BANK OF CANADA
BANQUE DU CANADA

Remarks by Filipe Dinis
Chief Operating Officer, Bank of Canada
Payments Canada
May 9, 2018
Toronto

Strengthening Our Cyber Defences

Introduction

Thank you for the invitation to speak here today.

The ability to control your home appliances or deposit a cheque with a few clicks on your phone is hardly a novelty anymore. These innovations were introduced and widely adopted in record time. More are in the pipeline, and the speed of technological change is most certainly not slowing.

I see that in my own family. Before I was even able to master some of the new payment methods, my three children—including my 12-year-old daughter—were referring to them as “old fashioned.”

The modernization project launched by our host, Payments Canada, is designed to strengthen the underpinnings of the payments system and facilitate innovation and competition in retail payments. But delivering a faster retail payments system will be pointless if users don’t have confidence that the system will be better able to protect their account information and their own payments.

That applies to the entire financial system. Maintaining the trust of Canadians is essential. We need strong protections within each institution and collaborative partnerships between public agencies and the private sector to share information on cyber threats and strengthen our defences on every front.

Despite our best efforts, some attacks will inevitably succeed. Given the sophistication and frequency of cyber incidents, we need Canadians to know that in the event of a successful attack, we have recovery mechanisms in place. Limiting the damage and quickly getting the system back up and running is critically important.

That’s my topic today—cyber security defences and recovery plans. I’ll start with a short overview of the cyber risk environment. I’ll explain the Bank of Canada’s mandate and the role we play in cyber security for the financial system. I’ll describe the three main areas where we are concentrating our efforts and the partners we work with in Canada and internationally. And I’ll outline the actions we are taking.

I would like to thank Paul Chilcott, Ron Morrow, Grahame Johnson and Sylvain Chalut for their help in preparing this speech.

Not for publication before May 9, 2018
17:00 Eastern Time

Cyber threats, systemic risks

Think of all the ways that you can access your bank accounts, aside from standing in line waiting for a teller. You can use your watch, cell phone, tablet, automatic-teller machine and point-of-sale terminal. And think of all the places that accept electronic payments these days. All of this works relatively seamlessly and will become even more so with payments modernization. The real-time retail system that is part of the modernization program means that payments will be final and in your account in seconds rather than days.

Yet in many ways we're just getting started. The digital economy is expanding rapidly, with artificial intelligence, robotics, biometrics and other emerging technologies. The number of electronic devices that you can use to connect to the Internet is multiplying exponentially. Each has broadened the web of connections between users and available services.

The financial industry is keeping pace with these changes by investing in innovations that are reducing their costs and improving the customer experience. We all want better and faster banking services. But the more the industry adopts new technologies and amasses larger libraries of customer information, the greater the incentives for, and risk of, cyber attacks.

Banks, credit unions and other players in Canada's financial system process daily cash payments of $175 billion and more than $500 billion in trades of stocks and bonds. These kinds of numbers have made the financial system worldwide a favoured target of cyber criminals.[1]

Canada's financial institutions have strong defence mechanisms in place to repel attempts to steal money, grab information or simply disrupt their operations by causing damage. Our concern is not with individual firms but with the interconnections among them. Institutional protections are an excellent first line of defence, but they need to be complemented by effective sector-wide action, because a rare, successful breach at one institution could quickly morph into a broader disruption of the financial system.

Let me now turn to the role the Bank of Canada plays in enhancing the cyber security of the financial system.

Mitigating the risk

One of the Bank of Canada's responsibilities is fostering a stable and efficient financial system. With the steady increase in the scope and seriousness of cyber attacks worldwide, we are devoting more time and attention to the threats to financial stability that they pose.

How are we helping to mitigate the risk? Our focus is on three main areas.

First, we invest to ensure that the Bank itself is resilient to cyber threats.

Second, we ensure the financial market infrastructures overseen by the Bank are taking appropriate steps to mitigate cyber threats.

---

[1] See E. Kopp, L. Kaffenberger and C. Wilson, "Cyber Risk, Market Failures, and Financial Stability," International Monetary Fund Working Paper No. 17/185 (August 7, 2017).

And third, we collaborate domestically and internationally with financial system participants, regulators and oversight bodies to improve the resilience of the financial system.

Let me give you more detail on each.

Keeping our own house in order

Governor Stephen Poloz said in a recent speech that one of the things that keeps him up at night is cyber threats. If they keep him up at night, then I can assure you they keep me up at night as well.

Within the Bank, we are constantly investing in and augmenting our own cyber security program to prevent, detect and respond to a rapidly evolving array of threats that may compromise the confidentiality, integrity and availability of our digital information. Our security measures are multipronged, aligned with international standards and always up to date.

To protect our internal systems, we have conducted network-penetration tests, enhanced the controls governing access and deployed vulnerability-scanning tools. We ensure our data is encrypted and perform regular security updates.

We regularly communicate to staff best practices in online and email safety to make them aware of the risk of cyber attacks and encourage and reinforce appropriate responses. We've seen a significant improvement in the ability of employees to identify phishing e-mails, but we know we can't let our guard down.

We monitor the external environment to detect and respond to cyber threats. This includes the collection of threat intelligence and assessment information, a comprehensive review process for any third parties we interact with, a robust access-management program and implementation of enhanced SWIFT controls.

We are also making significant investments in our operational redundancies to ensure the resilience of our systems and our people. It is vital that our key functions can be maintained in the event of a major disruption, be it a cyber attack or natural disaster.

Finally, we are putting in place strategies to contain and recover from any damage such attacks might cause. More about this in a minute.

Our oversight of financial market infrastructures

The Bank is responsible for the regulatory oversight of financial market infrastructures, or FMIs, that we determine have reached a critical mass where their disruption could affect our entire system. These FMIs include the Large Value Transfer System and the Automated Clearing Settlement System—both of which are owned and operated by Payments Canada. FMIs are hubs for financial transactions. Their connections allow for the safe and efficient exchange of funds, securities and other financial products.

Given the central role that FMIs play in the financial system, a prolonged interruption, compromised data integrity or a loss of confidence in them could have a far-reaching impact on the financial system and the real economy. Protecting them from cyber-related threats is of the highest importance.

The Bank of Canada helped draft international guidance on cyber security. We use it in our work with the FMIs to assess whether they are taking appropriate steps to mitigate cyber threats. The FMIs internally assess their cyber resilience and also have outside experts conduct independent reviews. We evaluate these assessments to ensure that appropriate cyber security tools and practices are in place.

One area that we are concerned about is the growing operational risk from third-party providers such as the concentrated set of firms that provide many of the new technologies to the financial sector. Some of these firms offer critical data services and cloud computing and fall outside the purview of system regulators. As the Financial Stability Board recently noted, reliance on these same third parties and the interconnections between institutions could pose a systemic risk to the financial system. Greater global coordination is essential for addressing this issue.

We are also active participants in Payments Canada's modernization program. We want to ensure that cyber resilience is top of mind as payment and settlement systems are being redesigned.

An important initiative Governor Poloz launched recently—and that I am leading—is collaboration with the six largest Canadian banks to test and enhance the cyber resilience of the wholesale payments ecosystem. The goal is to have a rapid, collaborative approach to recovery should a key participant be affected by a serious cyber security event, such as the corruption of critical data that results in a prolonged operational outage.

Resilience through collaboration

The financial system's domestic and global interconnections mean it is important that we communicate, coordinate and align our work with what other participants are doing.

Within Canada, we study and assess vulnerabilities and risks to the financial system. In our November *Financial System Review* we listed cyber attacks on the financial system as a critical vulnerability and discussed how the Bank is working with industry, international bodies and federal and provincial authorities to enhance information sharing and improve policies.

We work to ensure that Canadian FMIs are speaking to the relevant security agencies, such as the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service.

In that regard, the National Cyber Security Strategy outlined in the recent federal budget is an important step forward. The government is allocating $507 million over five years, with almost $110 million per year afterward, to build an innovative and adaptive national cyber ecosystem. The strategy is designed to support effective leadership and collaboration among government, the business community, academia and trusted international partners.

An equally important part of the government's strategy is the creation of a new Canadian Centre for Cyber Security. The centre will become a single source of expert advice, guidance, services and support on operational matters related to

cyber security. We are looking forward to building on the Bank's already strong relationship with the CSE and the new Centre.

To improve not just cyber readiness but the operational resilience of FMIs and the broader financial system, we helped create and are chairing a partnership called the Joint Operational Resilience Management Program (JORM), which includes the Department of Finance, Canadian FMIs, large Canadian banks and the Canadian Bankers Association. Last year, JORM conducted a day-and-a-half long exercise that took 20 months to plan and involved more than 180 participants in three different cities. We wanted to assess escalation and communication protocols and public messaging at a national level during a systemic crisis. To do so, we simulated the operational failure of a key FMI, which would have halted major Canadian debt and equity markets for more than 30 hours.

We learned some key lessons from the exercise and are working to improve the financial sector's ability to coordinate actions in the event of such a major disruption.

Perhaps the most important lesson we learned is the value of trusted relationships and partnerships among regulators, financial system participants and other sectors. Individual firms in the financial system know their own business but don't always understand all their connections with others. This can lead to decision making that ignores threats to the system.

We also discovered—and this is certainly not unique to this exercise—the importance of coordination and communication protocols in the event of a systemic crisis. At such a stressful time, the last thing we want is confusion and ambiguity. We are now developing improved protocols to address this shortcoming.

On the international front, we participate in organizations that keep us up to speed on strategy, such as the development of regulatory and supervisory policies and the promotion of financial system resilience.

For example, we are active in the G7 Cyber Expert Group, which was created to strengthen cyber security in the international financial system. Cyber threats cut across borders so we coordinate with the expert group on policies such as third-party risks and penetration testing.

We participate in the SWIFT Global Oversight College. The college oversees the cyber resilience of SWIFT's messaging services. Our participation helps improve our own cyber security as well as that of the financial system in general.

We also work with other G7 countries, the Bank for International Settlements and numerous central banks to discuss emerging threats, our responses to threats, security monitoring and other related topics.

Conclusion

Let me sum up. Cyber threats aren't going away, so our job will never be done. The threats are constantly evolving and the digital economy is rapidly expanding. It is no longer enough for each institution to maintain its own alarm system. While

doing so provides a certain level of protection and comfort, we need to invest in system-wide defences.

To achieve that, we need close collaboration and coordination between the public and private sectors in Canada and abroad to share information and develop effective detection, response and recovery strategies.

We can only do this by building and maintaining trusted relationships with partners who know that the information they share with us will be protected.

Thank you.