SEPTEMBER 2018

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Cyber Risk Management and Privacy Protection Require More than Technology

Effective cyber risk management and privacy protection require a comprehensive framework based on three pillars – people, processes and technology. The importance of people and processes for effective privacy protection is demonstrated by a recent decision of the Supreme Court of Newfoundland and Labrador regarding the admissibility of expert evidence in a medical record snooping class action lawsuit.

Hynes v. Western Regional Health Authority

The decision in *Hynes v. Western Regional Health Authority* involved a class action lawsuit on behalf of over one thousand individuals whose privacy was violated when the defendant's employee accessed the plaintiffs' electronic medical records without a valid reason. The plaintiffs relied on several legal causes of action (e.g. breach of statutory and common law privacy rights, negligence and breach of contract) based on the defendant's failure to adequately safeguard the plaintiffs' personal health information. The parties applied to court to qualify their respective expert witnesses to give opinion evidence to assist the court in determining the applicable standard of care owed by the defendant to the plaintiffs in safeguarding their personal health information.

- **Plaintiffs' Expert**

The plaintiffs applied to qualify a proposed expert witness to give evidence in areas of computer operating systems, servers, programming language and the logic/operation of a database management system. The plaintiffs argued that determining the appropriate standard of care required an understanding of computer systems. The court rejected the plaintiffs' argument and refused to accept the expert's opinion evidence on the basis that it was "not logically relevant to an issue at trial". The court stated:

> *The proposed evidence does not meet the threshold requirement of relevance. This is not a case about the computer operating systems. Opinion evidence in these areas will not assist the trier of fact in determining the appropriate standard of care, or assessing whether the Defendant's conduct fell below that standard.*
>
> *… the facts in issue will not require technical expert evidence on computer operating systems, servers, programming language, and database management. In my view, detailed and technical opinion evidence about computer systems will complicate what is a relatively simple issue, and will waste the court's time.*

- **Defendant's Expert**

The defendant applied to qualify a proposed expert witness to give evidence in areas of health information systems (including available privacy safeguards within those systems) used in Canada at the relevant time, and standard practices, policies and procedures of Canadian health authorities and hospitals regarding the handling of electronic health information, privacy, privacy breach response practices, staff education and training regarding privacy and confidentiality, privacy audits and monitoring access to and use of health information. The court accepted the expert's opinion evidence on the basis that it was logically relevant to deciding the appropriate standard of care, outside the experience and knowledge of the court, and necessary to help the court understand the available options for protecting the privacy of electronic medical records and monitoring access to those records. The court stated:

> *The type of evidence being offered… may not be highly technical or scientific type opinion evidence, but it is a subject matter for which ordinary people are unlikely to form a correct judgment, if unassisted by persons with special knowledge.*

Comment

Studies consistently indicate that a significant portion of cybersecurity incidents originate from, or are facilitated by, a current or former insider (e.g. a director, executive/manager, employee or contract worker) of the affected organization or its business partners. The data breach that gave rise to the *Hynes v. Western Regional Health Authority* lawsuit illustrates how employees can be a major source of cybersecurity and privacy risks. An insider risk management program can help reduce those risks. For more information, see BLG bulletins: *Cyber Risk Management – Insider Risk*; *Insider Risk Management and Rogue Employees*; *Insurance for Cybersecurity Incidents and Privacy Breaches*.

The decision regarding the admissibility of expert opinion evidence in *Hynes v. Western Regional Health Authority* is consistent with the view that effective cybersecurity and privacy protection require a multidisciplinary approach that uses people, processes and technology to identify and mitigate cyber risks and safeguard personal information. For more information, see BLG bulletins: *Cybersecurity Framework for Ontario's Electricity Industry*; *Regulatory Enforcement Action Emphasizes Need for an Information Security Governance Framework*; *Cybersecurity Guidance from Investment Industry Organization*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at blg.com/cybersecurity.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances. Copyright © 2018 Borden Ladner Gervais LLP.

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com