CSA/ACVM Canadian Securities Administrators Autorités canadiennes en valeurs mobilières

CSA Staff Notice 11-326
Cyber Security

September 26, 2013

Strong and tailored cyber security measures are an important element of issuers', registrants' and regulated entities'[1] controls in promoting the reliability of their operations and the protection of confidential information. The risk of a major cyber attack on key Financial Market Infrastructure (FMI) has been highlighted by the International Organization of Securities Commissions (IOSCO) and the World Federation of Exchanges (WFE) in a recent report issued July 16, 2013.[2]

The IOSCO report defines cyber crime as *"a harmful activity, executed by one group (including both grassroots groups or nationally coordinated groups) through computers, IT systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity."* Although cyber threats have existed in the past, more recently two major types of cyber threats, Denial of Service (DoS) attacks and Advanced Persistent Threats (APT), have increased in frequency and sophistication.

To manage the risks of a cyber threat, issuers, registrants and regulated entities 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.

Specifically:

- Issuers, registrants and regulated entities who have not considered the risks of cyber crime to date should consider how they can best address the risks of cyber crime. Steps they could take include:
    - educating staff on the importance of, and their role in, ensuring the security of their firm's and client information and computer security;
    - following guidance and best practices from industry associations and recognized information security organizations; and
    - as appropriate, conducting regular third party vulnerability and security tests and assessments.
- Issuers, registrants and regulated entities that have already taken steps to address the issue should review their cyber security risk control measures on a regular basis.

[1] Regulated entities include self-regulatory organizations, marketplaces, clearing agencies and information processors.
[2] "Cyber-crime, securities markets and systemic risk", joint staff working paper of the IOSCO Research Department and World Federation of Exchanges, July 16, 2013.

Issuers should consider whether the cyber crime risks to them, any cyber crime incidents they may experience, and any controls they have in place to address these risks, are matters they need to disclose in a prospectus or a continuous disclosure filing.

Registrants should consider whether their risk management systems allow them to manage the risks of cyber crime in accordance with prudent business practices.

Regulated entities, especially those that are key market infrastructure entities, should consider the measures necessary to manage the risks of cyber crime.

Future Action

The CSA will consider these issues in its reviews of issuer disclosure and in its oversight of registrants and regulated entities.

Questions and comments

Questions and comments may be referred to:

Noreen C. Bent
Manager, Corporate Finance Legal Services
British Columbia Securities Commission
604-899-6741
nbent@bcsc.bc.ca

Tom Graham
Director, Corporate Finance
Alberta Securities Commission
403-297-5355
tom.graham@asc.ca

Samad Uddin
Senior Economist, Strategy and Operations Branch
Ontario Securities Commission
416-204-8950
suddin@osc.gov.on.ca

Leslie Byberg
Acting Director, Strategy and Operations Branch
Ontario Securities Commission
416-593-2356
lbyberg@osc.gov.on.ca

Élaine Lanouette
Director, Exchanges and SROs
Autorité des marchés financiers
514-395-0337 ext. 4321
elaine.lanouette@lautorite.qc.ca

Kevin Hoyt
Director, Securities
Financial and Consumer Services Commission (New Brunswick)
506-643-7691
kevin.hoyt@fcnb.ca