

# Cybersecurity Guidance From Investment Industry Organization

12 janvier 2016

Cyber risk management is an increasingly important challenge for organizations of all kinds. The Investment Industry Regulatory Organization of Canada (IIROC), the national self-regulatory organization that oversees investment dealers and their trading activity in Canadian markets, has published detailed guidance to help investment dealer firms manage cybersecurity risks. The guidance provides useful checklists and helpful summaries of industry standards and best practices. The guidance emphasizes the need for organizations to proactively manage cyber risks and to prepare for cybersecurity incidents.

## Cyber Risks

Cyber risks are the risks of harm, loss and liability (e.g. business disruption, trade secret disclosure, financial loss, loss to stakeholder value, reputational harm, legal noncompliance liability and civil liability to customers, business partners and other persons) to an organization resulting from a failure or breach of the organization's information technology systems. Cyber risks can result from internal sources (e.g. employees, contractors, service providers and suppliers) or external sources (e.g. nation states, terrorists, hacktivists, competitors and acts of nature).

Cyber risks appear to be increasing in frequency, intensity and harmful consequences as a result of various circumstances, including increasing sophistication and complexity of cyber-attacks, increasing use of information technology and data, increasing regulation and increasing legal liability. 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.

## Cybersecurity Best Practices Guide

IIROC's Cybersecurity Best Practices Guide sets out a voluntary, risk-based cybersecurity framework, comprised of industry standards and best practices, to manage cyber risks. The Guide's stated purpose is to provide an understanding of standards-based security controls that make up a best practices cybersecurity program. The Guide emphasizes that cybersecurity is a multi-faceted challenge that requires an

enterprise-wide, interdisciplinary approach to implement a comprehensive strategy to avoid, mitigate, accept or transfer cyber risks.

The Guide discusses best practices relating to governance and risk management, insider risk, physical and environmental security, awareness and training, threat assessment, network security, information system protection, user management and access controls, asset management, incident response, information sharing and breach reporting, cyber insurance, vendor risk management and cybersecurity policies. The Guide includes a Cybersecurity Incident Checklist and a Sample Vendor Assessment form.

The Guide identifies the following key points:

- **Governance** : A sound governance framework – strong leadership, board and senior management engagement and a clear accountability – are essential for a successful cybersecurity program.
- **Training** : Effective training of personnel can significantly reduce the likelihood of successful cyber-attacks.
- **Technical Controls** : A cyber risk management program should include technical controls appropriate for the organization's particular circumstances.
- **Service Providers** : An organization should exercise strong due diligence and implement clear performance and verification policies to manage cyber risks that arise from relationships with service providers who have access to the organization's sensitive firm or client information or information technology systems.

## Cyber Incident Management Planning Guide

IIROC's Cyber Incident Management Planning Guide is designed to assist in the preparation of cyber-incident response plans. The Guide emphasizes that an organization must be able to respond to cybersecurity incidents in a consistent, coordinated and timely manner. The Guide explains the five phases of cybersecurity incident management: plan and prepare, detect and report, assess and decide, respond and post-incident activity. The Guide includes recommendations (based on the National Institute of Standards and Technology Computer Security Incident Handling Guide) for implementing a cybersecurity incident response plan. The Guide also includes a simple, ten-step guide for how an organization should respond to a cybersecurity incident when the organization is not prepared.

## Comment

IIROC's cyber risk management guidance is described as "voluntary", and "not intended to create new legal or regulatory obligations". Nevertheless, guidance issued by IIROC and other financial industry organizations and regulators (e.g. SEC, FINRA, CSA and OSFI) will likely be considered by courts and regulators when determining the reasonable standard of care required of an investment dealer firm that is the victim of a cybersecurity incident. IIROC's guidance, while directed to investment dealer firms, can be helpful for organizations of all kinds.

[Bradley Freedman](#)

## Services

[Cybersécurité, respect de la vie privée et protection des renseignements personnels, Technologies](#)

---

## BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

[blg.com](http://blg.com)

## Bureaux BLG

### Calgary

Centennial Place, East Tower  
520 3rd Avenue S.W.  
Calgary, AB, Canada  
T2P 0R3

T 403.232.9500  
F 403.266.1395

### Ottawa

World Exchange Plaza  
100 Queen Street  
Ottawa, ON, Canada  
K1P 1J9

T 613.237.5160  
F 613.230.8842

### Vancouver

1200 Waterfront Centre  
200 Burrard Street  
Vancouver, BC, Canada  
V7X 1T2

T 604.687.5744  
F 604.687.1415

### Montréal

1000, rue De La Gauchetière Ouest  
Suite 900  
Montréal, QC, Canada  
H3B 5H4

T 514.954.2555  
F 514.879.9015

### Toronto

Bay Adelaide Centre, East Tower  
22 Adelaide Street West  
Toronto, ON, Canada  
M5H 4E3

T 416.367.6000  
F 416.367.6749

Les présents renseignements sont de nature générale et ne sauraient constituer un avis juridique, ni un énoncé complet de la législation pertinente, ni un avis sur un quelconque sujet. Personne ne devrait agir ou s'abstenir d'agir sur la foi de ceux-ci sans procéder à un examen approfondi du droit après avoir soupesé les faits d'une situation précise. Nous vous recommandons de consulter votre conseiller juridique si vous avez des questions ou des préoccupations particulières. BLG ne garantit aucunement que la teneur de cette publication est exacte, à jour ou complète. Aucune partie de cette publication ne peut être reproduite sans l'autorisation écrite de Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Si BLG vous a envoyé cette publication et que vous ne souhaitez plus la recevoir, vous pouvez demander à faire supprimer vos coordonnées de nos listes d'envoi en communiquant avec nous par courriel à [desabonnement@blg.com](mailto:desabonnement@blg.com) ou en modifiant vos préférences d'abonnement dans [blg.com/fr/about-us/subscribe](http://blg.com/fr/about-us/subscribe). Si vous pensez avoir reçu le présent message par erreur, veuillez nous écrire à [communications@blg.com](mailto:communications@blg.com). Pour consulter la politique de confidentialité de BLG relativement aux publications, rendez-vous sur [blg.com/fr/ProtectionDesRenseignementsPersonnels](http://blg.com/fr/ProtectionDesRenseignementsPersonnels).

© 2025 Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Borden Ladner Gervais est une société à responsabilité limitée de l'Ontario.