As new and evolving technologies continue to disrupt the financial sector, Canadian consumers are putting pressure on financial institutions (FIs) to deliver innovation without compromising security.

They are becoming more aware of the risks associated with sharing their personal information and demanding increased transparency on how it is used by their financial service providers. As noted in KPMG’s 2019 report *Me, My Canadian Life, My Wallet*, less than 60 percent of Canadians trust banks with their payment data while, at the same time, they expect the convenience and value of cutting-edge solutions from their FIs.

FIs are responding to the challenge. From back office processes to insightful data analytics and mobile banking tools, today’s leaders are using a broad range of innovations to change the way they deliver value to their clients.

Moreover, FIs are often partnering with smaller, less established, innovative fintechs to stay competitive and be first-to-market with sought-after products and services. While these partnerships can help organizations appeal to consumers, they can introduce additional cyber risk and potentially expose the FI to privacy regulation non-conformity if not managed appropriately.

With cyber incidents on the rise and the level of sophistication increasing, FIs need to address the challenges posed by increased reliance on new technology, information sharing across platforms and between organizations, partnerships with less mature firms, and evolving regulation around personal information.

This requires focus in several key areas.

**Align cyber security with broader risk management strategies**

As digital transformation introduces new risks to FIs, leaders are recognizing that responsible security investment and risk-informed decision making can help safeguard the business and build consumer confidence. In an effort to accelerate their business, protect their sensitive information, and build trust, FIs need to balance innovative technologies with risk-mitigating investments in security.

By aligning cyber security efforts with broader enterprise risk management, organizations are able to define priorities, gauge program effectiveness, and guide security investment. This alignment will also serve to improve an FIs preparedness for the upcoming third-party information risk challenges, that will be introduced through incoming changes, to the digital ecosystem, such as Canada’s move to open banking.

Canadian FIs are able to build consumer and shareholder trust by discussing cyber risk in business terms rather than in technical terms, making their risk mitigation strategies accessible to a broader audience. To do this, many FIs are looking to their security and risk management teams to provide regular cyber risk reports which tie the internal, external, technology, and regulatory elements of the threat landscape to business impacts. These can include operational, financial, reputational, and legal consequences, which can meaningfully impact the business.

**Let regulations guide good practice and build customer**

Canadian FIs are facing increased pressure to meet evolving cyber security and privacy regulatory requirements across jurisdictions and demonstrate compliance.

Here at home, PIPEDA (Personal Information Protection and Electronic Documents Act) provides guidance and requirements on the handling of personal information in the private sector, while in the EU the robust and wide-reaching GDPR (General Data Protection Regulation) sets out the standards for handling EU citizens’ data. Non-compliance can carry significant consequences, including hefty fines, prompting FIs to closely monitor changes to regulation.

The rise of fintech partnerships has led FIs to share more information across platforms, organizations, and geographies, presenting data residency and use challenges in light of stringent regulation.
As high profile breaches continue to shine a light on potential cyber concerns for consumers, regulatory requirements are often looked to as a benchmark to contextualize what ‘good practice’ looks like in terms of securing, sharing, and using personal and financial information. When organizations can show the public they are acting in accordance with relevant legislation and rules, they are demonstrating to their clients that they are treating their information responsibly.

Proactive and transparent reporting on compliance at a high level can help FIs reassure shareholders and consumers that they can be trusted to manage personal and financial information.

**Streamline third-party risk management programs**

Building relationships with government, industry associations, and peers can provide valuable insights into common threats. In some cases, these relationships can provide formal or informal incident response alliances. This trend was borne out in our 2019 Canadian CEO Outlook which found the majority of CEOs are looking to strategic alliances to help them tackle a range of issues; notably, cyber security.

Partnerships can also help FIs bring innovative solutions to market quickly and responsibly. By partnering with smaller, more agile fintechs, established FIs are able to remain competitive and move beyond more traditional, slower sources of innovation, such as internal incubators or outsourced vendors. Recent examples of these types of collaborations include TD partnering with MCST, RBC with Wave, and CIBC with Borrowell. Each of these examples showcases an opportunity for a fintech to broaden its reach and leverage the trust Canadians have in established consumer banks, while providing those banks with the agility and innovation that clients are demanding.

To ensure successful partnerships with fintechs, FIs need to have robust onboarding and responsible, streamlined third-party risk management programs that allow collaborations to be thoroughly vetted without being unnecessarily lengthy or burdensome for smaller firms. Holding fintechs to a high standard, and conducting regular assessments to monitor compliance is key for ensuring that FIs maintain consumer trust while delivering differentiating products and services.

**Drive cyber governance and oversight from the top**

In our most recent CEO Outlook, the majority of Canadian CEOs report that they view cyber as a significant risk, up nearly 50 percent from 2018. This has prompted established FIs to extend mature governance structures and processes to help them address cyber security concerns.

There is also an increasing expectation from regulators, shareholders, and clients that directors and executives will take on more responsibility around cyber security. To this end, many leaders are striving to provide oversight of cyber security strategies and actively support the development and implementation of robust, scalable cyber security programs. By ensuring there is appropriate leadership in place at the executive level, seeking to understand and quantify their cyber risk, and allocating responsible levels of investment in security, organizations are taking steps to demonstrate a strong commitment to cyber security.

Directors and executives also have a role to play in the development and oversight of incident response planning and execution, ensuring there are holistic and relevant processes in place which involve leaders from across the business including technology, risk, legal, communication, and leadership teams.

As the group that sets business priorities, directors and executives are uniquely positioned to drive a strong cyber security culture and foster compliance with cyber policies, procedures, and regulations. They can also promote consumer-facing transparency of their overall cyber strategy, providing a view of how they are tackling cyber threats, what their stance is on the use and protection of personal information, and the value of sharing information with strategic partners.

**Striking a balance**

Today’s consumers and regulators expect FIs to take cyber security seriously. While clients are looking for value-driven, personalized, and convenient banking solutions, they are also increasingly cyber-savvy and concerned about how their information is being used.

With the pace of innovation continuing to accelerate, FIs are recognizing the need to move quickly to implement new technologies and be first-to-market with new products and services, while acting to preserve and enhance consumer trust.

By focusing on robust governance practices, sound cyber risk management, regulatory compliance, and strategic partnerships, established Canadian FIs can remain competitive and secure while making the most of innovative technology.

**Contact us**

John Armstrong
National Industry Leader
Financial Services, KPMG in Canada
KPMG in Canada
wjohnamstrong@kpmg.ca
416 777 3009

© 2019 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 23842. The KPMG name and logo are registered trademarks or trademarks of KPMG International.