policy. 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 insured organization. Breach of a contractual duty to give notice of a data incident may result in civil liability for damages resulting from the breach, loss of contract benefits (e.g. insurance coverage) and contract termination.

COMMON LAW AND CIVIL LAW NOTIFICATION OBLIGATIONS

Generally applicable common law (in provinces and territories other than Québec) and Québec's civil law may require an organization that suffers a data incident to warn individuals and other organizations if the warning would enable them to avoid or mitigate harm caused by the incident. Whether or not a duty to warn exists will depend on the particular circumstances, including the nature of the relationship between the organization suffering the data incident and the individuals and other organizations affected by the incident and whether it is reasonably foreseeable that a warning would help avoid or mitigate harm. Breach of a duty to warn may result in liability for financial losses that could have been avoided or mitigated had a timely warning been given.

OTHER CONSIDERATIONS

It may be prudent for an organization to give relevant stakeholders (e.g. customers, business partners and investors) prompt notice of a data incident even if there is no legal obligation to do so. For example, an organization may decide to give notice of a data incident if there is a real risk that the incident will be publicly disclosed by other persons (e.g. persons responsible for the incident) or if notice is appropriate for customer relations purposes.

COMMENT

An organization's data incident response plan should include the organization's data incident notification obligations under statute, contract and generally applicable common law and civil law, so that the organization can promptly comply with those obligations when an incident occurs. In addition, a data incident response plan should address whether and how an organization should give notice of a data incident to relevant stakeholders even if the notice is not legally required. ■

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 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