FEBRUARY 2018

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Insurance for Cybersecurity Incidents and Privacy Breaches

Employees and other insiders are a major security risk. A cybersecurity incident or privacy breach caused or facilitated by an organization's insiders can result in significant losses and liabilities. Insurance can be an effective way to help manage insider risk. An organization should obtain appropriate professional advice when making important decisions about privacy and cyber insurance.

Insider Risk

Studies consistently indicate that a significant portion of privacy breaches and other cybersecurity incidents are caused or facilitated by a current or former insider (e.g. an employee or contract worker) of the affected organization or its business partners. An organization's insiders present significant risk because they have authorized 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.

Insiders can cause or facilitate a cybersecurity incident or privacy breach inadvertently – due to carelessness or manipulation by other persons – or deliberately for various motives. Regardless of whether an insider's acts are inadvertent or deliberate, the potential results can be the same – significant losses to the organization and civil lawsuits (including class actions) and liabilities to individuals and organizations harmed by the incident. An insider risk management program can help reduce insider risk. For more information, see BLG bulletin *Cyber Risk Management – Insider Risk*.

Vicarious Liability for Employee Misconduct

An employer can be vicariously liable for a cybersecurity incident or privacy breach caused by an employee's negligent or inadvertent act while performing assigned work or caused intentionally by a rogue employee, even if the employer is not at fault and could not have prevented the misconduct. For example, in the December 2017 decision in *Various Claimants v. WM Morrisons Supermarket PLC*, the English High Court held the defendant Morrisons supermarket chain vicariously liable for a disgruntled rogue employee's deliberate privacy breach that was intended to cause harm to Morrisons. The court held that Morrisons had not breached any legal obligation and could not have prevented the privacy breach. Nevertheless, the court imposed vicarious liability on Morrisons 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 liable to the individuals affected by the privacy breach. For more information, see BLG bulletin *Insider Risk Management and Rogue Employees*.

Insurance for Cyber Incidents and Privacy Breaches

Insurance can be an effective way to help manage the risk of privacy breaches and other cybersecurity incidents caused by insiders. Traditional insurance policies (e.g. commercial liability and commercial crime policies) often do not cover privacy breaches or cybersecurity incidents, either because of narrow policy language or express exclusions. However, most insurance companies offer insurance policies specifically designed to protect an insured against losses and liabilities arising from privacy breaches and cybersecurity incidents.

The protection afforded by an insurance policy depends on the precise language of the policy (e.g. definitions, coverage descriptions, restrictions and exclusions) interpreted in accordance with legal principles established by Canadian courts. In 2017, two Canadian courts considered whether an insurance policy provided coverage for a cybersecurity incident or privacy breach.

Business Email Compromise Scam

In *The Brick Warehouse LP v. Chubb Insurance Company of Canada*, the Alberta Court of Queen's Bench held that a traditional crime coverage policy did not protect the insured against losses resulting from a business email compromise scam that deceived the insured's employee into instructing the insured's bank to transfer funds to a bank account controlled by the cyber-criminal. The insurance policy covered losses resulting from "funds transfer fraud", which the policy defined as "fraudulent … instructions issued to a financial institution directing such institution to transfer, pay or deliver money or securities from any account maintained by an insured at such institution without an insured's knowledge or consent". The court acknowledged that the insured expected the insurance policy to provide protection against loss resulting from criminal action, but reasoned that the policy only covered losses that fell within the restricted coverage set out in the policy. The court held that the circumstances did not constitute "funds transfer fraud", as defined in the policy, because an employee of the insured knowingly issued the funds transfer instructions to the insured's bank.

Privacy Breach by Employee

In *Oliveira v. Aviva Canada Inc.*, the Ontario Superior Court of Justice considered whether a "Professional and General Liability and Comprehensive Dishonesty, Disappearance and Destruction Insurance Policy" purchased by a Canadian hospital required the insurer to defend a hospital employee against a privacy breach lawsuit by a former patient. The patient alleged that the employee, who was not involved in providing care to the patient, breached the patient's privacy by repeatedly accessing the patient's medical records without any legitimate reason. The insurance policy provided coverage to the hospital and its employees for third party claims for "personal injury", which the insurance policy defined broadly as including invasion or violation of privacy, but only for liability "arising from the operations of" the hospital and only for employees "while acting under the direction of" the hospital.

The insurer refused to defend the employee against the privacy breach lawsuit on the basis that the alleged privacy breach did not arise from the "operations" of the hospital and the employee was not "acting under the direction of the hospital" when the employee committed the alleged privacy breach. The insurer argued that the employee abused her position and engaged in unauthorized activities that were unrelated to her employment by the hospital and contrary to her employment obligations. The insurer further argued that the hospital's "operations" were providing healthcare services to patients, and therefore did not include the employee's conduct because the employee was not providing medical care to the patient.

The court rejected the insurer's arguments because they would have excluded a significant portion of the privacy breach coverage that the insurance policy purported to provide. The court applied established legal principles for the interpretation of insurance policies, including: "the duty to defend is broader than the duty to indemnify", "the mere possibility that a claim falls within the policy will suffice to trigger a duty to defend", "coverage provisions should be construed broadly; exclusion causes should be interpreted narrowly" and "courts should avoid interpretations of policies that substantially nullify coverage". The court reasoned that insurance coverage for "invasion or violation of privacy" included the common law tort of "intrusion upon seclusion", which necessarily includes intentional, highly offensive invasions of privacy by employees outside a patient's circle of care. The court followed prior cases that broadly interpreted "acting under the direction of" a named insured and "operations" of a named insured. The court concluded that the insurer was obligated to defend the employee against the privacy breach lawsuit.

Comment

The privacy and cyber insurance market is evolving rapidly. At this time, there is no standard form language used in privacy breach and cyber insurance policies, and there can be significant differences in the coverage provided by similar kinds of policies. For those reasons, an organization should obtain advice from a lawyer and an experienced insurance consultant when applying for privacy and cyber insurance, when assessing the costs and benefits of various kinds of privacy and cyber insurance, and when determining whether an existing insurance policy provides coverage for a privacy breach or cybersecurity incident. ■

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