Internet and E-Commerce Law in Canada

Editor-in-Chief: Professor Michael A. Geist, Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law

VOLUME 14, NUMBER 9 Cited as (2013-14) 13 I.E.C.L.C. JANUARY 2014

• CYBER SECURITY CONSIDERATIONS FOR PUBLIC COMPANIES •

Simon Hodgett, *Partner*, Sam Ip, *Articling Student*,
and Janet Salter, *Knowledge Management Lawyer, Corporate*
Osler, Hoskin & Harcourt LLP

Recent developments, including a barrage of cyber attacks and revelations related to state-sponsored monitoring of electronic systems, have resulted in heightened interest by businesses and regulators about cyber security. The threat is real. Business relies increasingly on information technology, and that reliance extends to the Internet in numerous ways: through product offerings, maintenance of customer lists, processing of payment card information, and the increasing transfer of data and intellectual property (formerly residing internally) to hosted or cloud-based locations.

In response to the perceived cyber security threats to public companies, the Canadian Securities Administrators (CSA) has recently published for comment *CSA Staff Notice 11-326*, "Cyber Security" ("CSA Notice").[1] This CSA Notice follows a recent report issued by the International Organization of Securities Commissions and the World Federation of Exchanges, highlighting the risk of a major cyber attack on key elements of the financial markets' infrastructure.

The CSA Notice is not restricted to the cyber security concerns of public companies but also addresses concerns for registrants and for regulated entities such as self-regulatory organizations, marketplaces, and clearing agencies (together, "Market Participants").

The CSA Notice states that strong and tailored cyber security measures are an important element of Market Participants' controls to ensure both the reliability of their operations and the protection of confidential information. The CSA Notice states that to manage the risks of a cyber threat, Market Participants

> should be aware of the challenges of cyber crime and should take the appropriate protective and security hygiene measures necessary to safeguard themselves and their clients or stakeholders.[2]

The regulators suggest that Market Participants consider taking specific measures, including the following:

- educating staff on the importance of the security of the firm's and clients' information, and the staff's role in ensuring such safety
- following guidance and best practices of industry associations and recognized information security organizations
- conducting regular third-party vulnerability and security tests and assessments

As a result, senior management and boards of directors should institute active and sustained programs to implement specific and tailored measures and plans to satisfy the CSA Notice. These measures include establishing reporting to ensure that recognized security standards are implemented, promoting transparency within the organization to ensure that management understands and can effectively monitor risk of cyber security events occurring, and defining a clear set of procedures to limit damage should such events occur.

Similarly, on October 13, 2011, the U.S. Securities and Exchange Commission published the *CF Disclosure Guidance: Topic No. 2*[3] to provide guidance on disclosure obligations relating to such risks. While no disclosure requirement in securities legislation explicitly refers to cyber security risks, the U.S. federal securities law is premised on comprehensive, timely, and accurate disclosure. Consequently, the guidance requires material cyber security risks to be disclosed if doing so would influence the decision of a reasonable investor or, if such risks are not disclosed, would make other required disclosures misleading.

As a result of the real threats to cyber security that public companies are facing, and in light of the initiatives by regulators in Canada, the United States, and internationally, senior management and boards of directors must now carefully consider the company's cyber security readiness.

[*Editor's note*: **Simon Hodgett's** practice concentrates on corporate and commercial matters relating to technology and complex services arrangements. He advises software developers, service providers, and companies whose business relies on technology.

Janet Salter's responsibilities include monitoring legal and industry developments and providing the relevant information and resources to the department, the firm, and the firm's clients; supporting the department's business development activities including acting as editor of the *Osler Corporate Review* and the *Capital Markets Report*; and training and mentoring department members.]

1. <http://www.osc.gov.on.ca/documents/en/Securities-Category1/csa_20130926_11-326_cyber-security.pdf>.
2. *Ibid.*
3. <http://www.sec.gov/divisions/corpfin/guidance/ cfguidance-topic2.htm>.