BANK OF CANADA
BANQUE DU CANADA

Remarks by Filipe Dinis
Chief Operating Officer
Information Technology Association of Canada
November 12, 2019
Toronto, Ontario

Cyber Security: Breaking Down Barriers

Introduction

Good morning. It's a pleasure to be here in Toronto with you. I'd like to extend my sincere thanks to the Information Technology Association of Canada for inviting me.

I welcome this opportunity to talk about the work the Bank of Canada is doing on cyber security and the role of information technology and industry professionals like yourselves. It's an opportunity to open a dialogue about our common objectives.

In fact, ITAC's goals and those of the Bank are quite similar. You help Canada achieve a world-class, leading digital society that delivers prosperity and competitiveness in a global market. We help promote the economic and financial welfare of Canada, as mandated by the *Bank of Canada Act*.

So, we are both interested in the same outcome: a thriving, stable and secure economy for Canada and its citizens. And cyber security is certainly a key factor affecting our ability to deliver on these goals.

The Bank takes its role in safeguarding the financial system against cyber attacks very seriously. However, we can't tackle these challenges in isolation. We need to collaborate within the financial sector and ultimately throughout the economy to address these very real threats. And while we have made bold steps in working more frequently—and more effectively—with domestic and international partners, much work remains.

Let me start by telling you a bit more about the Bank of Canada's role in ensuring the resilience of the financial system.

The Bank of Canada's role

Not surprisingly, the people who founded Canada's central bank in 1935 didn't know a thing about cyber security—because they didn't have to. Lucky them!

At that time, central banks and individual institutions were far more concerned with physical security than mitigating the type of cyber-related risks we face today. The most prized possession of central banks used to be gold; today it is data.

In the 84 years of the Bank's existence, its areas of focus have stayed relatively constant. However, the way we conduct our business has evolved a great deal.

For example, one of our key responsibilities is fostering a stable and efficient financial system. Today, with the steady increase in the scope and seriousness of cyber attacks worldwide, this means we focus a lot of attention on the threats they pose. The Bank's 2019 *Financial System Review*, which identifies key vulnerabilities in the financial system, highlighted the worldwide increase in the frequency, severity and sophistication of cyber attacks and the potential for widespread disruptions.

This is also a major preoccupation of those in our country who specialize in risk management in the financial sector. Twice a year, the Bank surveys these experts. As noted in last spring's survey, cyber incidents continue to be identified as the greatest risk to the Canadian financial system. We're releasing the autumn 2019 edition of the survey next week, and we expect that cyber security will continue to be a preoccupation.

And with good cause. Cyber incidents are becoming more frequent, growing in sophistication and posing a real threat to the stability of the financial system. According to figures provided by data specialist firm Advisen, there were almost 5,000 successful cyber attacks in the global financial sector from 2014 to 2018. And these attacks affected over 550 million records, with known direct losses of more than $4 billion.

Such alarming numbers underscore why the Bank's own cyber defences must be strong enough to protect our valuable assets, whether they are financial, data or people. The Bank has made much progress on cyber security and has made significant investments over the past five years to enhance our overall resilience.

This includes our Business Recovery Enhancement program, which increases the resilience of our data centres, network and technology infrastructures, and business systems. This program will help the Bank withstand all types of shocks, including weather incidents and, of course, cyber threats.

We also invested in people, planning, infrastructure and training to bring our new Calgary Operational Site on-line this past spring. Staff in Calgary are fully integrated with the banking and market operations team in Ottawa. They can take over critical market functions at a moment's notice in the event of a major operational incident. This is a major step toward increasing our resilience.

In addition, last year we established the position of Chief Information Security Officer within the Bank of Canada. This reflects a best-practice governance model for aligning and coordinating cyber programs and activities.

These are examples of what we've done internally to improve our cyber security. But the Bank is also mandated to promote cyber security externally. So, this summer, I was pleased to present and post on our website the Bank's updated 2019–21 Cyber Security Strategy—an important next step in our cyber evolution.

The strategy acknowledges that—while much good work has been done—we have much more to do to fulfill this mandate.

First, we are continuing to innovate and enhance security within our own operations.

Second, we are collaborating with external partners to improve our individual and collective resilience. For example, we recently partnered with a cyber security firm to test the potential of using machine learning as a way to detect anomalies in our infrastructure and mitigate the risk of cyber incidents.

Finally, we are acting as leaders in the financial sector by promoting robust cyber security standards. This will help protect the domestic and international financial sectors against cyber risks.

Broad vulnerabilities require broad responses

At the Bank, we look at issues from a broad perspective, whether we are thinking about monetary policy, the financial system or cyber security. And when we talk with financial institutions and other market participants about cyber security, it's important for them to set aside their natural competitive instincts and think broadly about the issue as well. That's because broad vulnerabilities require broad responses.

Historically, most companies—including banks—tended to think of cyber security in terms of how it might affect their own operations. From a management point of view, it's relatively simple to think about the risks posed by ransomware or a targeted attack by hacktivists. You can calculate the potential cost to your own business and work out how much you should spend to mitigate that risk. This is just the cost of doing business.

The analysis becomes more complex when you extend it to cover your key suppliers or business partners. But even this approach is not broad enough because it misses the risk posed by a systemic cyber event—one that could affect financial institutions, networks, infrastructures and markets. And this event could be triggered by security flaws in widely used software, infrastructure vulnerabilities or even hostile governments.

As we are all aware, the growing interconnectedness of society is amplifying the risk of a systemic cyber event. The number of devices that are connected to the internet is rising at an exponential pace. While this has many benefits, we could also imagine an event where one financial institution's data and operations are breached, and this attack spreads to external partners. This is the scenario that keeps us up at night—a major event that disrupts national and international financial systems.

This interconnectedness makes it very hard to quantify the risk of a systemic cyber event. It may be the case that some companies are allocating the wrong amount of resources to the issue. Some may be underinvesting in cyber security because they aren't internalizing the systemic nature of the risk. Others might actually be overinvesting resources. Either way, what is clear to me is that better collaboration could bring about a better outcome for all of us at no greater cost. That is why collaboration is a win-win.

I work every day with economists, and I try to learn from them and the language they use. For example, when they talk about this kind of problem, they might use the phrase, "the tragedy of the commons." Let me explain. Think of a system

where everyone has to share a finite resource. Often, individuals will think of their own needs first and pay little attention to the common good. The problem is, if everyone thinks only of their own interest, the shared resource gets used up, and everyone is worse off.

The point is that there are situations where governments need to step in to protect the common good. Think back a decade or so to the global financial crisis. Before the crisis, regulations covering banks focused mainly on each institution. The system-wide perspective was missing—regulations paid little attention to risks to the entire financial system. And banks generally did not think about the impact of their risk-taking behaviour on the system as a whole.

Since the crisis, governments have taken on that system-wide perspective and worked hard—both domestically and internationally—on regulations that make the financial system safer.

We can see clear parallels with cyber security. Promoting the common good is an objective of the Canadian Centre for Cyber Security. Its mandate is to lead the government's response to cyber security events by ensuring broad collaboration among government, academia and the private sector on complex cyber issues.

And on a broader scale, this is why the federal government launched the National Cyber Security Strategy. In fact, in last year's budget the government boosted its investment in this area by over half a billion dollars.

The good news is that major Canadian financial institutions have shown that they appreciate the need for a broad perspective. They realize that an attack on one financial institution can quickly become an attack on all.

To this end, the Bank has been collaborating with the six largest Canadian banks, as well as the key providers of payment, clearing and settlement systems. This initiative, called the Resilience of Wholesale Payments Systems, is a big step forward. I applaud the participants' spirit of collaboration and transparency.

More recently, we launched the Canadian Financial Sector Resiliency Group, also known as CFRG. This forum comprises key players in the financial system, along with the federal finance department and the Office of the Superintendent of Financial Institutions. Its mandate is to manage a systemic operational incident by testing resilience protocols and looking for ways to improve information sharing—among other activities.

Through our collective efforts to date, we've built a degree of trust among the country's financial institutions. But trust is slow to gain and easy to lose. So, it is crucial now that we solidify that trust and keep chipping away at the barriers to working better, together.

Getting regulation right

How can we break down such barriers to collaboration? Maybe we should look to the other side for lessons. Hackers are fantastic at collaborating. Of course, they don't have to satisfy lawyers, comply with regulators or answer to shareholders. In a perverse way, they are compensated for collaborating. The point is, we need to think and act boldly to eliminate barriers to information sharing.

Sometimes the regulatory frameworks that are designed to protect institutions and customers can get in the way of collaboration. For instance, institutions have sometimes said they were legally prohibited from sharing information about cyber security.

Our regulatory environment has historically focused on protecting privacy and promoting competition. These are important objectives, but we need to increase our focus on the resilience of the financial sector. That means we should consider updating the balance of the current regulations and think about the necessary trade-offs to do so.

What do I mean by trade-offs? Some countries are relying on the widespread use of closed-circuit television and advances in facial-recognition technology to heighten security in the face of terrorist threats. Obviously, there are privacy considerations here. But these countries have decided that, for the greater good, this is a trade-off worth making.

In a similar fashion, everyone involved in cyber security needs to ask what sorts of regulations achieve the right balance between privacy and competition, while also working to keep us all safe from cyber threats.

Surely the goal of our regulatory framework should be to encourage collaboration and information sharing to reduce the risk of a successful cyber attack. At a minimum, regulatory frameworks should not be an impediment to collaboration.

I would argue that we need to take a two-pronged approach that would address both the reluctance to share information and the need for appropriate investment in cyber security.

Perhaps our regulatory framework can be strengthened by putting in place trusted, secure channels to transmit this kind of sensitive information, to protect the reputation and vulnerabilities of institutions.

Further, governments could also consider strengthening minimum requirements around cyber resilience and mandate industry-wide and cross-sectoral testing that requires institutions to fix problems identified by the tests.

I don’t expect that we’ll design the perfect regulations here today. But I would suggest that there is room to enhance our current regulatory frameworks that rely on financial penalties, albeit not exclusively. After all, if company management is unable to accurately gauge the risk of a systemic cyber event, it may well decide the fine for non-compliance is a cost that is worth paying.

So, policy-makers need to consider how best to design incentive-based frameworks to encourage collaboration and information sharing. This includes regulations with legislative protections for doing so.

These regulations should be technology-neutral, meaning they should be able to adapt as technology inevitably evolves. We should also strive for legislative reforms that are compatible with international norms, a common lexicon and approaches. This will help cross-border collaboration and decrease opportunities for companies to exploit jurisdictions with weaker cyber security regulations.

Just as national governments need to promote defences within their own borders, governments worldwide need to co-operate to promote global cyber

security. There are no walls between countries when it comes to cyber attacks. Given the interconnectivity of international financial institutions, the Bank of Canada also has an obligation to collaborate with partners in other jurisdictions.

Earlier this year, the G7 hosted a tabletop exercise with finance ministries, bank supervisors and central banks, simulating a cyber crisis. This prompted participants to consider their domestic tool kit to respond to such a scenario. It also brought about important questions about how and when to talk to international partners if the simulation should become reality.

Collaboration and the way forward

Beyond enhancing regulatory frameworks, we are committed to holding regular, realistic and stringent tests of our cyber defences across our domestic financial system, not unlike the G7 tabletop. Doing so will cement the spirit of collaboration among financial institutions, maximizing the likelihood of protecting the system and minimizing recovery times.

And it's equally important that this collaborative spirit spread beyond the financial sector to also include other sectors that form a part of our country's critical infrastructure, like telecommunications, energy and utilities, transportation and beyond. We need to urgently step up the spirit of collaboration throughout the Canadian economy. We need to encourage regular exercises that present companies with complex scenarios to test their cyber defences and response capabilities. Even the process of designing risk scenarios can help companies determine potential sources of risk.

The private sector has a role to play as well. I'm happy to see companies working together toward establishing best cyber practices. In particular, I'm glad to see ITAC partnering with the CIO Strategy Council in its responsible technology initiative. As you are aware, one of the goals of this initiative is to advance collaboration, expertise and knowledge across sectors. I know that ITAC can assist in bringing a sense of urgency about these goals in terms of cyber security.

All this work has brought key players to the table and established common goals. But it has also shown us that we still face significant challenges. What's more, we need to act quickly and forcefully to deal with them. After all, technology and the security threats we face are evolving at incredible speed. So, what's next?

I can suggest a couple of paths forward. First, industry groups can work with public sector authorities, including regulatory bodies and intelligence agencies, to design and implement the kinds of national cyber exercises I spoke about earlier, including pen tests.

These exercises can help companies improve their reactions and deepen the relationships needed to withstand such an attack. It's now time to build exercises that involve multiple economic sectors, to provide a more demanding and realistic test of our economic cyber security.

Another important way to increase resilience goes back to the need to increase information sharing. We need to build mechanisms that will significantly increase the sharing of cyber threat information and cyber defence best practices between

public and private sector organizations. This will be particularly important for smaller companies that have fewer resources to dedicate to cyber security.

We should also consider opportunities to build sector-wide cyber defence approaches and systems to protect many companies at a time. These would maximize resilience, rather than having each company solely responsible for its own defences. Think about how cloud computing companies work to provide specific services for many companies, freeing those smaller firms to concentrate on their core lines of business.

Conclusion

Regardless of how cyber security develops, it is clear the IT sector will be a big part of the solution. I'd like to wrap up my remarks by saying a few words about the role professionals like you have in making us all more cyber-safe.

First, from my public sector viewpoint, it is crucial that we take advantage of your expertise and agility in developing the right policies for cyber security. We need your perspective to help us ensure we maximize protection without stifling innovation and creativity.

Second, we need to partner with you on approaches that will uncover techniques to solve the trickiest problems in cyber security. What's the best way to deploy artificial intelligence in cyber defences, including from internal threats? How quickly can machines learn to detect fraud and adapt to new fraud techniques? If quantum computing has the potential to make current data encryption methods obsolete, what new techniques can be developed to keep our data safe?

So, let me throw down a challenge of sorts. I've laid out some of the key questions facing us today around cyber security. I'd invite you to help discover the answers to these kinds of questions that are vital to the economic security of Canada. And, of course, they will also be extremely valuable to the company that figures them out!

I'd like to thank you once again for inviting me to be here with you today. I hope I've achieved the goal you laid out for me in appearing before you—that is, how the Bank of Canada contributes to a resilient and secure financial system.

I hope I've given you a bit more insight into why working together toward this important objective is key to our success.

And finally, I hope I've provided some more detail about the steps we've taken to date on cyber security as well as an appreciation of how much more there is to do.

I would be happy to answer any questions you may have.