Cyber Security in the Financial Sector as a National Economic Security Issue

03/18/2019

Remarks by Charles Docherty
Assistant General Counsel

Delivered to the House of Commons Standing Committee on Public Safety and National Security

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Cyber Security

Good Afternoon. I would like to thank the Committee for the opportunity to speak with you today about cyber security and the financial sector. My name is Charles Docherty, and I am Assistant General Counsel for the Canadian Bankers Association (CBA). Joining me is my colleague Andrew Ross, Director, Payments & Cybersecurity. The CBA is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals.

Banks in Canada are leaders in cyber security and have invested heavily to protect the financial system and the personal information of their customers from cyber threats. Despite a growing number of attempts, banks have an excellent record of protecting their systems from cyber threats. Banks take seriously the trust that has been placed in them by Canadians to keep their money safe and to protect their personal and financial information.

Canadians have come to expect greater convenience when using and accessing financial services, and banks have embraced innovation to provide Canadians faster and more convenient ways to do their banking. Now consumers can bank anytime from virtually anywhere in the world through online banking and mobile apps, providing real-time access to their financial information. Today, 72 per cent of Canadians primarily do their banking online or on their mobile device. That's up from 52 per cent just 4 years ago.

As more and more transactions are done electronically, networks and systems are becoming increasingly interconnected. This requires banks, government, and other sectors to work together to ensure Canada's cyber security framework is strong and able to adapt to the digital economy.

The CBA was an active participant in the Department of Public Safety's consultation on the new National Cyber Security Strategy. Our industry is a willing and active partner that supports the government in working to achieve the outcomes outlined in the strategy, with the common goal of improving cyber resiliency in Canada.

The banking industry is strongly supportive of the federal government's move to establish the Canadian Centre for Cyber Security under the Communications Security Establishment as a unified source of expert guidance, advice and support on cyber security operational matters. We also welcome the creation of the centralized cybercrime unit under the RCMP.

A key priority for the new Centre will be to ensure cyber resiliency across key industry sectors in Canada. Encouraging a collaborative environment, with the Centre providing a focus where the public and private sector can turn for expertise and guidance, will enhance Canada's cyber resiliency.

The security of Canada's critical infrastructure sectors is essential in order to protect the safety, security and economic well-being of Canadians. The banking industry counts on other critical infrastructure sectors, such as telecommunications and energy, to deliver financial services for Canadians. We encourage the government to leverage and promote common industry cyber security standards that would apply to those within the critical infrastructure sectors. We recognize critical infrastructures such as energy cross jurisdictional boundaries, and we recommend that the federal government work with provinces and territories to define a cyber security framework across all critical infrastructure sectors. Having consistent, well defined cyber security standards will provide for greater oversight and assurance that these systems are effective and protected.

Effective sharing of information about cyber threats, and expertise about cyber protection, is a critical component to cyber resiliency and increasingly important to Canada's digital and data-driven economy. The benefits from sharing threat information extends beyond the financial sector to other sectors, the federal government and law enforcement agencies, as is a highly effective means of minimizing the impact of cyber-attacks. Banks are supportive and active participants in initiatives such as the Canadian Cyber Threat Exchange (CCTX), which promotes the exchange of cyber security information and best practices between businesses and government as a way to enhance cyber resiliency across sectors. To foster information sharing, and for such forums to be effective, we recommend the government consider legislative options, such as changes to privacy legislation and the introduction of safe harbour provisions, to ensure appropriate protections are in place when sharing information related to cyber threats.

Protecting against threats from industries or other nations requires a defensive response that is coordinated between the government and the private sector. The government can play a pivotal role in coordinating among critical infrastructure partners and other stakeholders, building upon existing efforts to respond to cyber threats. Establishing clear, streamlined processes among all major stakeholders will enhance Canada's ability to effectively respond and defend against cyber threats.

We understand that the government plans to introduce a new legislative framework that addresses the implications and obligations in a world that is increasingly connected, and we will look forward to engaging with the government on the framework.

The CBA also believes that raising awareness about cyber security among Canadians is imperative. Educating Canadian citizens is and should be a shared responsibility between the government and the private sector. General knowledge of the issues and an understanding of personal accountability to maintain a safe cyber environment are required to help ensure comprehensive cyber security extends to the individual user level. The banking industry looks forward to further collaboration with the government on common public awareness initiatives such as incorporating online cyber security safety into federal efforts to promote financial literacy.

A skilled cyber security workforce that can adapt to a changing digital and data driven economy is equally important, not only for our industry, but for all Canadians as well. Every year, the CBA works with members to organize one of Canada's largest cyber security summits, bringing banks together with leading experts to share the latest intelligence about threats to deepen the knowledge of our cyber security professionals.

As cyber security threats continue to rise, there is a growing demand for cyber security talent both in Canada and abroad. Canada's new cyber security strategy recognizes that the existing gap in cyber talent is both a challenge and opportunity for our country. To address this shortage, we encourage the federal government, in cooperation with provincial and territorial governments, to promote and establish cyber security curricula in grade schools, colleges, universities and continuing education programs to enable students to develop cyber security skills.

In conclusion, I want to reiterate that cyber security is a top priority for Canada's banks. They continue to collaborate and invest to protect Canadians' personal and financial information. And banks support the government's work to protect Canadians while promoting innovation and competition. However, the industry recognizes that threats and challenges are constantly evolving. We want to work more collaboratively with the government and with other sectors to ensure that Canada is a safe, strong and secure country to do business in.

Thank you very much for your time and I look forward to your questions.