APRIL 2018

CYBERSECURITY BULLETIN

Borden Ladner Gervais

U.S. Financial Institution Regulators Issue Guidance About Cyber Insurance

On April 10, 2018, the United States Federal Financial Institutions Examination Council ("FFIEC") issued guidance for financial institutions considering the purchase of cyber insurance to help manage cyber risks. The guidance is helpful for Canadian financial institutions and organizations in other industries.

Cyber Risks

Cyber risks are risks of harm (e.g. business disruption loss, financial loss, reputational harm, trade secret disclosure and other competitive harm) and costs/liabilities (e.g. incident response and remediation costs, litigation/regulatory proceeding costs, and liabilities to stakeholders, business partners, customers and regulators) suffered or incurred by an organization as a result of a failure or breach of the information technology systems used by or on behalf of the organization or its business partners (e.g. suppliers and service providers), including incidents involving unauthorized access, use, disclosure, modification or deletion of data in the organization's possession or control. Cyber risks can result from internal sources (e.g. employees, contract workers and system failures) or external sources (e.g. nation-states, terrorists, competitors, hackers, fraudsters, and acts of nature).

Cyber risk are relevant to almost any organization, regardless of the organization's size or industry, because almost all organizations use or depend on information technology and data to operate their business. Cyber risks appear to be increasing in frequency, intensity and harmful consequences as a result of various circumstances, including: increasing use of, and dependency on, information technology and data; increasing sophistication and complexity of cyber-attacks; and evolving legal requirements and liabilities. Commentators have said that there are only two kinds of organizations – those that have been hacked and know it, and those that have been hacked and don't know it yet.

Cyber Insurance

Insurance can be an effective way to help manage cyber risks. Traditional insurance policies (e.g. commercial liability, business disruption and commercial crime policies) often do not cover losses and liabilities resulting from cybersecurity incidents, either because of narrow policy language or express exclusions. Most insurance companies offer insurance policies specifically designed to protect against losses and liabilities arising from 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 established legal principles. Canadian courts recently considered whether an insurance policy provided coverage for a cybersecurity incident or privacy breach. See BLG bulletin *Insurance for Cybersecurity Incidents and Privacy Breaches*.

FFIEC Guidance

The FFIEC, on behalf of its members (the principals of the Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee), issued on April 10, 2018, a joint statement titled *Cyber Insurance and Its Potential Role in Risk Management Programs* to provide guidance regarding the potential role of cyber insurance in financial institutions' cyber risk management programs.

The statement emphasizes that cyber insurance does not remove the need for financial institutions to have sound operational risk management practices, and warns against overreliance on insurance as a substitute for those practices. The statement acknowledges that while cyber insurance may be a component of a broader cyber risk management strategy, an effective system of controls remains the primary defense against cyber threats.

Following is a summary of some of the important background information and guidance in the statement:

- Financial institutions of all sizes are affected by the increasing number and sophistication of cyber incidents.
- Financial institutions face a variety of cyber risks, including financial, operational, legal, compliance, strategic, and reputation risks resulting from fraud, data loss, or disruption of service.
- Traditional insurance policies (e.g. general liability or basic business interruption insurance) might not provide effective coverage for cyber risks.
- FFIEC members do not require financial institutions to maintain cyber insurance. Nevertheless, cyber insurance might offset some of the financial losses caused by cyber incidents that are not covered by traditional insurance policies.

- The cyber insurance marketplace is growing and evolving in response to changing cyber risks, and cyber insurance coverage options vary greatly.
- Understanding the scope of coverage provided by a cyber insurance policy is critical for making an informed risk management decision.
- If a financial institution is considering procuring cyber insurance, an assessment of cyber insurance benefits should include an analysis of the institution's existing cybersecurity and information technology risk management programs to evaluate the potential financial impact of residual risk.
- A financial institution's decision whether to purchase cyber insurance should be made with input from appropriate departments across the institution (e.g. legal, enterprise risk management, operational risk management, finance, information technology and information security management), and should be reported to the appropriate level of management.
- A financial institution's decision to purchase cyber insurance should be based on proper due diligence, with the assistance of outside advisors (e.g. lawyers and insurance brokers), to assess the potential benefits and costs of insurance coverage options. Due diligence should include: (1) review existing or proposed insurance coverage to identify gaps; (2) understand insurance policy terms, coverage, exclusions and costs; (3) consider the potential benefits and costs to assess the insurance coverage appropriateness; (4) recognize that policy terms and language may not be standardized, and that coverage may be different among insurance providers and tailored for institutions; (5) consider how coverage is triggered, the types of cyber incidents excluded from coverage, and the impact of sub-limits on the total coverage and claims process; (6) assess the financial strength and claims paying history of the insurance companies providing coverage and their ability to fulfill their policy obligations if multiple institutions file claims; (7) assess how the insurance coverage fits within the institution's business strategies, insurance programs, and risk management programs; and (8) understand the risk management and control requirements outlined in the insurance policy and ensure that the institution is able to comply with those requirements.
- A financial institution, with appropriate involvement of its board of directors, should evaluate annually its existing cyber insurance coverage (e.g. costs/benefits, sufficiency and effectiveness) relative to evolving cyber risks and threats, the availability of other insurance products and the institution's expectations.

Comment

Insurance can be an effective way for organizations of all kinds and sizes to help manage cyber risks. However, insurance is only one component of a cyber risk management program, and is not a substitute for appropriate operational cyber risk management practices. Moreover, failure to establish and following adequate cyber risk management practices might constitute a breach of the conditions for coverage outlined in the insurance policy and vitiate coverage.

An organization that is purchasing cyber insurance, or evaluating its current cyber insurance, should consider the FFIEC's guidance and obtain appropriate advice and assistance so that the organization's decision is properly informed. In addition, the organization should carefully document its decision-making process for future reference, including use in regulatory investigations and legal proceedings. ■

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