DECEMBER 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Insider Risk Management and Rogue Employees

People are a major security risk. An organization can be vicariously liable for cyber incidents caused by its employees, whether acting negligently or maliciously, even if the organization is not at fault and could not have prevented the incident. An insider risk management program can help reduce, but not eliminate, insider risks. Organizations should establish an insider risk management program, and consider procuring insurance for residual risk.

Insider Risk

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. An organization's insiders present significant risk because they have privileged access to the organization's information technology systems, special knowledge of the organization's valuable data and security practices and a greater window of opportunity for misconduct. Those circumstances often enable insiders to engage in misconduct that is harder to detect and remedy, and results in more harm, than external attacks.

Insiders can cause or facilitate cybersecurity incidents as a result of carelessness or manipulation by other persons. Insiders can also deliberately cause cybersecurity incidents for various reasons. Regardless of whether an insider's acts are deliberate or inadvertent, the potential results can be the same – devastating losses to the organization and significant liabilities on the part of the organization to its customers and other individuals and organizations harmed by the incident.

Effective insider risk management requires a risk-based, multi-functional approach by an organization's various departments and disciplines to deter, prevent, detect and respond to cybersecurity incidents caused by insiders. Insider risk management requires an organization to carefully engage, educate, train and disengage insiders, and to establish and implement administrative, technological and physical security policies and procedures to protect the information technology systems and data of the organization and its relevant business partners and to monitor and verify compliance. For example, see the Canadian Privacy Commissioner's *Ten Tips for Addressing Employee Snooping*.

Timely legal advice can help an organization address legal challenges (e.g. ensuring that risk management practices are lawful and legally effective) presented by insider risk management. For more information about insider risk management, see BLG bulletin *Cyber Risk Management – Insider Risk*.

Rogue Employees

Vicarious Liability

Vicarious liability is a legal doctrine that can result in an organization being liable for the misconduct (including deliberate misconduct) of its employees, even if the organization is not at fault and could not have prevented the misconduct. Vicarious liability is imposed where it is appropriate to hold one person legally responsible for the misconduct of another person because of the relationship between them and the connection between that relationship and the wrongful conduct. The most common relationship to give rise to vicarious liability is the relationship between employer and employee.

Vicarious liability is a form of strict liability because it applies without any fault or other wrongdoing by the person who is subject to it. The doctrine of vicarious liability imposes liability on the basis that the person who establishes an enterprise or authorizes activities should be liable for the harm resulting from the enterprise or activities. Canadian courts have held that vicarious liability should be imposed where: (1) the relationship between a wrongdoer (e.g. an employee) and the person against whom liability is sought (e.g. an employer) is sufficiently close to make vicarious liability appropriate; and (2) the wrongful conduct is sufficiently connected to the wrongdoer's authorized activities so that the wrongful conduct is part of the risk created by the authorized activities. Vicarious liability is intended to achieve two policy objectives: (a) providing a just and fair remedy to persons harmed by misconduct; and (b) deterring future harm by creating an incentive for organizations to minimize the risk of future misconduct.

The doctrine of vicarious liability can make an organization liable for the negligent or inadvertent acts of its employees while performing assigned work. Vicarious liability can also make an organization liable for the intentional misconduct (e.g. assault, sexual abuse, harassment and fraud) of a rogue employee, even where the organization was not at fault and expressly prohibited the misconduct.

Intentional Privacy Breaches

The vicarious liability doctrine has been invoked by Canadian class action plaintiffs to seek to impose liability on a defendant employer for its employee's intentional violation of the plaintiffs' statutory and common law privacy rights. Those cases have not resulted in a final decision after trial. However, preliminary, procedural decisions confirm that the vicarious liability doctrine might apply to an intentional violation of privacy rights. For example, see the British Columbia Court of Appeal decision in *Ari v. I.C.B.C.*, the Ontario Superior Court decision in *Evans v. The Bank of Nova Scotia*, and the Newfoundland and Labrador Supreme Court decision in *Hynes v. Western Regional Integrated Health Authority*.

The vicarious liability doctrine was considered by a Canadian labour grievance settlement board in *Ontario Public Service Employees Union v. Ontario (Ministry of Training, Colleges and Universities)*. The board held that the respondent employer was not vicariously liable for an intentional privacy violation committed by an employee because the violation was not sufficiently related to the employee's assigned work. An appeal from the decision was dismissed.

Recently, the English High Court applied the vicariously liability doctrine to hold the Morrisons supermarket chain liable for an employee's intentional disclosure of highly sensitive personal information of fellow employees. In *Various Claimants v. WM Morrisons Supermarket PLC*, a disgruntled senior IT auditor employed by Morrisons intentionally posted to a file sharing website, and disclosed to three English newspapers, the payroll information of approximately 100,000 current and former Morrisons employees. The rogue employee was motivated by a grudge against Morrisons (due to an earlier internal disciplinary matter), and disclosed the data to cause harm to Morrisons. The rogue employee was convicted of criminal offences and sentenced to eight years' imprisonment. Over 5,000 affected Morrisons employees commenced a class action lawsuit against Morrisons. The court held that Morrisons was not primarily liable for the data breach because Morrisons did not violate the applicable data protection statute or breach any common law duties to the plaintiff employees. Nevertheless, the court held that Morrisons was vicariously liable for its rogue employee's data breach because there was a sufficient connection between the rogue employee's assigned work and his wrongful conduct to make it fair for Morrisons to be held liable to the affected employees. In its judgment, the court referred to the Supreme Court of Canada decision in *Bazley v. Curry*, which explains the modern rationale for vicarious liability under Canadian law. The court concluded its judgment by expressing concern that imposing liability on Morrisons would, in effect, assist the rogue employee to harm Morrisons; and for that reason the court gave Morrisons permission to appeal the court's decision.

The decision in the *Morrisons* case is consistent with the vicarious liability doctrine as interpreted and applied by Canadian courts. The decision illustrates how a Canadian court might hold an organization vicariously liable for a rogue employee's deliberate privacy breach.

Comment – Residual Risk

A suitable insider risk management program can help an organization deter, prevent, detect and respond to insider risks and fulfil its legal obligation to protect sensitive, protected and regulated information (e.g. personal information). It is important to recognize, however, that insider risk, including the risk of deliberate misconduct by rogue employees, cannot be eliminated. The *Morrisons* case illustrates how an organization can be liable for a cybersecurity incident caused by a rogue employee even if the organization has not breached any legal obligation and could not have prevented the incident. For those reasons, organizations should consider procuring insurance for residual cyber risk. ■

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

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