Fidelity

FIDELITY CLEARING CANADA®

Cyber risk management roundup for investors: the Fidelity perspective

It's an uncomfortable truth that you can't afford to ignore: Cybercriminals may be targeting your firm's — and your customers'— privacy, information, and wealth.

Cyber fraud is on the rise. Massive data breaches combined with increased use of online services and digital devices (11+ billion worldwide!) have made it easier for cybercriminals to execute successful attacks.

Today's cybercriminals use an array of tools and techniques to breach victims' security and monetize their access.

Firms have responsibilities; federal and provincial regulations, as well as specific industry regulations may require financial institutions to implement controls to prevent identity theft. Take action to protect your customers and firm. While threats have intensified, adopting fundamental cybersecurity practices still goes a long way toward mitigating these risks.

Let's take look at some recent thought leadership from Fidelity around the world on cybersecurity. These articles will give you tips to safeguard your customers and your firm from cybersecurity risks and fraud.

Fidelity

FIDELITY CLEARING CANADA®

The insights in these white papers are gathered from research done by Fidelity security specialists in the U.S. Keep in mind that the tips and insights within these papers are intended to help you mitigate risk and are not intended as legal advice. There are many considerations to think about when developing information security policies and procedures. It is advisable to consult legal counsel and/or other professional advisors with whom you work.

Note: Links open previously published source content from our U.S. counterparts, in its original language.

Advisory firms: are your cyber risk management policies and procedures keeping up?

Summary:

This piece, written by Fidelity security specialists in the U.S, describes how firms can protect their customers in the environment of evolving and severe cybersecurity threats. Note that this piece mentions regulations and laws that pertain to businesses in the U.S.

In Canada, financial institutions may fall under privacy laws and specific industry regulations, or guidelines. For instance, the Office of the Superintendent of Financial Institutions (OSFI) primarily issues guidelines and expectations for federally regulated financial institutions rather than enacting specific legislation.

Similarly, the Canadian Investment Regulatory Organization (CIRO), the national self-regulatory organization that oversees all investment dealers, mutual fund dealers and trading activity on Canada's debt and equity marketplaces also has guidelines to ensure the cybersecurity and business continuity of members.

Additionally, provincial securities commissions, such as the Ontario Securities Commission (OSC) may issue regulations, guidelines, and

expectations that pertain to the areas of cybersecurity and business continuity requirements.

And lastly, many financial services firms will require their organization to have in place key cybersecurity and business continuity requirements.

The type of specific cybersecurity and business continuity guidelines and/or legislation you need to adhere to will depend on the type of business you operate, and what regulator bodies your business may be governed by.

Work with your I.S. or I.T. department to develop a security strategy or seek out the services of an information security company to develop a plan to keep your customers' data safe. Review your plan regularly to ensure that it reflects emerging current regulations, emerging cyber threats, and best practices in the field of software and security protection.

Learn more about how firms can protect data from cyber fraud and recommended actions for firms to consider.

Help your customers master cyber risk management

Summary:

How well are you helping your customers protect their investments from the scourge of cybercrime? Fidelity's Cyber Fraud Investigations Team has put together an essential guide to share with investors to help them bolster their accounts and data. Their guide covers:

- Using a password manager to keep track of passwords
- Steps for protecting financial accounts (including mobile and email accounts)
- How to protect computers, tablets, and mobile devices from malicious software
- Ensuring secure access to social media accounts using multi-factor authentication for extra log-in protection

FIDELITY CLEARING CANADA®

- Implementing a credit freeze as a preemptive step to protect yourself from the impact of identity theft
- Tips for spotting scams
- What to do if you think you've been compromised

At Fidelity Clearing Canada, security is at the core of our everything we do. We adhere to a robust combination of operational, cyber, and physical controls to protect our clients' assets and personal information. We work closely with brokerage firms and portfolio managers to help them understand evolving cybersecurity threats and make better-informed portfolio decisions, safely. And our best-practice digital business platform ensures everyone – from advisors to end-investors – stays on the leading edge of technology and innovation. For less do, and more u.

Let's mind your business.

Learn more about Fidelity Clearing Canada here.

Follow us on LinkedIn here.