Insurance as a cybersecurity and privacy risk management tool

October 19, 2021

While organizations primarily manage cybersecurity and privacy risks through practices, policies and procedures, organizations often look to manage residual risks through insurance. Two recent Canadian cases illustrate how traditional insurance policies might provide limited or no coverage for losses and liabilities resulting from cybersecurity and privacy incidents.

Organizations that seek to manage residual cybersecurity and privacy risks through insurance should seek expert advice to ensure that the scope and amounts of insurance coverage are adequate to meet their requirements.

Cybersecurity and Privacy Risks

Cybersecurity risks are risks of losses and liabilities suffered or incurred by an organization resulting from a failure or breach of the information technology systems and data used by, or on behalf of, the organization or its business partners. Privacy risks are risks of losses and liabilities suffered or incurred by an organization resulting from incidents that affect the security, confidentiality, integrity or availability of personal information in the organization's possession or under the organization's legal control. These losses and liabilities may include, for example, financial losses, business disruptions, reputational harms, trade secret disclosures, response and remediation costs, and litigation/regulatory proceeding costs.

Cybersecurity and privacy risks can result from internal sources (e.g., employees, contract workers and system failures) or external sources (e.g., hackers, fraudsters and acts of nature). Cybersecurity and privacy risks are relevant to almost any organization, regardless of size or industry, because almost all organizations use or depend on information technology systems and data, including personal information of employees and customers, to operate their business.

Recent Insurance Coverage Cases

Two recent Canadian cases illustrate how traditional insurance policies provide limited or no coverage for losses and liabilities resulting from cybersecurity and privacy incidents.

Hackers Post Confidential Report on Social Media

Family and Children's Services of Lanark, Leeds and Grenville v. Co-operators General Insurance Company (2021, Ontario Court of Appeal) (Family and Children's Services of *Lanark*) involved a dispute over whether an insurance company had a duty to defend two insureds against claims resulting from the unauthorized posting on social media of a report containing the personal information of 285 individuals. Unidentified hackers stole the report from the website portal of a social services society. The affected individuals commenced a $75 million class action against the social services society for defamation and negligently securing its website. The social services society initiated a third party claim for indemnity against its IT service provider for alleged breach of contract and negligence in performing services regarding the website.

The social services society and its IT service provider were insured under commercial general liability insurance and professional liability insurance policies issued by the same insurer. The two insureds claimed that the insurer had a duty to defend them in the class action and the third party claim. The insurer refused to defend the claims on the basis that both insurance policies had "data exclusion" clauses that excluded coverage for claims "arising out of the distribution, or display of 'data' by means of an Internet Website". The social services society and its IT service provider brought court applications for a declarations that the insurer had a duty to defend the claims.

While the applications judge held that the insurer had a duty to defend the social services society and its IT service provider, on appeal, the Ontario Court of Appeal held that the insurer did not have a duty to defend the claims. The Court of Appeal held that the data exclusion clauses were clear and unambiguous and applied to both the class action and the third party claims because the substance and true nature of the claims arose from the wrongful posting of the report on social media, which constituted a distribution or display of data by means of an Internet Website. The Court of Appeal reasoned that the data exclusion clauses were consistent with the main purpose of the insurance policies, did not nullify the coverage under the insurance policies and were not contrary to the reasonable expectations of the parties.

Social Engineering Fraud

Future Electronics Inc. (Distribution) Pte Ltd. c. Chubb Insurance Company of Canada (2020, Québec Superior Court) (*Future Electronics Inc.*) involved a dispute over the amount of coverage that a crime insurance policy provided for losses resulting from a fraudulent scheme. The fraudulent scheme involved emails, telephone calls and letters, purported to be from representatives of a supplier, which requested that the insured make payments of the supplier's invoices to a new bank account, which was controlled by the fraudsters. The fraudulent scheme deceived the insured's employees into giving instructions to its bank to make payments totaling nearly US$2.7 million to the fraudsters' bank account.

The insured claimed full indemnity for its losses under a crime insurance policy on the basis of policy provisions that described coverage for "Computer Fraud by a Third Party"

or “Funds Transfer Fraud by a Third Party”. The insurer refused to provide full indemnity on the basis that the losses suffered were covered by a “Social Engineering Fraud” endorsement that provided limited coverage of US$50,000.

The Québec Superior Court held that the losses resulting from the fraudulent scheme did not fall within the coverage for either “Computer Fraud by a Third Party” or “Funds Transfer Fraud by a Third Party” because both kinds of coverage were limited by definitions and exclusions in the policy. The Court held that coverage for “Computer Fraud by a Third Party” did not apply because the fraudsters did not unlawfully take any funds from the insured by means of a computer system. The Court held that coverage for “Funds Transfer Fraud by a Third Party” also did not apply because the fraudsters did not issue fraudulent wire transfer instructions to the insured’s bank without the insured’s knowledge or consent. In addition, the Court held that coverage would have been precluded by a clause that expressly excluded coverage for losses due to the insured knowingly giving money to a third party.

The Court agreed with the insurer that the insured’s losses were covered by the “Social Engineering Fraud” endorsement. The Court reasoned that the insured’s losses corresponded precisely to the social engineering fraud scenario contemplated by the “Social Engineering Fraud” endorsement. The Court held that an exclusion in the crime insurance policy precluded double coverage under both the “Social Engineering Fraud” endorsement and either the “Computer Fraud by a Third Party” provision or the “Funds Transfer Fraud by a Third Party” provision.

In the result, while the insured suffered losses of approximately US$2.7 million, the coverage provided by the crime insurance policy was limited to the US$50,000 limit of the “Social Engineering Fraud” endorsement.

Comment

The recent decisions in Family and Children’s Services of Lanark and *Future Electronics Inc*. illustrate how traditional insurance policies might provide limited or no coverage for losses and liabilities resulting from cybersecurity and privacy incidents, even though the insurance policies describe coverage in broad terms. Therefore, organizations that seek to manage cybersecurity and privacy risks through insurance should consider purchasing specific cybersecurity and privacy breach insurance with adequate coverage limits.

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

By

Danielle Windt

Expertise

Cybersecurity, Privacy & Data Protection, Insurance

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749