House of Commons
Chambre des communes
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 152 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, March 18, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Monday, March 18, 2019

● (1545)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): It's my privilege to open the meeting and invite the Canadian Bankers Association and the Canadian Chamber of Commerce to address the committee. Both groups have been instructed on the parameters of their presentations.

Did you do rock, paper, scissors as to who will go first, or will we just go with the Canadian Bankers Association?

Mr. Docherty.

Mr. Charles Docherty (Assistant General Counsel, Canadian Bankers Association): Thank you very much. Good afternoon.

I would like to thank the committee for the opportunity to speak with you today about cybersecurity in the financial sector.

My name is Charles Docherty. I am the assistant general counsel for the Canadian Bankers Association, or CBA. Joining me is my colleague Andrew Ross, director, payments and 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 cybersecurity and have invested heavily to protect the financial system and the personal information of their customers from cyber-threats. Despite the 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 any time from virtually anywhere in the world through online banking and mobile apps that provide real-time access to their financial information. Today 76% of Canadians primarily do their banking online or on their mobile device. That's up from 52% just four years ago. As more and more transactions are done electronically, networks and systems are becoming interconnected. This requires banks, government and other sectors to work together to ensure that Canada's cybersecurity 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 cybersecurity 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 cybersecurity under the Communications Security Establishment as a unified source of expert guidance, advice and support on cybersecurity 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 sectors 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 infrastructures such as telecommunications and energy to deliver financial services for Canadians. We encourage the government to leverage and promote common industry cybersecurity standards that would apply to those within the critical infrastructure sectors.

We recognize that critical infrastructures such as energy cross jurisdictional boundaries, and we recommend that the federal government work with the provinces and territories to define a cybersecurity framework across all critical infrastructure sectors. Having consistent, well-defined cybersecurity 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 extend beyond the financial sector to other sectors, the federal government and law enforcement agencies. Sharing information 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 that promotes the exchange of cybersecurity 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 that 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 and streamlined processes among all major stakeholders will enhance Canada's ability to effectively respond to, 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. We look forward to engaging with the government on the framework.

The CBA also believes that raising awareness about cybersecurity 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 that comprehensive cybersecurity extends to the individual user level. The banking industry looks forward to further collaboration with the government on such common public awareness initiatives as incorporating online cybersecurity safety into federal efforts to promote financial literacy.

A skilled cybersecurity 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 cybersecurity summits, bringing banks together with leading experts to share the latest intelligence about threats and to deepen the knowledge of our cybersecurity professionals.

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

In conclusion, I want to reiterate that cybersecurity is a top priority for Canada's banks. They continue to collaborate and invest to protect Canadians' personal and financial information. 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. I look forward to your questions.

● (1550)

The Chair: Thank you, Mr. Docherty.

We now have the Canadian Chamber of Commerce.

[*Translation*]

Dr. Trevin Stratton (Chief Economist, Canadian Chamber of Commerce): Thank you very much, Mr. Chair and members of the committee. It's a real pleasure to be here with you today.

[*English*]

I'm Trevin Stratton. I'm the chief economist at the Canadian Chamber of Commerce. The Canadian chamber is the voice of business in Canada, and represents a network of over 200,000 firms from every sector and region and every size of business. I'm here with my colleague, Scott Smith, the senior director of intellectual property and innovation policy at the chamber.

Banking transactions are increasingly being conducted in new ways, with 72% of Canadians primarily doing their banking online or through their mobile device. Disruptive or destructive attacks against the financial sector could, therefore, have significant effects on the Canadian economy and threaten financial stability. This could occur directly through lost revenue, as well as indirectly through losses in consumer confidence and effects that reverberate beyond the financial sector, because it serves as the backbone of other parts of the economy. For example, cyber-attacks that disrupt critical services, reduce confidence in specific firms, or the market itself, or undermine data integrity could have systemic consequences for the Canadian economy as a whole.

Banks have invested heavily in state-of-the-art cybersecurity measures to protect the financial system and the personal information of their customers from cyber-threats. In fact, cybersecurity measures and procedures are part of the banks' overall security approach, which includes teams of security experts who monitor transactions, prevent and detect fraud and maintain the security of customer accounts.

The sophisticated security systems in place protect customers' personal and financial information. Banks actively monitor their networks and continuously conduct routine maintenance to help ensure that online threats do not harm their servers or disrupt service to customers.

However, cybersecurity issues are marked by significant information asymmetries, where a disproportionate amount of intelligence and capacity resides with large institutions like the federal government, the Bank of Canada and a few large private sector companies, including financial institutions. Yet, small and medium-sized enterprises are no less vulnerable. It is important for them to secure a cybersecurity ecosystem. They are also disproportionately subject to mounting asymmetries in resources, technologies and skills to defend against nefarious adversaries who, with relatively primitive skill sets and resourcing, can inflict excessive financial and reputational damage.

My colleague, Scott Smith, will now outline the cyber-threat landscape facing Canada's small and medium-sized enterprises.

● (1555)

Mr. Scott Smith (Senior Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce): I believe you've heard from several witnesses over the past few months about the evolving cyber-threat landscape, some of the attacks that are being experienced across the board and how that's changing, and the challenge that represents. Instead, today I'm going to draw your attention to the growing attack surface and how economic disruption that impacts national security can come from unexpected places.

Canada depends on small business for economic well-being. There are 99.7% of businesses in Canada that have fewer than 500 employees, but they employ over 70% of the total private labour force. Small to medium-sized enterprises contribute 50% of Canada's GDP, 75% of the service-producing sector and 44% of the goods-producing sector. They also represent 39% of the financial, insurance and real estate sector.

Fintech has a projected continuous annual growth rate of 55% through 2020. Canada is a hot spot for fintech growth, especially in mobile payments, and most of the emerging companies are SMEs. SMEs collectively constitute a very large attack surface. This attack surface has attracted the attention of hackers.

With regard to some examples of the link between supply chains and major disruptions, in 2018, five natural gas pipeline operators in the U.S. had their operations disrupted when a third party supplier of electronic data and communications services was hacked in the spring of that year. The hacking of a third party vendor to more than 100 manufacturing companies was discovered in July 2018. Approximately 157 gigabytes of data that Level One Robotics was holding was exposed via rsynch, a common file transfer protocol used to mirror or back up large datasets.

The 2017 NotPetya malware outbreak forced shipping giant Maersk to replace 4,000 new servers, 45,000 new PCs and 25 applications over a period of 10 days, causing major disruption.

Why is this happening? Criminals are a bit like flood water; they follow the path of least resistance. Small to medium-sized enterprises have several challenges when it comes to security: limited financial resources, limited human resources and a culture of disbelief, the so-called “we're too small to be hacked” syndrome.

The digital economy has been a boon to small business growth, enabling rapid entry to global supply chains. However, this innovation and growth comes with significant risk if security concerns are not addressed, particularly given the increasing sophistication of cybercriminals. They've moved from the disruption of viruses, trojans and worms 10 years ago, which were common to hear about, to now generating usable digital trust certificates that bypass the human element.

The goal must be to reduce the attack surface, making Canadian business a less attractive target to criminals. The solution is a culture shift, through education, awareness and setting achievable industry-led standards, without stifling innovation. It's a big challenge. It also means investing in international criminal enforcement relationships and capabilities.

I'll stop there, and I'm happy to answer any questions.

The Chair: Thank you to both of you.

Our first questioner is Monsieur Picard.

[*Translation*]

You have seven minutes.

Mr. Michel Picard (Montarville, Lib.): Thank you, Mr. Chair.

Gentlemen, welcome to our committee.

[*English*]

I will ask my question in French, if you have your earpiece for translation.

[*Translation*]

My question is for the representatives of the Canadian Bankers Association, since they work in the financial sector, which is the topic of our study.

What strategy did you use to develop your cybersecurity program? What are the aspects or operations of your clients' activities that you took into account to develop the steps of the cybersecurity measures?

● (1600)

[*English*]

The Chair: To whom are you directing the question?

Mr. Michel Picard: It's addressed to the Bankers Association.

Mr. Charles Docherty: The banking industry takes its responsibilities for protecting clients' information extremely seriously. We appreciate the trust that customers have put in us to protect their personal information.

In terms of a strategy, the banks—in addition to protecting their own systems and infrastructure—are contributors to ensuring cyber-resiliency across Canada as well. They're heavy contributors to the Canadian Cyber Threat Exchange, which allows not only banks but also other industries to access information related to cyber-incidents and threats. Of course, they've invested billions of dollars in ensuring that their IT infrastructures are safe and secure.

[*Translation*]

Mr. Michel Picard: I would like your approach to be more concrete.

The purpose of this study is to ask the private sector, including your association, to help us find ways to improve our financial services infrastructure.

You are in the financial sector. We know that you manage personal data. On the ground, you had to start somewhere; someone got up one morning and decided to begin by examining this or that operation, by using this tool, by examining this or that banking services sector. Indeed, there are a whole range of financial services. Could you summarize the process that led to the development of your cybersecurity strategy?

[*English*]

Mr. Andrew Ross (Director, Payments and Cybersecurity, Canadian Bankers Association): This is obviously an evolving space and our strategy continues to evolve with it.

At the end of the day the banks go through rigorous risk management frameworks to assess the various threats they see.

As my colleague mentioned, one thing we believe we are very good at is detecting cyber-threats. We've contributed to the government's strategy as well. I think one area where we can to do more is information sharing, not only to improve the financial sector itself but beyond the sector.

At the end of the day it comes down to risk mitigation, identifying those areas that need to be dealt with, and assessing and defending against those.

Mr. Michel Picard: Okay.

I have a choice of two tricky questions.

First, why are banks asking for fees from their customers for additional insurance to protect their personal information from identification theft? I thought that when I was doing business with banks, since I have to give them all of my precious information, they would take care of it without my having to pay more to have the same information protected. Is it because your system does not protect my ID enough? Or is it just a marketing stunt?

Mr. Charles Docherty: As I mentioned at the outset, banks take their responsibilities to protect the personal information of their clients very seriously. They do provide products and services to their clients to help ensure that their personal information remains safe.

I can't speak to exactly the economic model you're referring to of charging extra for personal identification monitoring specifically. But in some cases if a client wanted there to be more monitoring, then they should have that option to have their personal information monitored more closely. In that case, that is a product or service that a bank may be willing to offer to them.

Mr. Michel Picard: So, as I understand it, it's safe to say that my personal information is quite safe in any bank in Canada, because they have all the means and tools to protect me.

Mr. Charles Docherty: Absolutely.

Mr. Michel Picard: Excellent.

On sharing information, we've talked more and more about open banking. What is your take on that?

Mr. Andrew Ross: Certainly, we are involved in the consultations the Department of Finance is undertaking in looking at the merits of open banking.

From our perspective the sector supports innovation and competition in financial services. As we have outlined, we need to look not only at the benefits, but also at the risks that are associated with open banking. Cybersecurity is one of those areas. We feel that through the consultation, if we're able as a country to mitigate those risks and the benefits are identified and seen, then we would support open banking.

● (1605)

Mr. Michel Picard: What is the nature of the risks that you have identified in your firm?

Mr. Andrew Ross: As mentioned earlier, there is the risk of others playing in the financial space that may not have the same resources as a bank. I think that's one.

Generally speaking, I think the more entities you have involved, the more interconnected channels that exist, then the greater the risk of a cyber-threat.

Mr. Michel Picard: Thank you, gentlemen.

[*Translation*]

The Chair: Mr. Paul-Hus, you have the floor for seven minutes.

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

Good afternoon, gentlemen. Thank you for being here with us.

Banks handle business banking and personal banking. Since I own some businesses, I know that technology like SecureKey is needed to access accounts. Access to a business account is very complex, as compared to accessing a personal account.

My colleague asked this question, but I would like to know whether, from the outside, it is easier to attack a business account than to attack a personal account, or whether it is the same thing.

[*English*]

Mr. Charles Docherty: Certainly, I believe the risks would be the same. Corporations would necessarily need to have controls in place, as there are more people working within a corporation who might have access to the banking system of the corporation.

Mr. Pierre Paul-Hus: Do you know what I mean?

[*Translation*]

I'd like to know whether in your opinion the protection of business accounts against cyber-attacks is superior to the protection of personal accounts.

[*English*]

Mr. Charles Docherty: No, it would be the same standard. Banks take their obligations seriously regardless of the type of entity involved.

[*Translation*]

Mr. Pierre Paul-Hus: Fine.

Some witnesses told us that in certain countries the disclosure of cyber-attacks is mandatory. Are banks here required to disclose cyber-attacks on their systems to the Government of Canada?

[*English*]

The Chair: Excuse me, Pierre. We lost translation for about 10 seconds there.

Could you go back and start again, please? Thank you.

[*Translation*]

Mr. Pierre Paul-Hus: Fine, I'll repeat my question.

Several witnesses mentioned that in some countries banks have to disclose cyber-attacks. Is that the case in Canada? Does the Royal Bank, for instance, have to inform the government within a prescribed time?

[*English*]

Mr. Charles Docherty: Yes, it would. Banks, like any other organization that's governed under PIPEDA, the federal privacy legislation, are obligated in the event of a breach of their security safeguards to notify the Office of the Privacy Commissioner and any impacted individuals.

[*Translation*]

Mr. Pierre Paul-Hus: Are the banks reluctant? If, for instance, the Bank of Montreal is subject to an attack, this could affect its reputation. Do you think they are reluctant, or is disclosure automatic, without being called into question?

[*English*]

Mr. Charles Docherty: They are not wary of disclosing the fact that they've been attacked. It's a statutory obligation. In addition to that, because of the trust that the customers have placed in the bank, they want to make sure their customers are aware in the rare circumstance that there's been a cyber-attack.

Mr. Andrew Ross: May I add that OSFI also requires banks to report?

[*Translation*]

Mr. Pierre Paul-Hus: I would now like us to talk about individuals.

[*English*]

The Chair: We have a problem with translation, and I had better stop the clock or Pierre will get upset.

I'm told that the interpreters' booth has technical problems and that, absent translation, we'll be obliged to suspend, regrettably. It's Pierre's fault that this whole thing has fallen apart.

A voice: I hope you haven't been hacked.

Voices: Oh, oh!

● (1610)

Mr. Pierre Paul-Hus: I won't complain about the official language. I'll ask my question in English as well.

The Chair: In order for me to proceed, I must have the unanimous consent of the committee to proceed in one official language.

Some hon. members: No.

The Chair: We're suspended.

● (1610)

(Pause)

● (1620)

The Chair: Ladies and gentlemen, apparently we've fixed whatever difficulties we had.

We got started about 10 or 15 minutes late and we lost another five minutes with that exercise. This is inevitably going to bump us into our next panel. My thought is that we simply add 15 minutes on to this panel and start the other panel later. Is that acceptable? I believe we still have a vote here, so we're essentially not going anywhere anyways. This might work out.

Are you fine with that, Mr. Motz?

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): I thought you were buying me supper in-between, so I was a little concerned about that.

The Chair: Mr. Motz, the day I buy you supper will be....

Some hon. members: Oh, oh!

Mr. Glen Motz: On your retirement.

The Chair: Yes.

Mr. Paul-Hus, we'll give you four minutes.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

In the brief presented by the Canadian Bankers Association, which you tabled earlier, you spoke about the security of Canada's essential infrastructures: “The banking industry counts on other critical infrastructure sectors such as telecommunications and energy to deliver financial services for Canadians”. This leads me to my next question, which is about critical infrastructures abroad, such as in the United States, Europe or elsewhere in the world.

Do you collaborate and hold discussions with the financial sector representatives of other countries to find out about appropriate techniques, and which entities are responsible for cyber-attacks against their systems?

[*English*]

Mr. Andrew Ross: Yes, our banks are involved in certain different international groups, one in particular in the U.S. called FS-ISAC, an information-sharing hub created in the U.S. but with a global reach. Our banks are certainly involved in that, as much as we share in Canada, as well.

[*Translation*]

Mr. Pierre Paul-Hus: Recently, the Americans expressed concerns regarding the infrastructure of telecommunications companies. Do you discuss issues that could arise from the integration of the 5G network in Canada with your American partners?

[*English*]

Mr. Andrew Ross: From a national security perspective, that's not something we would have a lot of insight about. Certainly, that question would be better asked of the telecom industry.

[*Translation*]

Mr. Pierre Paul-Hus: I see; but have the Canadian banks that are a part of your network ever expressed concerns with regard to telecommunications and banking information?

[*English*]

Mr. Andrew Ross: Again, we would rely on the proper diligence being performed from a national security perspective on any telecom provider introduced into Canada. Obviously, whatever telecommunication provider comes into Canada would be required to support more than just the financial sector, so we would really rely on the national security review and the telecom sector.

[*Translation*]

Mr. Pierre Paul-Hus: With respect to the protection of assets, those of enterprises and those of individuals, can the banks that are members of your association compensate the losses due to fraudulent transactions, attacks or phishing operations? How does that work? First, is it a major problem? Second, do your clients and your banks incur losses?

[*English*]

Mr. Charles Docherty: There's no problem. Banks, in the rare circumstance of a cyber-attack that results in a financial loss to their clients, will reimburse them.

● (1625)

[*Translation*]

Mr. Pierre Paul-Hus: I believe there is a $100,000 limit on compensation.

Is there a maximum for insurance, or the bank's liability?

[*English*]

Mr. Charles Docherty: You may be referring to the CDIC deposit insurance. That's not something related to cyber-threats or cyber-attacks. In terms of a cap for banks, if a fraud has been committed and the clients are not at fault, but the security safeguards have been breached, they will be reimbursed.

Mr. Pierre Paul-Hus: Would it be 100%?

Mr. Charles Docherty: Yes, sir: 100%.

Mr. Pierre Paul-Hus: Okay.

Thank you.

[*Translation*]

The Chair: Mr. Dubé, you have seven minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you Mr. Chair.

Gentlemen, thank you for being here.

I have a question about the banks and the credit card companies. That relationship is more complicated than people realize.

There is a belief that the banks are responsible for several of the steps in a credit card transaction, but in fact, it is the credit card company that is responsible.

The Privacy Commissioner shared concerns about the fact that the credit card company servers are located elsewhere, such as in the United States. The legal protections conferred on clients by citizenship are not necessarily the same. There is also the fact that an ill-intentioned actor could pose additional risks, should the relationship between two countries deteriorate. From that perspective, the servers that contain our data, for instance the ones in the United States, could become a target.

Do the banks that deal with those enterprises have a role to play in this? Can the Government of Canada do anything to protect the data and transactions of Canadians?

According to what I understand, credit card companies are independent from the banks. Nevertheless, the banks deal with those enterprises for certain important aspects of their activities.

[*English*]

Mr. Andrew Ross: I think it's fair to say that banks and credit card companies are interconnected. The data is shared. Credit card companies have data related to the transaction, but so do the banks. At the end of the day, if it's a Canadian-issued credit card, then obviously banks would be obligated to follow the requirements as set out by Canadian legislation.

[*Translation*]

Mr. Matthew Dubé: I want to make sure I understood.

Certain obligations are imposed on you. If you do business with the credit card company, whether Visa or Mastercard or another company, the data on clients' credit card transactions are kept on the servers of the credit card company. Does this create a problem with respect to the legal protection offered in countries where the data are kept? Do the same obligations apply? If Visa, for instance, knows about a leak on American servers, is it the Canadian bank that is responsible for that leak?

[*English*]

Mr. Charles Docherty: I can speak to the fact that banks remain responsible and accountable for the personal information of their clients. When they contract with a third party, let's say, and outsource the processing of data, they are responsible in those circumstances to ensure that the privacy and security safeguards are in place. They would inform their clients that their data was being stored in another jurisdiction and was subject to that jurisdiction's laws.

The important thing to remember is that when they've outsourced their data, it doesn't mean they've outsourced their obligations. Canadians can feel confident and secure that their data is being protected by the banking industry.

Mr. Matthew Dubé: I just want to make sure I understand that answer correctly. I apologize; I'm not trying to lay out a trap or anything. This is just to try to get a better understanding of this, with data transiting all over the place. That's part of the objective of this study.

Let's say a bank has an agreement with a credit card company and that credit card company is in the United States. We'll assume that the majority of them operate primarily in the States. If their servers are there, per the agreement you have with them, you would then respect your obligations under Canadian law for the bank if something happened in another jurisdiction relating to the credit card company that affected Canadian clients.

● (1630)

Mr. Charles Docherty: If it's an outsourcing arrangement, then yes, definitely. If it's an independent third party, then the laws of the country where the information is being held by that third party may apply.

Mr. Matthew Dubé: When you say “independent third party”, would that be similar to how we talk about open banking and things such as that?

Mr. Charles Docherty: Yes, but I want to just reiterate that when it comes to the banks and protecting their clients' information, in the event of a breach of the bank's security safeguards—which would be a rare circumstance—they would comply with Canadian law and take all steps necessary to make their customers whole.

Mr. Matthew Dubé: If there's a breach at a credit card company that deals with multiple banks, do the banks consider it their responsibility if they have consumers that are affected? Am I understanding that correctly?

Mr. Andrew Ross: Yes, the banks would hold the customer relationship directly in that circumstance.

[*Translation*]

Mr. Matthew Dubé: That is fine, thank you.

There's another point I'd like to discuss.

In your presentation, you mentioned that 72% of Canadians use the Internet or mobile applications to do their banking transactions.

One aspect that is brought up frequently concerns wireless networks. You may well have the most secure network in the world, but if software updates on our equipment or our cell phones are not done on time, this may create breaches and cause serious problems with respect to financial transactions.

In the past, your organization has said that we should adopt standards for the products people use to access their data. Could you tell us more? We often hear about the concept of the Internet of Things, an expression I like. It may have consequences on financial transactions.

[*English*]

Mr. Andrew Ross: When it comes to things such as Wi-Fi, again, that falls under the telecom sector specifically and whatever safeguards they would be required to undertake. Again, Wi-Fi would affect things beyond financial services and financial transactions. That said, we've been very vocal in terms of sharing information with our customers. It comes back to educating customers in terms of where they should and should not perform financial transactions. We continue to share that message with them. Public awareness is one area where we would certainly encourage the government to do more, so that again, Canadians can feel safe in whatever type of transaction they are doing through Wi-Fi, financial or otherwise.

The Chair: Thank you, Mr. Dubé.

Madam Sahota, for seven minutes, please.

Ms. Ruby Sahota (Brampton North, Lib.): I'd like to start by saying to the Canadian Bankers Association that so far this committee has heard only really great things about the effectiveness of the banks in the area of cybersecurity. Most witnesses have told us that the banks are basically leading the way.

I'm very curious about how much of an investment this has been for the banks, how you work with other banks overseas and what partnerships you have. You mentioned in your introduction that you think it's important for the government to invest in academia—I believe you were saying to establish a cybersecurity curriculum and to invest in that area.

Have you already been doing that on the private side as well? If so, can you elaborate on what institutions you've been working with and where your cybersecurity experts train and upgrade and get their skills?

There's a whole bunch of questions in there, I know, but you can tackle them one by one.

Mr. Charles Docherty: I'll speak to some of that, certainly.

In terms of skills development, the banks are heavy investors in hackathons and these types of events that are aimed at promoting cyber-skills within Canada.

Andrew, is there anything you'd like to add?

● (1635)

Mr. Andrew Ross: Certainly, the banks are fortunate to have the resources to put against cybersecurity risks. As we mentioned in our remarks, trust is at the forefront of everything we do in banking, so we need to invest significantly in cyber. We do a number of things in the private sector. We mentioned our own CBA cybersecurity summit, where we have a thousand security experts from the various banks come in for a one-day session. As well, many of the banks have invested in partnerships with universities across the country and around the world.

Ms. Ruby Sahota: What universities are leading the way in this area?

Mr. Andrew Ross: There are a number of them. Waterloo is one, with quantum computing. We also see a lot of work being done out west. New Brunswick has had a significant focus on cybersecurity. There are various hubs that continue to pop up. Obviously, Canadian banks want to support it. We do think there is a good story in Canada; we're starting from a good place. But there is a worldwide shortage, and we see a continued shortage of cybersecurity expertise. It's important to get it into the everyday psyche of Canadians, which is why we suggested starting with public school education and getting people thinking about cybersecurity as a first order of business.

Mr. Charles Docherty: In terms of specific examples of investment, our members have funded cybersecurity labs at the University of Waterloo. Members have invested internationally, including in Ben-Gurion University in Israel, which is a globally renowned cybersecurity hub. Another member has a strategic alliance with the Israeli bank, Leumi, and the National Australia Bank to collaborate in areas of digital banking, financial technology and cybersecurity. We've got a few examples of investment both with Canadian institutions and abroad.

Ms. Ruby Sahota: Where do your members hire professionals in-house? Are they able to find people in Canada or are they hiring from overseas? If so, where?

Mr. Charles Docherty: They're not restricted in whom they hire. Certainly there is a global shortage of cyber-skills out there, so they're looking in every country to try to find cyber-talent to protect the personal information of the clients we serve.

Ms. Ruby Sahota: Have there been repercussions in terms of fines, or has it been just in the interest of public security and in the interest of keeping business going? What has motivated the banks to be leading the way in cybersecurity?

Mr. Andrew Ross: I think it's maintaining the trust that Canadians have come to expect from the banking sector. I think it's the whole financial stability of the economy in general.

We've been very vocal in our interest in sharing our knowledge with other sectors. We mentioned in our earlier remarks that the banks are strong supporters of the Canadian Cyber Threat Exchange. This will essentially allow the banks, which are very good at detecting cyber-incidents, to share with others who may not be as capable.

Ms. Ruby Sahota: How much time do I have?

The Chair: A little less than two minutes.

Ms. Ruby Sahota: Okay.

Recently there was some news about a digital currency company called Quadriga. I was wondering if you've heard a little about that. After the owner died they discovered that the digital currency that people had invested in was completely empty. Apparently they were called “wallets” or something—it's like a Bitcoin, I guess.

How do you feel about the current regulations these companies operate within versus the regulations the banking industry is required to operate within? Do you have any comments on that?

● (1640)

Mr. Andrew Ross: As far as I'm aware, the government is looking at some cryptocurrency legislation. Those entities currently fall outside the financial sector, or at least the requirements and regulations under which banks operate.

Ms. Ruby Sahota: I know the government is looking at it. Do you have any suggestions or opinions as to how these companies can be regulated so they can better protect the digital currency they're involved with?

Mr. Andrew Ross: My only general comment would be that, as we move into a digital world, these sectors that continue to move into that space need to make sure they have the proper oversight to ensure that things like cybersecurity provisions are established.

The Chair: Mr. Motz, you have five minutes.

Mr. Glen Motz: Thank you, Chair.

Thank you for being here.

You indicated earlier that education is a big component of improving cybersecurity and the cyber-frauds that are perpetrated. Do your banks support any specific organizations that work on improving education or best practices for your consumers, or for Canadians at large?

Mr. Charles Docherty: Certainly the Canadian Bankers Association supports initiatives aimed at financial literacy. Part of that education relates to not falling for fraud scams and those sorts of things. We also have information on our website. It's Fraud Prevention Month right now so we're certainly involved in that.

I know we're heavy contributors to the Canadian Cyber Threat Exchange, so we're sharing information about cyber-threats.

Mr. Andrew Ross: We also partner with Public Safety on Cyber Security Awareness Month.

Mr. Glen Motz: Okay.

When this study was initiated, my colleague Michel Picard wanted us to focus on the.... When we talked about cybersecurity, we said we wanted to focus on the economic impacts on Canadians and on the financial end of this from a cybersecurity perspective. From many of the witnesses we've had to date, we've heard, almost exclusively, technical information about how it happens and some of the vulnerabilities that exist in our Internet and infrastructure.

I guess from a Canadian consumer perspective, from the Canadian public's perspective, there has to be, from both of your organizations, a perspective on how we can leverage this whole study, if you will, or the whole concept of cybersecurity to reduce the risk of identity theft for Canadian consumers. We all know that data's the biggest theft commodity on the black market, on the dark web. Obviously, then, that leads into financial gain.

With that in mind, what things do you see that we as a committee can do or recommend to ensure that the Canadian public is.... I know they play a role in their own vulnerabilities—we get that—but from a government perspective, what can be done to try to mitigate that risk?

Mr. Andrew Ross: To me it comes down to public awareness. If the government is able, and the financial sector is willing to work with government, to spread the word, at the end of the day, we do our best within the sector to share with our customers the vulnerabilities that exist. We need to recognize that there are a lot of vulnerabilities beyond the financial sector. If we as Canadian companies across sectors and with the public sector can get the message out on the risks that exist, that, to me, would be the number one step.

Mr. Glen Motz: That said, if companies on either side, chamber members or banking companies, identify a vulnerability in their own systems, are they prone to having that reported or would they try to cover it up? If we're talking about protecting Canadians, there's a line, and we have to make sure that we're all in the same boat together and try to fix a vulnerability. What are you seeing industries and businesses doing to deal with their own vulnerabilities in order to protect Canadians?

● (1645)

Mr. Scott Smith: If you don't mind, I might like to tackle this one. CCTX, the Canadian Cyber Threat Exchange, was mentioned a couple of times. It's a group of businesses that have gathered together under one umbrella to share information about vulnerabilities.

Maybe we want to just focus on the language here for a second. There's a big difference between a vulnerability and a breach. A vulnerability means there's a back door open somewhere and I don't know about it. There may be a threat existing on my network, but that doesn't necessarily mean there's been a breach or any significant harm from a breach. It means there's a hole I need to close up. Sharing of information is important. That's happening with a group of large businesses right now, like the banks and the insurance companies and some of the telecom companies. They're sharing information right now. What's happening is that it's not making it out to the large majority of businesses out there, which don't have a concept of what some of those threats are. I think that's the hurdle government could help cross, by getting some of that information out to those small businesses.

I know that at the CCTX they're looking for ways to engage small businesses—they've certainly come to us, and we're trying to find ways to help them do that—and to get that information out to the business community, beyond just the major banks, the telecom companies and the major transportation companies, which are all doing an excellent job right now of protecting Canadians.

The Chair: Thank you, Mr. Motz. That does bring our questioning to a close, unfortunately.

We are going to have Mr. David Masson in the next panel. In his paper he argues that industries are currently more at risk than they imagine. He says that at Fortune 500 companies, his own company has detected 80% of the time a cyber-threat or a vulnerability the Fortune 500 company didn't know about, whether dormant malware, a misconfigured network, or so on. In smaller companies the risk went up to 95%.

Mr. Smith, what would you say to Mr. Masson? He's sitting back there, right behind you.

Mr. Scott Smith: I'd say he's probably right on the smaller companies. I think the average number of days that a threat exists on a network before it's discovered is 271 days. That's probably less true of larger organizations. Honestly, I couldn't tell you what that number is. There are a number of different surveys that scatter about on what that numbers is, but it's bigger than it should be.

The Chair: With that, I unfortunately have to bring this panel to a close.

We'll suspend for a couple of minutes while we re-empanel.

Thank you.

● (1645)

(Pause)

● (1650)

The Chair: Ladies and gentlemen, the meeting is back on.

We have with us Professor Andrew Clement by video conference from Salt Spring Island, British Columbia.

You're in a better place, Professor.

We also have with us Mr. David Masson.

Given that we've had some technical difficulties today with various things, I think we should probably go with Professor Clement first so that we don't have any potential technical difficulties.

Professor Andrew Clement (Professor Emeritus, Faculty of Information, University of Toronto, As an Individual): I thank the committee for this opportunity to contribute to your important deliberations on cybersecurity in the financial sector as a national economic security issue.

l'm pleased to respond to your invitation requesting insights into the context of critical infrastructure, internet routing, routing of data and communications technologies.

ln previous hearings you've heard many valuable points, notably that Internet infrastructure is critical infrastructure not just for the financial sector but for the Canadian economy more generally; that this infrastructure is changing quickly in ways that are risky and not generally transparent or well understood; that threats to security of this infrastructure are multi-faceted, complex and growing.

ln addressing these risks, I particularly endorse Professor Leuprecht's earlier recommendation:

> that Canada should pursue a sovereign data localization strategy, reinforced by legislative and tax incentives to require critical data to be retained only in Canadian jurisdictions; set clear standards and expectations for the resilience of Canadian communication infrastructure; monitor that resilience; and impose penalties on critical communication infrastructure players who fail to adhere to standards or fail to make adjustments without which they would be left vulnerable.

I will elaborate on this recommendation made in the context of 5G networks, but will apply it to reducing the threats posed by excessive volumes of Canadians' domestic data communications, including financial data, flowing outside of Canada even when headed for Canadian destinations. These flows add a host of unnecessary cybersecurity risks while undermining Canadian economic security more generally.

To be sovereign economically and politically a nation must exercise effective control over its Internet infrastructure, ensuring that critical components remain within its territory, under its legal jurisdiction and operated in the public interest. Most obviously, this refers to locating databases. Less obviously, though no less critical, are the routes data takes between databases, users and processing centres. This latter area of vital concern is much less well understood and the one to which I direct my comments.

I'm Andrew Clement, a professor emeritus in the Faculty of Information at the University of Toronto. Beginning in the 1960s, l was trained as a computer scientist, so l've seen a lot of remarkable changes, good and bad, in the digital infrastructure that is now an essential part of our daily lives. Much of my academic life has focused on trying to understand the societal and policy implications of computerization. I co-founded the cross-disciplinary ldentity, Privacy and Security lnstitute to address in a practical, holistic, manner some of the thorniest issues raised by the digitization of everyday life. Currently l'm a member of the digital strategy advisory panel advising Waterfront Toronto on its smart city project with Sidewalk Labs.

One of my main research pursuits has been to map Internet communication routes to reveal where data travels and the risks it faces along the way. My research team developed a tool, called IXmaps, short for Internet Exchange mapping, that enables internet users to view the routes their data follows when accessing websites.

Early in our research we generated a trace route, found on the first image, called Boomerang, which shows the data path between my office at the University of Toronto and the website of the Ontario student assistance program that is hosted in the provincial government complex a short walk away.

This route surprised us, especially since the route to and from the U.S. went through the same building in Toronto, Canada's largest Internet exchange, at 151 Front Street. At the very least it challenged presumptions of maximal efficiency of Internet routing, prompting our further investigations into how widespread this phenomenon was as well as into the reasons for this counterintuitive behaviour. We dubbed this type of path—data leaving Canada before returning —"boomerang" routing. It turns out to be quite common. We estimate at least 25% of Canadian domestic traffic boomerangs to the U.S. The Canadian Internet Registration Authority, CIRA, recently put the figure much higher.

There are several problems related to Internet routing that are relevant to this committee.

The longer route adds risk from physical threats, even as banal as a backhoe cutting through the fibre optic cable. The extra distance adds both expense and latency, undermining economic efficiency and opportunity.

● (1655)

Data passing through major switching centres faces bulk interception by the United States National Security Agency, the NSA. Even before the Snowden revelations, we knew that New York and Chicago were prime sites for NSA surveillance operations. It not only poses risks for Canadians' personal privacy, but also for financial and other critical institutions. At your latest meeting, Dr. Parsons pointed you to a Globe and Mail report that the NSA was monitoring the Royal Bank of Canada and Rogers' private networks, to mention only those beginning with the letter R. The article suggested that the NSA's activities could be a preliminary investigative step in broader efforts to "'exploit' organizations' internal communication networks".

Boomerang poses a further, more general threat to national sovereignty. If one country depends on another for its critical cyber-infrastructure, as Canada does with the U.S., it makes itself vulnerable in multiple respects—and not just from their spy agencies or to shifts in the political relationship, as we're seeing now. Will even the best ally keep the interests of its friends in the fore, when its own critical infrastructure is threatened? If the U.S. experiences a cyber-attack, might it not feel compelled to shut down its external connections, leaving Canada high and dry? Previously, you've heard that some see Canada as a softer target than the U.S. and, hence, potentially, as an entry route into the U.S. At some point, might the U.S. see Canada as a source of threat and disconnect us?

So far I've focused on the risks from routing Canadian domestic traffic through the U.S. A similar argument applies to Canada's communications with third countries, but even more so. Our mapping data suggests that approximately 80% of Canadian internet communications with countries other than the U.S. pass physically through the U.S. This is related to the relative lack of transoceanic fibre cabling that lands on Canadian shores, as shown clearly in the maps produced by the authoritative TeleGeography mapping service. You can see the slides, I hope.

Only three transatlantic fibre cables land on our eastern coast, compared with much greater capacity south of the border. Most of our traffic with Europe goes via the U.S. Remarkably, on our west coast there are no trans-Pacific cables, so all traffic with Asia transits the U.S. One way of assessing how well banks can withstand severer financial downturns is subjecting them to stress tests. What would a stress test of Canada's cyber-infrastructure reveal? If, for whatever reason, our connection with the U.S. was cut, even in its own legitimate self-defence, how resilient would Canada's Internet prove to be? We should know the answer, but we don't. However, the evidence available suggests very poorly.

What should we do about this? Broadly speaking, the appropriate policy response, as mentioned, is to pursue a strategy of “sovereign data localization” that includes data routing. More concretely, this would involve a coordinated set of technical, regulatory and legislative measures designed to achieve greater resilience.

First, we should require that all sensitive and critical Canadian domestic data be stored, routed and processed within Canada. Second, we should support the development and use of Canada's Internet exchange points for direct inter-network data exchange to avoid U.S. routing. CIRA has lead the way on this. Third, we should increase fibreoptic capacity as needed within Canada, as well as between Canada and other continents. Fourth, we should include transparency and accountability reporting requirements in cybersecurity standards for financial institutions and telecom providers, in relation to routing practices. Fifth, we should establish a Canadian cyber-infrastructure observatory, with responsibility for monitoring Canadian cyber-infrastructure performance and resilience, responding to research requests and reporting publicly.

Thank you for your attention and I look forward to your questions.

● (1700)

The Chair: Thank you, Professor Clement.

Mr. Masson, you have 10 minutes, please.

Mr. David Masson (Director, Enterprise Security, Darktrace): For the sake of brevity, I won't read it all because I believe you've all got a copy on your desk.

Good afternoon, Mr. Chair, members of the committee and ladies and gentlemen. My name is David Masson, and I'm the country manager for Canada of Darktrace, a cybersecurity company.

We are the world's leading AI company for cyber-defence. We have thousands of customers worldwide, and our self-learning AI can defend the entire digital estate that people have. We've more than 800 employees—actually, it's 900 now—and 40 offices worldwide, and here in Canada we have three offices.

Prior to joining Darktrace and establishing the company in Canada in 2016, it was my immense privilege and honour, as an immigrant to Canada, to serve my country at Public Safety Canada for several years. Prior to that, I had worked inside the United Kingdom's national security and intelligence machinery, and had done so since the Cold War. I've been a witness, as the previous witness just said, to cyber's evolution over time, from before the Internet to its current mass prevalence and ubiquity in our society today.

In earlier meetings of this committee, I think you heard an awful lot about the scale and size of the cyber-threat that exists in this country, so I'm going to focus on three things. First I plan to share with you some reasons why cybersecurity poses a seemingly insurmountable challenge, and I'll dive into some specific threats. I'll close by offering some suggestions and solutions to these issues.

What we're seeing at Darktrace is that most organizations, unfortunately, aren't as secure as they think they are. When we install our artificial intelligence software in the networks of a Fortune 500 company—sir, you mentioned this earlier—80% of the time we detect a cyber-threat or vulnerability that the company simply did not know about. Outside of the Fortune 500, when we look at smaller businesses, this percentage of companies compromised in some way jumps up to 95%, so that's pretty much all the time.

These statistics highlight two things. First and foremost, obviously, no organization is perfect or immune. Organizations of every size and every industry not only are vulnerable to cyber attacks but are currently more at risk than they imagine. Successful attacks against some of the biggest companies in recent years have revealed that something isn't working. Even Fortune 500 companies, which have budgets, resources and staff to deal with cyber-threats, are still found wanting.

Second, this raises the question: Why are so many companies and organizations unaware they are under attack or vulnerable? The legacy approach that businesses have previously taken to cybersecurity does not work in the face of today's threat landscape and increasingly complex business environments.

In brackets, it's not just the cyber-threat that we're facing. It's actually just business complexity that's bamboozling people.

In the past, companies were focused on securing their networks from the outside in, hardening their perimeter with firewalls and endpoint security solutions. Today, migration to the cloud and the rapid adoption of the Internet of things has made securing the perimeter nearly impossible. Another traditional approach, known as rules and signatures, relied on searching for known bad. However, attackers evolve constantly, and this technique fails to detect novel and targeted attacks. Most importantly, these historical approaches fail to provide businesses with visibility and awareness into what is taking place on their networks, making it hard, if not impossible, to identify threats already on the inside.

I'll now look at two potential types of attack that have far-reaching impacts.

Attacks against critical national infrastructure are increasing around the world. When one mentions critical infrastructure, people commonly think of power grids, energy and utilities, companies, dams, transportation, ports, airports, roads. However, Canada's financial sector, the purpose of this committee, the big banks, etc., are also part of a nation's critical infrastructure. Just as roads connect our country physically, these organizations connect the national economy. A successful cyber-attack against these core institutions could dramatically disrupt the rhythms of commerce. The security of financial institutions should be discussed in the same breath and with the same severity as the security of our power grids.

Another type of attack that's more common in recent years is trust attacks. These attacks are not waged for financial gain. As a company, we haven't been able to work out what the financial gain of these attacks is. Instead, they're waged to compromise data and data integrity. Imagine an attacker is looking to target an oil and gas company. One tactic would be just to shut down an oil rig, but another more insidious type of attack would be to target the seismic data used to identify new locations to drill. Effectively, what they do is they get the company to drill in the wrong place.

I also want to touch briefly on what we at Darktrace think we can expect from the future of cyber-attacks. We use artificial intelligence to protect networks, but as artificial intelligence becomes ubiquitous in seemingly every industry, it is falling into the hands of malicious actors as well. Although there's some debate as to when exactly we'll see AI-driven attacks, we think it might be this year, but others think 2020 or 2025. They're something that we will no doubt have to contend with in the near future.

● (1705)

Darktrace has already detected attacks so advanced that they can blend into the everyday activity of a company's network and slip under the radar of most security tools.

Up until now, highly targeted advanced attacks could only be carried out by nation-states or very well-resourced criminal organizations. Artificial intelligence lowers the bar of entry for these kinds of attacks, allowing less-skilled actors to carry them out. AI is able to learn about its target environment, mimic normal machine behaviours and even impersonate trusted people within organizations.

Companies will soon be faced with advanced threats on an unprecedented scale. We think it's critical that companies and government—both in Canada and around the world—consider what this will mean and what steps need to be taken to ensure that they can defend against AI-driven attacks.

As this committee and the broader industry looks for answers and solutions, I want to propose a few.

In October 2018, (ISC)^2 announced that the shortage of cybersecurity professionals around the globe had soared to three million. I saw this figured repeated again this morning on LinkedIn. Roughly 500,000 of these unfilled positions are located in North America. In Canada, I think we're seeing 8,000, but I suspect it's more. This shortage is only expected to increase. Businesses are struggling to hire professionals. Those individuals they can hire are struggling to keep up.

Threats are moving at machine speeds now. In the time that an analyst steps away to grab cup of coffee, ransomware can enter a network and encrypt thousands of files. Beyond these machine-speed attacks, analysts are faced with a deluge of alerts around supposed threats that they need to investigate, handle and remediate. We need to find a way to lighten the burden for cybersecurity professionals, expand the field of potential candidates by hiring more diversely, and arm them with the technology and tools to succeed.

I'll skip the next two paragraphs.

Collaboration between the private and public sector will also be key to solving the challenges we face. The previous witnesses spoke to some of that. Governments around the world collect a wealth of information on adversaries' attacks and attack techniques. Although certain limitations about what governments can share is understandable and necessary, I'd urge the Canadian government and the intelligence community to share what information they can with corporations. Information is an asset. If companies understand the attacks they are facing, they can better defend against them. The Canadian economy is better ensured from the impacts of these cyber attacks.

On the other hand, it's critical that private companies like mine share insights and lessons-learned with the government. The private sector's ability to pivot quickly and trial new technologies make it in some ways a testing ground for new cybersecurity technologies and techniques. Through discussions around what's working and what isn't, the government can learn what's necessary for companies to succeed, compile and disseminate this information—perhaps through CCTX, which I know has been mentioned several times—and help entire industries quickly improve their security practices.

I want to close with a call for innovation. Attackers are constantly coming up with new ways to infiltrate networks, attack businesses and wreak havoc. It's critical that we, the defenders, are innovative as well. Whether this be by developing novel technologies, adopting cutting-edge techniques or enacting new regulation, creative thinking and collaboration are going to be the key. At the end of the day, it's not just about keeping up with attackers, but getting one step in front of them.

I look forward to your questions.

Thank you.

● (1710)

The Chair: Thank you so much, both of you, for your presentations.

With that, we'll go to Ms. Sahota for seven minutes, please.

Ms. Ruby Sahota: Thank you for both of your presentations. They were very insightful.

Recently the Diplomat & International Canada magazine published a survey in which sources said they were concerned about their online privacy. Their top concern was cybercriminals; the second was Internet companies themselves attacking their privacy.

Do you think that companies, especially social media companies and any that you probably have as clients, could be doing more, not only to ensure that their users' data is protected but also to ensure that users have a sense of protection? From your presentation, it seems like things are very grim. With all of the technology we're using, everything is in the cloud now. It seems like it's more unsafe than ever.

Where do we go from here? I know you've proposed a couple of solutions. In terms of innovation and investment by the government, you talked about exchanging information between the private sector and the government. How do you think a government can spur innovation?

You mentioned regulations as well. How do you think they can regulate it? Is there something we can do? Is there a jurisdiction that's doing it better than us at this point? What lessons should we learn from them?

Mr. David Masson: Those are a lot of questions.

On the social media bit, can I ask the professor to step in first? I think his take will be slightly more interesting than mine.

Prof. Andrew Clement: Well, I don't know about that, but yes, there has been a great deal of press recently about the role that social media companies play, particularly Google and Facebook, because of their business model, which requires the monetization of personal information and the communications between individuals.

I would say that they in particular need to be subject to much greater regulation and we need to understand much better what they are doing. This is a moment, particularly in the case of Facebook, when this can be pressed because we are learning almost daily about the behind-the-scenes work they have been doing of resisting oversight, and also of how they are trying to monetize this. That would be one place to start, with the largest of those.

Ms. Ruby Sahota: Is any jurisdiction ahead of us in regulating these companies?

Prof. Andrew Clement: Well, certainly Europe is, with their recent GDPR, the General Data Protection Regulation, which I believe you've heard about and that imposes stiff penalties. They have fined some of these companies for various offences. I would look to Europe as not necessarily being ideal, but they are doing a much better job in grappling with this than Canada or the United States.

Ms. Ruby Sahota: They are definitely imposing major fines. Do you have an data on the effectiveness of creating regulations that impose fines? Has there been an increase in the number of companies stepping up and increasing their security when it comes to—

Mr. David Masson: I will give you a quick example of GDPR working. When Facebook got hacked last year, they told the Irish data commissioner within 24 hours that they had been hacked, and the provision under the GDPR is 72 hours. They didn't hang about. They admitted it pretty damn quick. So there you go: It's that's an effective piece of legislation, I would suggest.

Ms. Ruby Sahota: Yes.

Did you want to say something.

Prof. Andrew Clement: Oh, I would just say that these are still early days for the GDPR. It only came into effect in May last year. It certainly got people's attention. I don't think there has been time to study its effectiveness, but I would say that the signs are good that it is beginning to grapple with the issues. Canada faces the challenge of determining whether its own privacy legislation, PIPEDA, will be considered substantially equivalent to the GDPR. Hopefully, PIPEDA will be strengthened so that an equivalency determination can be maintained.

● (1715)

Mr. David Masson: I go to a lot of conferences and trade shows, and for the last couple of years everybody has been talking about the GDPR. As a new immigrant to Canada, I was a bit upset that nobody seemed to be concerned about the Digital Privacy Act and the upgrade to PIPEDA that we were going to do. People were more worried about the effect of GDPR than our own legislation. They are probably right to have been worried because the GDPR is more draconian than ours, I believe.

In ours, you don't have to report by a specific time other than “as soon as possible, please”. There was talk of fines of up to $100,000, but I haven't actually seen it actually saying what you have to pay. At the end of day, it's about breaches of personal information; it's not about breaches in general, whereas GDPR, I think, covers both of them.

Ms. Ruby Sahota: Okay, thank you.

Do I have another minute?

The Chair: You have a little more than a minute.

Ms. Ruby Sahota: Okay, perfect.

A lot of this work comes down to money and how much the government has to spend on making investments in the right place. We definitely put a lot of money towards cybersecurity in our last budget, over $500 million, so it's definitely a step in the right direction the government is taking.

Where would you like to see the funds spent, and if there is more funding needed, where should that funding go?

Mr. David Masson: I think one of the best steps in the right direction was absolutely setting up the Canadian Centre for Cyber Security as a one-stop shop, because prior to that, there was a bit of confusion about whom to talk to. I mean, if anybody gets hacked, whom do you call? Nobody is really sure about that. That's not a great place to be.

They probably want to put some more money into considering some more regulation. History shows that large conglomerations never do anything until they are forced to, but I've shown you that Facebook certainly jumped to it with GDPR when they got hacked, so you probably want to look into that. In addition, you probably want to look into some more legislation to stop foreign influence in elections, looking at fake news and foreign influence activity. That's actually in there. You probably want to do a bit more on that front.

The Chair: We'll have to leave it there, unfortunately. Ms. Sahota's time is up.

[*Translation*]

Mr. Paul-Hus, you have the floor for seven minutes.

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

My colleague's question is in keeping with my approach to this matter.

You mentioned that Canadians always say “please”. I think that we Canadians are very naive when it comes to cybersecurity. We always think it is someone else's problem, or we don't dare act.

Mr. Masson, regarding Canada's general stance on cybersecurity, without mentioning artificial intelligence and future issues, do you think we are seriously behind with regard to protection?

Our current study is about banks and the financial system. On a scale of one to ten, how would you rate the vulnerability of our banking system?

[*English*]

Mr. David Masson: I'll go first, Professor, but I'll be very quick.

A lot of effort in Canada goes into what we'll do after it happens. We'll wait until it happens and then we'll deal with it. A lot of effort goes into dealing with it afterwards. I really would like to see Canada put more effort into not having the hack in the first place, into making sure it doesn't happen, or into doing our best to make sure it doesn't happen. A lot more effort could be done that way.

In terms of the banking system, outside of government there's not a lot of information about the scale of the threat we face in Canada. Inside government, where I used to be, there's a lot. I'm sure you've heard talk about the millions of hacks at the government, but outside of government we don't really know. With the DPA coming out last week, with the provisions for reporting breaches of privacy through cyber-activity to the Office of the Privacy Commissioner, we probably have a chance now to get a better evaluation of what the scale of the threat is outside of government. I'm not entirely sure if the Office of the Privacy Commissioner is the right place for that, to do evaluations, but that's where it will be that they will gain that information.

To give you a scale of one to 10 on the banks, who pretty much keep to themselves—albeit I'm sure they're very open with the Bank of Canada—I'd be swimming it to come up with an assessment for the banks, to be honest with you. I'm going to say that they're probably better than most western liberal democracies that we live in. The fact is that Canada has a history of fairly good regulation of the financial system, which is why Canada didn't suffer the way everybody else did in 2008. They were still buffeted by it afterwards, but they came out reasonably okay. So I would go for about a seven or an eight. There you go.

● (1720)

[*Translation*]

Mr. Pierre Paul-Hus: I'd like to go back to the matter of attitude. As you confirmed, it's important today to understand the Canadian attitude to the problem. Do you think it is important to put out the message that we have to have a firm attitude?

You worked for another government in the past and you now work in the private sector. I know that people who worked for the government and are now in the private sector have a very different view of the issues. People who came to meet with us from HackerOne, for instance, or other enterprises, have a clear vision of things.

From a governmental perspective, there are always obstacles, and people only talk about investment. It is true that investment is important, but should our attitude to the problem be very different, starting now?

[*English*]

Mr. David Masson: Yes; I will say yes. I mean, you need a carrot and a stick, but you probably do need a bigger stick. The DPA is saying that you have to report breaches as soon as possible. Really? Why not go for the 72 hours like everybody else? Yes, definitely you could beef up the stick part; absolutely.

For a carrot in terms of investment, replying to something that Ms. Sahota said earlier, it would certainly be directing your investment into those parts of the Canadian private sector, but probably more academia, that are doing some really innovative work right now in combatting this problem and allowing the private sector, who, as I said before, can pivot quite quickly, to fail forward and fail fast. We do that all the time. We're not bothered about it; you know, failure's success. Put that investment in those companies who are prepared to do that to try to get to where we need to be as quickly as possible.

The professor might have a comment on that.

Mr. Pierre Paul-Hus: I have another question for him, if I may.

[*Translation*]

Mr. Clement, you wrote an article entitled “Addressing mass state surveillance through transparency and network sovereignty, within a framework of international human rights law—a Canadian perspective”, which was published in a special issue of the *Chinese Journal of Journalism and Communication Studies*. I'd like to know how that article was received in China.

[*English*]

Prof. Andrew Clement: That's an interesting question. I can't really speak to that specifically. I was invited to an Internet governance session in Beijing, and I've been writing about network sovereignty for some time, but I was also aware in going to China that Chairman Xi Jinping used the term “network sovereignty” in a very, very different sense about Chinese Internet infrastructure.

I took pains to make it clear that the sovereignty needed to be understood within an international framework of human rights, and that's what I developed in that. My presentation was very well received by some of the people in the audience. I got compliments for it, and the editors were keen to have it published in the journal that came out of it, but it was published in Chinese, and, unfortunately, I have not heard anything further from them.

I don't know if it was met with stony silence, or whether people are quietly appreciating it, which is what I hope. Thank you for finding that paper.

● (1725)

The Chair: Thank you, Mr. Paul-Hus.

Mr. Dubé, you have seven minutes, please.

Mr. Matthew Dubé: Thank you, both, for being here.

Mr. Masson, sticking with machine learning and AI.... In this study, we've looked a lot at the implications of non-state actors—people trying to steal money, and things of that nature. It's a very abstract idea, but I'm just wondering where your thoughts are on the uses of AI by state actors. In other words, we've clearly delineated what the boundaries are for use of force and, for example, when there's a conflict between countries, what a war crime is, and things like that. Unless I'm mistaken, I don't think that delineation is quite as clear when it comes to attacking critical infrastructure, particularly if we're using this kind of machine.

I'm just wondering—and this question is kind of open-ended—what your thoughts are on how state actors are deploying this and what kinds of concerns there could be in the financial sector, or others that could potentially be affected, where those rules of engagement don't necessarily exist yet.

Mr. David Masson: I used to be a British diplomat. I remember 12 or 14 years ago having it explained to me that a cyber-attack by a nation state or another state was an act of war. However, ever since then, it seems to have become a very, very grey issue. I was at a conference the other week where it cropped up again, and nobody could actually define at what point you reach that stage. Maybe it's because a lot of the time it's been easier, particularly for western democracies, to just ignore that issue, for obvious reasons.

State actors are investing heavily in AI because everybody is investing heavily in AI. The witnesses who were here before invest a lot in AI for their banking systems. This isn't about cybersecurity or cyber-attacks. They're just using AI because AI can do so much more so much more quickly and so much more accurately.

We use AI because we are saying that human beings can't keep up with the scale of this threat, so we use AI to do all the heavy lifting for human beings. It's a bit of a myth to say that AI is going to replace people. That is not the case. There is no broad AI [*Editor—Inaudible*]. That doesn't exist.

What you see at the moment is AI being used for specific purposes for specific tools in specific areas. We use it for cybersecurity, but the bad guys—and I'm happy to say “bad guys” because we get stuck with the Internet of things—are going to use it because it's going to make things easier for them. In my statement, I pointed out how some of the nation state attacks that we used to see, such as the attack against Sony—a lot of resources went into that—or some of the attacks we've seen in Ukraine, need people, time, money and effort. However, if you use AI to do that, you need less money, time and effort, and, as I say, it will lower the bar for entry to these kinds of attacks.

When we see the first AI attack—we, as a company, think it might be this year; we've been seeing hints of it for quite a few years, but it could be later on—many of the current techniques and systems that are used for protecting networks from cyber-threats will become redundant overnight. That will happen very, very quickly.

Some state-threat actors and others are using AI in the foreign influence field, in the misinformation campaigns that go on. There's a lot of stuff about that. You may have noticed that some of the media platforms have been heavily criticized following the horrendous attacks in New Zealand because they didn't do anything about it quickly enough. But now, if you use AI—we can do it now—you can construct a lie at scale and at speed. It doesn't matter how palpably untrue it is. When you do that, that sort of quantity develops a quality all of it's own, and people will believe it. That's why bad guys are going to start investing in AI.

Mr. Matthew Dubé: So, my question becomes this: If we look at Bill C-59, for example, where you're giving CSE defensive and offensive capabilities—and part of that is proactively shutting down malware that might be...or an IP, or things like that—is there concern about escalation and where the line is drawn?

Part of this study.... The problem is that we're all lay people, or most of us anyway—I won't speak for all—when it comes to these things. My understanding of AI—because I've heard that, too—is that it's not what we think of it as being from popular culture. Does that mean that if, due to employing AI to use some of these capabilities that the law has conferred on different agencies, AI is continuing...? How much human involvement is there in the adjustments? If that line is so blurry as to what the rules of engagement are, is there concern that AI is learning how to shut something down, that the consequences can be graver than they were initially, but the system is sort of evolving on its own? I don't want to get lost. I don't know what the proper jargon is there, but....

● (1730)

Mr. David Masson: It's already the case that some attacks that large actors carry out might be targeted against a particular target, but they don't consider collateral damage. There was an attack a few years called NotPetya. It targeted Ukraine, but it spread worldwide and caused havoc absolutely everywhere.

With regard to the way that people are using AI now—when I talk about narrow AI, that is specific tools for specific occasions—if your concern is that they'll launch an AI attack and it will develop a mind of its own and do its own thing, that's not the case. This is the kind of AI where there's still a pilot in the cockpit. There are still human beings running it and deciding to let it loose. You're still going to get collateral damage, particularly if it's unregulated state actors that are doing it—

Mr. Matthew Dubé: If I may, because my time is running out....

My intention was less about humans losing control and that caricature of it, and more just wondering about if they're learning the best pathways to be on the offensive, for example.

Mr. David Masson: Any offensive that a country like Canada is likely to have will have been thought through very carefully. It's not just a case of being able to judge the impact you're going to have; that's absolutely what they'll be doing before they launch this.

Mr. Matthew Dubé: The pathways you're perhaps unintentionally shutting off aren't at random.

Mr. David Masson: You will have to be absolutely accurate on what they're going to do.

The Chair: You unfortunately have about 20 seconds. You can save it for the final round. Thank you.

Mr. Graham, welcome to the committee. Bear in mind the translators are trying to translate whatever language you're speaking.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): If they can encrypt me in real time, we'll be all set.

I have a lot of questions, so I'll ask you to keep your answers as short as my speaking, if it's possible. They're to both of you, not specifically to one or the other.

To start with, what's the life expectancy of an unpatched or unmaintained server on the Internet? If somebody puts a server on the Internet and doesn't touch it again, how long is that going to be online?

Mr. David Masson: Minutes.

Mr. David de Burgh Graham: That's an important point.

Mr. David Masson: When you talk of a patch, you should patch the minute they tell you.

Mr. David de Burgh Graham: For the record, what's a zero-day?

Mr. David Masson: A zero-day is an attack that nobody has seen before. It's completely new and novel.

Mr. David de Burgh Graham: You mentioned earlier there's a shortage of about a half a million cybersecurity employees or professionals. I've been involved in the free software community for about 20 years and the people around me today are very much the same people who were around me 20 years ago. How do we modernize the people in the software industry and the cybersecurity industry? How do we get the next generation to be interested in it and to learn it?

Mr. David Masson: I would highly recommend the efforts of the Province of New Brunswick, which has has been teaching cybersecurity in school for some years now, to the point where major companies are now snapping up kids when they graduate at 18.

Mr. David de Burgh Graham: Okay. Do we generally do security by design or are we more reactive as a society?

Mr. David Masson: Right now, it's reactive. I'm a big fan of Dr. Ann Cavoukian when she talks about privacy by design—and it should be “security by design”.

A new term has come out called Sec and DevSecOps and DevOps —that is, as you're writing your code, you should be considering security, absolutely.

Mr. David de Burgh Graham: Dr. Clement, make sure that if you have something to say, you speak up, because I'm going through this fairly quickly. Don't be shy.

Prof. Andrew Clement: Sure.

Mr. David de Burgh Graham: Are there advantages in security of open source versus closed source that you know of? Is there any security in having a closed-source system, where there's no public access to that code?

Mr. David Masson: Professor?

Prof. Andrew Clement: Being able to keep a code open so it can be checked is an important means for ensuring confidence and security.

Mr. David de Burgh Graham: We've heard a lot of security concerns about Huawei devices and a lot of discussion about whether we should ban Huawei in Canada. Is the issue with Huawei that their hardware may have Chinese back doors, as opposed to back doors endorsed by Five Eyes agencies, for example. Where is the source of the issue and is there such a thing as an uncompromised or uncompromisable system?

Mr. David Masson: Professor?

Prof. Andrew Clement: I don't think there are uncompromisable systems, and I would caution that in some ways Huawei is mirroring what's happened to the undermining of security in western-developed technologies.

● (1735)

Mr. David de Burgh Graham: There has been a lot of talk over the years about software and having back doors. Once a back door is in place, is there any way to ensure that only the organization that asked for it to be there can use it, or once the back door is there, can anybody get to it?

Prof. Andrew Clement: I wouldn't say anybody could get to it, but once you've created a back door, you've opened the possibility that people you don't know and don't want can access it.

Mr. David de Burgh Graham: Right. Do we know how much of our Internet infrastructure is compromised at the manufacturing point? A couple of months ago there was a story about a motherboard found to have an extra chip inserted on it at the factory. I don't remember who it was, but you've probably run across this.

Prof. Andrew Clement: I don't know of any estimates. I think it would be extremely hard to find, and we are discovering things that were buried in code ages ago. It's a very difficult thing. We need much more transparency and ability to interrogate code and devices.

Mr. David Masson: And interrogate the supply chain.

Mr. David de Burgh Graham: That makes sense.

Professor Clement, in your opening comments, you talked about our ability to move data within the country versus outside the country. Do we have the network capacity to move all our data within Canada today, or is expanding our Internet infrastructure a question of national security?

Prof. Andrew Clement: I don't have a measure on the actual capacity versus what we need, but my guess is that we have unused capacity that would be available and that we would need to assess our internal domestic requirements and then make the decision about investing in capacity. The investment will be very small compared with the kinds of investments we've made previously in other network infrastructure, starting with the railway.

Mr. David de Burgh Graham: Fair enough.

Are either of you familiar with Quintillion and their project in the Arctic?

Prof. Andrew Clement: I'm not.

Mr. David de Burgh Graham: I'll come back to this at a later date.

Do you have any servers in Canada, because all of the traffic at base essentially starts with a DNS request? Do you have any servers besides .ca in Canada?

Prof. Andrew Clement: I don't know of any.

Mr. David Masson: I don't know of any.

Mr. David de Burgh Graham: All traffic at some point has to at least communicate with outside of the country to at least express the initial intention of who wants to talk to whom. That metadata is available to whoever has the route service, which is mostly in the U. S.

Prof. Andrew Clement: Yes.

Mr. David Masson: If the server is not here, somebody else has access to it. Remember that when it comes to the cloud. It's not a cloud; it's a server somewhere.

Mr. David de Burgh Graham: Oh, that's right. It's not a cloud; it's somebody else's computer.

Are we sure that AI base attacks are not already running?

Mr. David Masson: We thought we saw an algorithm fight an algorithm in 2015, and we've seen hints of it since, but we haven't actually seen a full on AI attack yet. That's we, the company. I can't speak for anybody else.

Mr. David de Burgh Graham: So it's clearly in development. The black hatting of AI base attack is definitely in development.

In the study we've talked an awful lot about privacy but a whole lot less, I find, about security. I want to know, in the root causes of cyber-mobility—I know I don't have much time left—what's the role of default passwords and default back doors? I talked about back doors earlier. There's a huge amount of hardware out there that has “admin” as the login, “admin” as the password to log into it, and you can do anything you want with it. How big a problem is that side of things?

Mr. David Masson: It's a major problem. It's one of the things I talk about all the time. I say, if you buy an Internet of things device, for God's sake, change the default password as soon as you get it in the house, if you can change the default password.

Mr. David de Burgh Graham: Do I have time for one more?

The Chair: No more.

David, you've got in about three committee meetings' worth of questions in seven minutes.

Mr. David de Burgh Graham: I like to question the witnesses.

The Chair: Yes, high compression. David was compressing you.

Mr. Motz, a lower compression rate, for sure, thankfully.

Mr. Glen Motz: Dr. Clement, you wanted to speak on a number of occasions there and didn't get an opportunity. I want to give you an opportunity to interrupt David and say what you want to say.

Prof. Andrew Clement: Partly, I might have given expressions of interest because I was supporting some of the statements that Mr. Masson was making. I guess the one comment that I wanted to get in had to do with the question of investments. I guess the question was whether the Canadian government was well-enough prepared to deal with these cyber-threats.

My view is that a big part of the problem we encounter now has been the way in which the development of the Internet and services on it have been driven almost entirely by the business interests of entrepreneurs. Obviously, in many cases, they're doing wonderful things, but governments have explicitly had a hands-off approach, and I think we are reaping some of the costs of that. Part of that is that now I would say that public institutions have lost an image of what a publicly oriented infrastructure would even look like. That, I think, is a deep, structural problem that needs a lot of education and talk. That, I think, would have protected us quite a bit.

Go a bit slower, but do things more carefully and more transparently so that they can be held more accountable. The urgency of more innovation, pile-on innovation, very often deepens the problem, because we're fixing problems that we should have thought about more carefully.

● (1740)

Mr. Glen Motz: That's a great segue to a comment that both of you alluded to just a few minutes ago, which was the interrogation of the supply chain. How do we go about that? How do we best ensure that the supply chain we talk about is secure and safe? How is that best accomplished? Is it accomplished as you suggest, Dr. Clement, through government intervention, or is it best accomplished in some other way?

I ask both of you the question.

Mr. David Masson: I'll let the professor go first.

Prof. Andrew Clement: Go ahead.

Mr. David Masson: Okay.

What I would suggest you do is to accept that threats are going to get inside. In fact, accept that a threat has already arrived. Maybe it arrived through your supply chain, through your third party vendors and all that kind of thing. Expect that it's going to happen and start coming up with some systems that expect this to happen but can find it without having to know what it is and without having to know what the bad stuff is.

There are a lot of stringent regulations right now. I think CSE publishes a lot of stuff about what you have to abide by when you get a government contract, but at the end of the day, if somebody got at the chip in the factory, as one of the MPs mentioned earlier, the only way you're going to find out about it is once you've plugged the chip in and have seen what has happened.

Prof. Andrew Clement: This gets into oversight mechanisms. While there are some, I would say that they are lagging behind in the development of these complex systems. I would be particularly careful when you develop highly tightly coupled systems, so that when something goes wrong, the damage can spread quickly. Allow for some buffers in there. That's not the nature of competitive supply chains, because speed is primary, but if we take a longer strategic view, then we need to slow down a bit and pay closer attention.

Mr. Glen Motz: I have one last question for both of you.

We know that in this country and across the globe there are higher rates and a higher incidence of cyber-intrusion. The theft of data and the theft of finances seem almost inevitable. I think the Canadian public almost seems immune—it's going to happen anyway—unless or until it happens happens to them, and then it's a big problem.

I hate to be a doomsdayer, but should we be preparing for this to be a common occurrence, in that if you're hooked up to the Internet, you're going to get hacked and you're going to get stuff stolen, so get used to it? Or are we saying that there's hope on the way?

The Chair: Very briefly, please.

Mr. David Masson: Can I go first? I'll just say that if you use AI, there's hope. All right? If you use AI, you can get ahead of the attackers and put the advantage back in the hands of the defender.

Professor.

Prof. Andrew Clement: Yes, I would say that we don't accept that kind of approach in other areas of our vital infrastructure. As in the development of other infrastructure, we need to look much more closely and carefully at what's being put in place and have it meet public interest requirements, so that we're not just loading things onto the public and expecting them to suck it up, which is basically what's happening now.

● (1745)

The Chair: Thank you very much, Mr. Motz.

Mr. Picard, please, for five minutes.

Mr. Michel Picard: As a government, if I ask what are the steps I should look for in terms of building my cybersecurity, it's as if I'm assuming that I don't have a system in place. I think it's fair to say that my system should be fair to good somewhere, because I do have agencies that work with me. I have protection. I have systems. I have tools. I'll just twist my question. What are the steps that I should make sure I have covered and on which I can build something strong and improve on that? What are the main parentheses?

The Bankers Association said that the best solution for good cybersecurity was awareness. If I base my cybersecurity on publicity, I'm in trouble, I think. I need more than just publicity and awareness. What are the main topics that I should address in order to make sure that I have at least the basis for a good cybersecurity system?

Mr. David Masson: I'll let you go first, Professor.

Prof. Andrew Clement: An important point in that, I think, is independent expert review that's independent of the organization and that has the capacity to actually examine what has been proposed and the possible threats and to advise on that. That's the one general thing you can say. Otherwise, you have to get more specific about what kinds of systems you're talking about.

Mr. David Masson: In terms of looking at the future, I've spoken a lot about bad actors using AI, so let's move on. I would be advising the government to really focus big-time on critical national infrastructure attacks, absolutely, and particularly attacks on what are known as OT systems. Most of what we've talked about there was IT systems. I'm talking about OT systems, the things that run the robots in a car factory and that kind of thing. There should be a big major focus on that, absolutely, particularly on those systems inside critical national infrastructure.

Mr. Michel Picard: A very old question that I ask quite often—and I asked the same question in the ethics committee where we talked about something similar—refers to one risk that I will never be able to control, namely the human risk. What do you suggest by way of solutions to reduce or just minimize the risk of human resources? I can't eliminate it.

Prof. Andrew Clement: Well, yes, you can never eliminate risks. You can mitigate and minimize them. For human resources, it's a general precept that when you hire, when you train, when you manage people, they be given respect and be signed-up for the mission of the organization.

It's only through people acting carefully, with attention to the wider picture, that they are going to serve the interests of that organization. It's a basic question about any kind of organization.

Mr. David Masson: Yes, people always say that humans are the weakest link, but sometimes I feel as though that's a derogation of responsibility by larger organizations. They just blame it on the people all the time.

Absolutely, more education and awareness is needed, but also the development of a proper security culture inside organizations, not just the people down below. Everybody must have this kind of security culture and make sure it's delivered in a sincere manner. It's not a case of people barking commands at you, but a genuine prevalence and leadership by people who are trying to promote a security culture.

Mr. Michel Picard: When the Chamber of Commerce commented on small businesses, they said that some of them perceive themselves as too small to be hacked. I think it's a case of their being too small to have a budget to be secure. These are companies that do deal with the Internet, web services and the virtual world.

As an individual, someone who hacks my phone can anticipate whether I'm home or not, because I can control my heating system from my phone. When they see that I am not on the scheduled heating system, it's because I am not there and I keep my temperature low, so my phone is not safe.

Apparently, my fridge is not safe, because it can talk to me. Everything with a chip in it can talk to me, so as a person, the presentation we heard scared the hell out of everyone. Sorry, I almost said it.

Is it too late for me?

● (1750)

The Chair: It probably is. You're past your five minutes.

We're going to have to leave Mr. Picard in a state of anxiety.

We have about five minutes left and a number of questions. Mr. Motz has very generously decided to split his time with me.

When you made your presentation, Mr. Masson, you were very concerned about the data, the network, the transmission staying in Canada. You essentially adopted Professor Clement's recommendation.

The Bankers Association, however, seemed to be a bit more relaxed about it and their argument was, "Well, we still have jurisdiction over the data."

What would your response be to the Bankers Association? It felt perfectly comfortable with the current situation, which may mean that the data goes from Toronto to Chicago to New York, and back to Toronto to be stored, or stays in New York to be stored, or wherever. What would your response be?

Prof. Andrew Clement: I think I heard that exchange at the end of their session. They said they relied on the contractual arrangements with the outsourcing party that they could insist on, and that they would then take full responsibility for making good to individual consumers. I'm not questioning the ability of the banking companies to fulfill that in narrow and specific cases, but if there's a major problem, what are they going to do when their data is outside the country? Are they going to be able to sue the outsourcer? They're going to have to go to another jurisdiction. I don't think contractual arrangements are adequate. As they mentioned or alluded to, these arrangements don't deal with the laws of the country that the data is in. Those laws apply, and any outsourcer is going to have to comply with them, even if it means breaking their contract—or they're going to be in a dilemma there.

I was much less reassured by their confidence that they could just outsource to other countries and rely on the contracts. I think they'd be much better off if they could bring that service within Canadian jurisdiction and Canadian territory. I don't see any major reason why they can't, at least in the long term, hit that goal—have their cake and eat it too, so to speak.

The Chair: The final question has to do with the maps that you very kindly provided to us. They reminded me of a trip I took on a Canadian frigate this summer. We went from Iqaluit down Frobisher Bay and to Greenland. In Greenland we met with the Danish general in charge of NATO and, of course, there was some commentary on Russian intrusions into NATO territories, etc. Apparently the Russians have an immense fascination with scientific investigation of the cables that connect Europe and North America. That seems to speak to your concern, Professor Clement, that one of the ways all of these networks could easily be hacked is by attaching devices in some manner or another to those cables.

You graphically demonstrated the vulnerability of all of our data.

● (1755)

Prof. Andrew Clement: Yes, the cables going across the ocean do present a point of vulnerability for several thousand kilometres. I know that the U.S. has the capability of pulling up those cables and splicing in and intercepting. I wouldn't be surprised if the Russians and the Chinese do as well. One of the ways to get around that is through redundancy: You build over-capacity so that if one link goes down, you have others that are working. That is the case for at least one of the cables that land in Nova Scotia—the Hibernia cable. It's a sort of loop.

I think we need to invest in redundancy to minimize the number of critical points of failure, so that if there is an attack, it is much harder for everything to come down at once, and if one thing comes down, you can reroute around it. Unfortunately, the emphasis and imperative toward efficiency and speed means that very often there's a tendency to put too many eggs in a few baskets. I'd say a general approach to security is through redundancy and duplication—and that needs to be invested in. We need to be aware of that and not discover too late that when one thing goes down, everything goes down.

The Chair: Regrettably, that is going to have to be the end of our discussion with you. It's been absolutely fascinating. We appreciate your contributions to our study and wish both of you well.

With that, we'll adjourn.

**Published under the authority of the Speaker of
the House of Commons**

**Also available on the House of Commons website at the
following address: http://www.ourcommons.ca**

**Publié en conformité de l’autorité
du Président de la Chambre des communes**

**Aussi disponible sur le site Web de la Chambre des communes
à l’adresse suivante : http://www.noscommunes.ca**