British Columbia Securities Commission

Timely Tips

Cyber security – Are you managing the risks?

Questions to ask about cyber security

How vulnerable to cyber-attack are you or your clients? Would you, or your custodian or other service providers, be able to detect when a client's e-mail account (or yours) is compromised by an imposter? How do you assess the authenticity of e-mail communications with clients?

Why the concern?

We have become aware of instances when registrants unknowingly enabled fraud stemming from e-mail account invasions. This type of cyber-attack involves:

- a client's compromised e-mail account
- fraudsters monitoring e-mail habits and then posing as the client to:
  - request redemptions (often instructing the funds be sent to other countries)
  - trade in securities to create false and misleading trading volumes
- a recipient not obtaining verbal confirmation of instructions

Cyber-attacks through client e-mail accounts are surfacing at firms of all sizes, even the larger firms with the ability to dedicate resources (both human and financial) to these issues. Smaller firms with fewer resources may be at increased risk.

Cyber security threats are constantly changing. Your vigilance is required to reduce the risks.

What do regulators expect?

Managing cyber security risks are part of your regulatory responsibilities under section 11.1(b) of National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations.*

We suggest that you:

- recognize this is an issue facing your firm and every firm
- create and enforce strict policies about receiving and verifying e-mail instructions. For example, you should require that your staff follow up on all e-mail instructions **directly by phone or in person** with the client, using the contact information in the client file…not in the e-mail
- ensure your custodian and other service providers have equivalent, or better, policies and practices
- seek outside cyber security expertise to assess your risks if you do not have adequate in-house resources. Solutions such as antivirus programs and firewalls may not, in themselves, be adequate
- perform regular risk assessments to ensure you are proactively managing these risks

You may want to check out other information about this subject: CSA Staff Notice 11-326 *Cyber Security* and a recent Investment Executive article

If you have questions, contact your relationship manager at BCSC.

February 2015