NOVEMBER 2013

INFORMATION TECHNOLOGY BULLETIN

Borden Ladner Gervais

REGULATORY GUIDANCE FOR CYBER RISK SELF-ASSESSMENT

Canadian financial regulators have issued guidance for the self-assessment of cyber security practices. The guidance emphasizes the need for senior management to comprehensively review cyber risk management policies and procedures, and provides a detailed self-assessment template. All organizations can benefit from the regulatory guidance.

On October 23, 2013, the Office of the Superintendent of Financial Institutions of Canada (known as "OSFI") issued a memorandum entitled "Cyber Security Self-Assessment Guidance" (online: www.osfi-bsif.gc.ca/app/DocRepository/1/eng/notices/osfi/cbrsk_e.pdf) to assist federally regulated financial institutions ("FRFIs") in the self-assessment of their preparedness for cyber attacks.

The memorandum explains that OSFI expects a FRFI's senior management to review their institution's cyber risk management policies and practices to ensure that they remain appropriate and effective in light of changing circumstances and risks. The memorandum also indicates that a FRFI's board of directors, or committee of the board, should regularly review and discuss the institution's cyber risk management practices.

The memorandum includes a detailed self-assessment template that covers the following broad areas: (1) organization and resources; (2) cyber risk and control assessment; (3) situational awareness; (4) threat and vulnerability risk management; (5) cyber security incident management; and (6) cyber security governance. The template explains that the self-assessment should focus on the institution's current state of cyber security practices on an enterprise-wide basis, and should include the institution's material outsourcing arrangements (as defined by OSFI's Guideline B-10) and critical IT service providers (including related subcontracting arrangements).

The memorandum encourages FRFIs to use the self-assessment template to assess their current level of preparedness for cyber attacks and to develop and maintain effective cyber security practices. The memorandum also notes that OSFI might request FRFIs complete the template during future supervisory assessments.

Cyber attacks are an increasing risk for many kinds of organizations. OSFI's memorandum, while directed to financial institutions, is a useful reminder and a helpful tool for any organization that wishes to establish and maintain effective cyber security practices.

To find out more, please contact the BLG Technology Law Group – www.blg.com/ITGroup

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

Author
Bradley J. Freedman
T 604.640.4129
F 604.622.5829
bfreedman@blg.com