HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 155 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, April 3, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, April 3, 2019

● (1610)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I see quorum.

I also see that it's 4:10, and we have a vote at 5:45, I believe, in which case we will likely have to be done by 5:30, or a little bit later than that, but not much later.

We have, from the Privacy Commissioner's office, Mr. Smolynec —

Dr. Gregory Smolynec (Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada): That's correct.

The Chair: —and Ms. Fournier-Dupelle.

I'm going to invite them to make their opening statement. The TD witness who is about to arrive is a little concerned that what TD has to say is a little different from what the Office of the Privacy Commissioner has to say.

I'm going to play it by ear a little bit as to whether we merge the two witnesses, or go back and forth.

With that, we'll ask you to make your opening statement.

[*Translation*]

Dr. Gregory Smolynec: Good afternoon, Mr. Chair and members of the committee.

Thank you for the invitation to speak to you today. I'm grateful for the opportunity given your study touches on issues with which Canadians and the Office of the Privacy Commissioner, or OPC, are seized.

I will reiterate the concerns I voiced when I appeared before the Standing Senate Committee on Banking, Trade and Commerce on its study of open banking: the financial sector must be built upon a foundation that includes respect for privacy and other fundamental rights at its core. Banks and other financial institutions must have robust standards for both cybersecurity and privacy.

It is important to clarify the difference between a privacy breach and a security breach as the two terms are often used interchangeably.

A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information, regardless of the means. A privacy breach is broader and can occur without any compromise of security systems.

And this is the challenge: cybersecurity and privacy have some overlap in that the former can help protect the latter, but in some cases, cybersecurity can create risks for privacy. For example, it is vital to ensure that cybersecurity strategies and activities do not lead to the development of massive surveillance regimes for unlimited and unending monitoring and analysis of the personal information of individuals.

Both the public and private sectors have obligations to report breaches. Under the public sector Privacy Act, that obligation resides in Treasury Board policy, which requires that OPC officials be notified of material privacy breaches. A breach is “material” if it involves sensitive personal information, could reasonably be expected to cause harm or involves a large number of individuals.

On the private sector side, the Personal Information Protection and Electronic Documents Act, or PIPEDA, requires organizations to report breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals. Organizations must notify affected individuals about those breaches and keep records of all breaches.

● (1615)

[*English*]

An example of a high-profile privacy breach is the World Anti-Doping Agency—otherwise known as WADA—case. As a result of a phishing attack in 2016, WADA's database containing extremely sensitive personal information of athletes was compromised by Russian military intelligence operators, who subsequently released some of this data into the public domain, with the threat of releasing more.

ln the OPC's WADA investigation, we concluded that cybersecurity measures should be proportionate both to the sensitivity of the personal information being protected and to the attractiveness of the information to malign actors. This reasoning also applies to cybersecurity in the financial sector. The Supreme Court of Canada has ruled that financial information is indeed sensitive. Other major breaches in recent memory have been those concerning Equifax, Ashley Madison and the Phoenix pay system.

Privacy breach reporting in the private sector has been mandatory since November 1, 2018. Since then, we have seen an approximately fourfold increase in breach reports from the private sector. With six months of private sector data breach reporting under our belt, and considerably more experience on the public sector side of the house, we have made a number of observations. These include that institutions are not always aware of the personal information they hold, where it goes or who has access to it. Oftentimes in the rush to protect against hackers, the internal threat is overlooked, yet privacy breaches involve not only loss of personal information to external forces, but also inappropriate access by internal actors. Mandatory breach reporting requirements can be a tool to enable institutions to confront the adequacy, or lack thereof, of cybersecurity plans and preparations. Furthermore, the OPC uses this information to inform our guidance to organizations.

The challenge for our office and for Canadians is to keep pace with technology. Understanding how personal data will be used, by whom and for what purpose, is equally difficult. While it's the case that privacy policies are seldom read, we may be approaching a time where how data is used is equally ill-understood. The office has done work in the area of examining notions of consent in this space, and has recently launched guidelines for organizations subject to PIPEDA on how best to obtain meaningful consent for the use of personal information.

As others have indicated before this committee, we believe that these issues are best addressed with a collaborative approach. To that end, we work together with other data protection and privacy offices on joint investigations. We participate in Global Privacy Enforcement Network sweeps, and have found that this enables sharing of best practices. The OPC also participates in the cyber security analysts network group, chaired by Public Safety, with the participation of other federal government departments. Our government advisory directorate also provides advice to federal government stakeholders in this area. Other solutions involve education and outreach for companies, particularly small and medium-sized enterprises, which are often hard pressed to ensure their information, including personal information, is adequately safeguarded.

ln conclusion, privacy regulators and advocates have a role to play to ensure that cybersecurity strategies, principles, action plans and implementation activities promote privacy protection both as a guiding principle and an enduring standard. We also need to reform our privacy legislation to make it fit for purpose to ensure that the privacy of Canadians is protected as technologies and economies change, including those in the financial sector.

I welcome your questions.

● (1620)

The Chair: Thank you, Mr. Smolynec.

Just to update colleagues before I ask Mr. de Burgh Graham for his seven minutes of questions, TD does have a concern about sitting at the same table with a regulator. I think we should respect that concern, so I'm therefore going to have to divide the time in half, in which case members are not going to get the same amount of time for questions of the Office of the Privacy Commissioner, which I think is quite regrettable.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Chair, I have a quick question.

I've never seen a precedent where the witnesses asked to be separated that way. We often have contradictory witnesses in same panel. I don't see why this is necessary, given the time we have.

The Chair: It's not so much about having contradictory witnesses, and on that I generally agree with your point, but about having a financial institution with one of its regulators sitting side by each on a panel. That's a concern that's been raised by the financial institution. There is an issue of appearance, if not a reality issue.

That does make it difficult to allocate time for some questions here —

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): When do we have to be done, Mr. Chair?

The Chair: I'm just calculating that. We have to be done by 5:30. That will pretty well be a hard stop, because you have a vote at 5:45. We might press that—

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): The vote is at 6 o'clock. The bell is at 5:30.

The Chair: Well, if colleagues will grant the chair the opportunity to extend the hearings....

An hon. member: [*Inaudible—Editor*]

The Chair: All right. Thanks very much.

Let's start with six-minute rounds, because, regardless, it's going to be cut back—

Mr. Glen Motz: By 4:55 they have to be done and the next group has to be on.

The Chair: Yes, it will somewhere in there.

Mr. Glen Motz: Yes.

The Chair: Let's start with six-minute rounds. Then we'll go to four-minute rounds and see how far we get with that.

Mr. de Burgh Graham.

Mr. David de Burgh Graham: Thank you.

To start, you talked about the number of reported incidents increasing massively. I'm more curious about the unreported incidents. Do we have any way of gauging how many there are? And how can we ensure that unreported incidents cease to happen and they all become reported?

Dr. Gregory Smolynec: Offhand, I do not know of how we can gauge unreported incidents that would be more than big estimates. We have a comparison of what was voluntarily reported before November 1. We now have some indication of what's been reported since November 1.

Have we studied this issue...?

Ms. Leslie Fournier-Dupelle (Strategic Policy and Research Analyst, Office of the Privacy Commissioner of Canada): I think on the public sector side of the house, sometimes what happens is that there are institutions that are holders of personal information and that, according to the sense we have from other reporting, may have under-reported. In that case, we can reach out to them and suggest that perhaps breach training is required. Sometimes the breaches are published in the media as “security incidents”, and they are in fact privacy breaches, or there's a privacy element in there as well. We can reach out to institutions or to companies. So there is some sense, but as to how to measure what we don't know, we don't know yet. Perhaps when we have more reporting, we'll be able to track some trends more carefully.

Mr. David de Burgh Graham: Understood.

In our last meeting, we had an extensive discussion with Mastercard about their systems. One question that Mr. Dubé and I brought up a lot was about the fact that the data is processed in the United States, which from a technological point of view is very logical but from a privacy standpoint raises some obvious concerns, especially with the U.S. PATRIOT Act. I wonder if you have any thoughts or input on how to deal with that aspect and data transiting foreign countries.

Dr. Gregory Smolynec: We're currently taking a serious look at our transborder data flow guidance. We intend in the not-too-distant future to consult widely on this guidance. It's a live issue for our office. We're thinking deeply about it and trying to solicit input from various stakeholders.

Mr. David de Burgh Graham: So we don't have any clear answers at the moment, but there should be some coming.

Dr. Gregory Smolynec: Yes.

Mr. David de Burgh Graham: Whether in this Parliament or the next, when you have answers could you send them to this committee?

Dr. Gregory Smolynec: Of course.

Mr. David de Burgh Graham: I would appreciate that. Thank you.

I have one last question. In the interest of time, I'll then share what time I have left with Mr. Picard.

Is there any privacy without security?

● (1625)

Dr. Gregory Smolynec: My initial response would be, yes, I can imagine circumstances where security concerns are not paramount, let's say, and a person wants to maintain some aspect of their identity or their personal information private. I suppose you could characterize something as a security issue, but it might be more of a privacy incident. Let's say it's an issue of privacy where an individual who might have access to a space legally, one where security clearances aren't a factor, really shouldn't be snooping—in a workplace, in a domestic setting, in a neighbourhood.

Mr. David de Burgh Graham: So not really. There are theoretical edge cases where you have privacy without security for it. At the core, if there's no security to protect privacy, the privacy is more or less meaningless in technology.

Dr. Gregory Smolynec: I wouldn't say so. I think you could have instances where people could be prying into the personal information of others without crossing any kind of physical or other barriers or security impediments, and where it's still a privacy violation that's taking place, but it doesn't necessarily indicate a breach of security.

Mr. David de Burgh Graham: Thank you.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Good afternoon.

Here's a scenario for you.

In the age of cloud computing and platforms such as iCloud, information on Canadians is stored on servers that belong to Canadian companies based abroad or on servers that belong to foreign companies. In either case, the information is on servers outside Canada; it's just the owner that's different.

To what extent can Canada regulate (a) data stored abroad and (b) third parties holding the information when they are not necessarily Canadian? Where does Canada's legislative authority end? What would you recommend on that front?

Dr. Gregory Smolynec: First of all, if the personal information of Canadians is at stake, any foreign company holding the information is subject to Canadian law. Canadian statutes applicable to the private sector stipulate that Canadians must provide express consent before their data can be transferred to a foreign jurisdiction.

Second of all, there are limits. Of course, technological advancements and business models operate on a large scale, so it's complicated, but the laws still apply.

The Chair: Thank you, Mr. Picard.

Mr. Paul-Hus, you may go ahead for six minutes.

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

I missed the last question, so I may ask a similar one.

Foreign companies have a hand in our telecommunications networks and infrastructure. When companies with infrastructure in Canada are controlled by countries whose rules are different from ours, it gives rise to privacy protection concerns. Do you share those concerns?

Dr. Gregory Smolynec: It depends on each case.

Mr. Pierre Paul-Hus: Here's a real-life example. Chinese company Huawei and its 5G infrastructure are top of mind these days and people are concerned. China could decide to deploy its Huawei infrastructure in Canada. Has your office discussed the issue with the government?

Dr. Gregory Smolynec: Yes. Since 5G networks are used to share personal information, privacy protection issues or concerns certainly come into play. That is clear.

It is therefore important to make sure the networks are secure and provide adequate protection against a variety of threats including, of course, known threats. As for other countries' companies, we don't have the authority to conduct that kind of analysis.

● (1630)

Mr. Pierre Paul-Hus: I referred to Chinese company Huawei, but I can put the question in more general terms. Does your mandate to protect the personal information of Canadians include monitoring all the infrastructure in place in Canada?

Dr. Gregory Smolynec: Yes.

Mr. Pierre Paul-Hus: You have a duty to inform the government of various risks, so do you?

Dr. Gregory Smolynec: Yes.

Mr. Pierre Paul-Hus: Very well.

Now I'd like to turn to mobile devices. My iPhone has a facial recognition feature. Apple says my privacy isn't at risk and that the information stays on my phone. I have a hard time believing that. Do you pay attention to issues related to mobile devices such as visual and retinal recognition and the potential transfer of data to companies?

Dr. Gregory Smolynec: Yes, of course.

We perform technical analyses through our technology analysis directorate.

Mr. Pierre Paul-Hus: Can you tell us whether we are protected or at risk?

Dr. Gregory Smolynec: It depends on the specific device.

Mr. Pierre Paul-Hus: I see.

You can't say whether some companies pose a greater risk than others?

Dr. Gregory Smolynec: Right now, I can't, no. Not here.

Mr. Pierre Paul-Hus: Very well.

That is nevertheless the kind of information that is available and in the government's hands.

Dr. Gregory Smolynec: We have limited capacity. We currently have six people working at the technology analysis directorate, so we don't have the resources to examine every device, network and so forth.

Mr. Pierre Paul-Hus: Do you have information indicating that, right now, for instance, the facial data captured by my phone has been transferred to some database? Does that happen, in your view?

Dr. Gregory Smolynec: No, not as far as your personal cell phone goes. Other investigations, however, are concerned with data obtained through visual recognition.

Mr. Pierre Paul-Hus: You're referring to devices located near doors and other systems.

Dr. Gregory Smolynec: Yes.

Mr. Pierre Paul-Hus: I see.

Are Canada's current laws robust enough to deal with organizations or individuals that misuse people's personal information?

Dr. Gregory Smolynec: As Mr. Therrien, the commissioner, has already said, reforms are needed to bring Canada's privacy laws up to date in both the public and private sectors. It's definitely time for reforms.

Mr. Pierre Paul-Hus: You mentioned in your opening statement how quickly technology is changing right now. Do you think our laws and your office are keeping pace with all of that change or are we behind?

Dr. Gregory Smolynec: Legislatively speaking, we are definitely behind. The priority, in our view, is bringing our laws up to date and adopting measures to ensure privacy protection is at the heart of our laws.

Mr. Pierre Paul-Hus: Thank you.

[*English*]

The Chair: You can give your 20 seconds to Mr. Motz in the next round.

Mr. Dubé, please, for six minutes.

[*Translation*]

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

I'd like to thank all the witnesses for being here today.

[*English*]

To our witnesses, with respect, just quickly before I get to my questions, I did have an opportunity to send my colleagues a notice of motion. I understand that I'm not within the 48-hour delay, but I did want to take an opportunity with my time to read the motion and explain in 30 seconds or less its rationale. It reads:

> That, pursuant to Standing Order 108(2), the Committee invite the Minister of Public Safety and Emergency Preparedness to appear, no later than Friday, June 21, 2019, to respond to and take questions on the 2018 Public Report on the Terrorism Threat to Canada tabled in Parliament on Tuesday, December 11, 2018.

Quickly, for the benefit of colleagues, the rationale is that we've heard from communities named in this report that there is a concern about what impact that can have. I think that when we see some of the terrorist activities being committed here and abroad against faith groups and other communities, it's become pretty clear that there needs to be a rethinking of how these groups are identified in these reports and a better understanding of the thought process behind them.

I understand that it's based on information from our national security services, but at the same time, the government is the one responsible for tabling it in the House. We're looking to have a dialogue with the minister on that issue given the concerns that have been raised. Among others, they include the Sikh community. At the appropriate time, I will move the motion forward for debate and, hopefully, for approval.

● (1635)

[*Translation*]

That said, thank you for indulging me. I was just taking advantage of the opportunity.

I have a few questions for you.

We often hear about the Internet of things. You mentioned that, oftentimes, businesses aren't aware of all the data they hold or that, conversely, they are aware but keep it anyway even when the data aren't pertinent.

My question ties in with some of the questions that were asked earlier.

When people download apps on their phone and give their consent, rarely do they realize how much access to the data on their phones they are agreeing to share in exchange for the app. In terms of repercussions, how does that tie in with the issue we are studying? When people use banking applications or fingerprint identification to access their account from their phone, for example, what is the impact of using their phone in that way?

Dr. Gregory Smolynec: You raise a very relevant point. It ties in with public education. Even for people who are familiar with information technology, all sorts of details are not apparent or clear. Our office and the government, as a whole, should conduct public awareness campaigns to educate people about the potential loss of their personal information in different circumstances.

Mr. Matthew Dubé: A public education scenario we often hear about involves government regulatory requirements related to vehicles. For example, if a particular model is under recall because of a safety defect, manufacturers go to great lengths to inform customers, advertising in the media, making phone calls, sending emails and even using snail mail.

Do you think manufacturers should be required to do more to inform customers about cell phone operating system updates? Unless they pay attention to the right websites or subscribe to sites like Gizmodo, customers rarely know the reason for an iOS update on their cell phone, for instance.

Dr. Gregory Smolynec: It has to do with consent. If an individual is abreast of changes, new software, new techniques and such, and a major change is made, the company in question absolutely has to obtain the individual's express consent again. Whenever changes are made to the technology, the company must contact consumers to notify them of the change and its effects.

Mr. Matthew Dubé: Thank you.

I have two more questions for you.

If a data breach occurs or information is disclosed, are the mechanisms in place under the current requirements adequate, for instance, in terms of fines?

My next question follows up on what you said earlier. Should more resources be allocated to the Office of the Privacy Commissioner so that it can keep pace with technological changes? Perhaps that's something we could take into account in our study.

Dr. Gregory Smolynec: Yes, definitely.

The commissioner and the commissioner's office do not have sufficient authority to deal with the challenges emerging as far as business and society in general are concerned. Not only are legislative improvements needed, but also, the commissioner needs to be empowered to impose penalties and fines, for example.

● (1640)

[*English*]

The Chair: Thank you, Mr. Dubé.

Mr. Picard, you have six minutes.

Mr. Michel Picard: I will give my time to Ms. Dabrusin.

The Chair: Ms. Dabrusin, go ahead for six minutes.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you.

My first question is about moneylenders, because we've been talking about financial institutions and banks. I am hoping you can clarify whether there are differences in the rules applying to moneylending institutions. I know, for example, that OSFI covers banks but not moneylending institutions. Are there differences, and does that give you any cause for concern, from a privacy perspective, when we're looking at cybersecurity as an issue?

Dr. Gregory Smolynec: Our office does have a mandate to look at federally regulated institutions like our banks. The office does have an oversight role with respect to banks, as well, and the protection of privacy in banks.

I would add that the banking world is changing. We have the potential for open banking internationally, and coming to Canada, too, which will change business models and the way personal information and data flow among financial institutions. This is also extraordinarily consequential with lots of implications.

The bottom line is that the standards, regulations and laws have to be adapted for this evolution, which is both technological and also in business models. They have to be in place before major changes take place.

Ms. Julie Dabrusin: Fair enough about the open banking, but I'm talking about the places that are on corners. I don't want to give any names specifically, to be picking on any names, but I'm talking about the places used by people who don't really have bank accounts and who are bringing in a cheque and getting their money back at whatever the interest rate is. These are not banks, then, so they fall outside of those regulations. I'm wondering if you have any comment on that with regard to privacy issues.

Dr. Gregory Smolynec: The general context is that these businesses are covered by our private sector law, or provincial laws that are substantially similar. They are subject to the law, but I have nothing to offer to the committee specifically about these particular institutions.

Ms. Julie Dabrusin: They don't fall within your purview. Do you review them, as well?

Dr. Gregory Smolynec: Yes, we do in those instances where the provincial laws are not substantially similar.

Ms. Julie Dabrusin: We talked a little while back with HackerOne, who suggested that maybe we would want to consider legislation that would allow what they termed “white hat hackers”—I wish I could think of a better term for it and say “good person hackers”—who would help to poke at systems and find out where the problems might be.

From a privacy perspective, what would your thoughts be? If we were going to create that kind of legislation, what kind of protections would we need to be thinking about to enable people out there who are not part of, say, the public sector to start hacking into our systems?

Dr. Gregory Smolynec: In part of my statement, I referred to cybersecurity reinforcing privacy and that they could be mutually reinforcing, but you also have occasions where perhaps excessive or inappropriate cybersecurity could have implications for privacy.

How good is the white hat hacker at protecting someone's privacy? They should not have access to some individual's personal information, if they are doing this hacking in the interest of cybersecurity. It would still not be good from a privacy perspective if individuals who are doing something for the benefit of enhancing cybersecurity are violating privacy.

Ms. Julie Dabrusin: I see that. I'm just trying to see what kind of protections we might be able to build in to enable that kind of a system, if we were going to do what had been asked of us by the HackerOne people. I can't remember what they suggested, but money would be offered to white hat hackers if they could find weaknesses in a system, as a way of getting people who are creatively hacking in.

The problem is, I guess, is that once they do that, they do have access to private information, potentially. Is there anything you can think of that we should think about as far as building in protections is concerned?

● (1645)

Dr. Gregory Smolynec: There might be some ways of doing things in an experimental environment that do not put real people's private information at risk. In the military and other organizations, as well as in some cases...in the privacy world too you can war-game cyber operations in a protected space. That might be an area to explore. In the privacy world there's even some war gaming of privacy protection as well.

Ms. Julie Dabrusin: I see that I have half a minute. I'm going to give that....

The Chair: You're going to give it to Mr. Motz. Mr. Motz loves this.

Ms. Julie Dabrusin: I was giving it to the collective pool of extra time. I could just talk it out for the next 20 seconds.

The Chair: There's a plus and a minus here, Mr. Motz.

You have four minutes, please.

Mr. Glen Motz: Thank you, Mr. Chair.

Thank you, witnesses.

I just want to continue the line of questioning by Ms. Dabrusin.

Would Canada be better off having a vulnerability disclosure agreement with what I'll call “ethical actors”, so they are protected when they find faults in a company's system, so that it can be fixed before it is exploited. I think what you're trying to get at is that it would be beneficial to all Canadians.

Dr. Gregory Smolynec: I haven't considered, nor has our office considered, the implications of ethical or white hat hacking for us to be able to give a detailed response. We could undertake to consider this space and come back to the committee with a more considered answer.

Mr. Glen Motz: At my age, I know that sometimes I forget some of the witnesses' testimony, but we did have specific individuals here —and HackerOne was one of them—who do great work ethically to protect the consumer.

If this or the next government is looking at protecting against an adverse economic impact on Canadians by improving our cybersecurity, I would think we should have some understanding around some protections for those individuals. What are your thoughts on that?

Dr. Gregory Smolynec: Our interest would be ensuring that people's privacy is protected, regardless of what the.... There may be a balance of interests here to consider, but in this context, I would say that citizens' privacy needs to be protected in their own right.

Mr. Glen Motz: Yes, I agree with that. I suppose it's like national security to some degree. There's a balance between privacy and the need to protect national security. I think in the same way, if we have an ethical hacker who is able to protect the.... If there's some structure around how they operate, some protections for them as well as protecting the data of consumers, it's something that I would think that we should maybe consider pursuing.

I'll move on to a different line of questions.

You made a number of recommendations when you were at the Senate banking committee. One of them was that your office be granted enforcement authorities, including the right to independently verify compliance without grounds to ensure that an organization is in fact accountable for protecting personal information. Have you had any push-back from the private sector since you made that recommendation at the Senate?

Dr. Gregory Smolynec: No, nothing.

Mr. Glen Motz: How do you envision those enforcement authorities working for the Privacy Commissioner's office?

Dr. Gregory Smolynec: Pardon me?

Mr. Glen Motz: How would you see those authorities working for the Privacy Commissioner's office?

Dr. Gregory Smolynec: This is something that exists in the United Kingdom, and we're actively looking at the United Kingdom in this particular area of enforcement activity to understand what the British experience has been on inspection without grounds.

Mr. Glen Motz: I have one last question.

We had a witness, I believe it was on Monday, who called Canadians innocent when it comes to our own cybersecurity. What needs to change in Canada, from your perspective, sir, so that citizens are more vigilant about cybersecurity, and thus, their own privacy? You mentioned something to Mr. Dubé about that, but is there something more specific from your side that we can do from a legislative perspective or whatever?

● (1650)

Dr. Gregory Smolynec: I'd say the number one objective, the number one priority, would be privacy law reform, rights-based privacy law reform.

The Chair: Explain that very briefly.

Dr. Gregory Smolynec: Currently, I would say that our private sector law is principles based and, in a sense, very broad. In passing, it refers to the privacy rights of Canadians, but a rights basis would recognize, as Canada does, that privacy is an internationally recognized human right and, in the context of a human right, that there are also procedural rights associated with it. It would also recognize that this would be applied broadly across both public and private sectors. Canadians should be informed of their rights and how to exercise those rights. It's both a legislative challenge and an associated public education challenge.

Mr. Glen Motz: With rights and responsibility?

The Chair: Thank you, Mr. Motz.

I think you've used up Mr. Paul-Hus' extra time and Ms. Dabrusin's extra time.

Mr. Glen Motz: Thank you, I appreciate your indulgence.

The Chair: Mr. Graham, you have the final four minutes, please.

Mr. David de Burgh Graham: Thank you.

It's not directly related to you, but I want to use this opportunity to clear up some questions that keep coming up.

Black hat hackers and white hat hackers are long-held terms in the technology community. I just want to put that out there since there's confusion about it. There are also grey hats, and we can get into a whole discussion about that.

Another point I want to make sure everyone is aware of is cracking versus hacking. If you put duct tape on a bottle of WD-40 to make it go to space, that's a hack. If you use that to break into a bank, that's a crack. I want to make sure we have that distinction very clear out there.

The Chair: I'm going to buy a can of WD-40 much differently from now on.

Mr. David de Burgh Graham: Yes, I hope you do.

I want to come back to you for a second. You said you had a technical research division of six people. What kind of expertise do they have? Are they looking at servers, networks and routers and taking phones apart? What kind of people are they and what kind of things are they doing?

Dr. Gregory Smolynec: We have a small group of technologists, scientists and engineers. They look at things, from particular devices to larger systems such as the Internet of things. They participate in the development of guidance, for instance, on biometrics, on de-identification, on the Internet of things itself and on the risks and vulnerabilities to privacy associated with new technologies. They support our investigations with forensic analysis, and we're developing a capability for the custodianship of evidence, etc. It's part of our investigative program.

It's a wide range of activities and tasks that absolutely exceed the capacity of the small team, which is very capable in its own right, but there are only six people with a small lab.

Mr. David de Burgh Graham: Okay. It's a full lab, but just not a very big one.

Dr. Gregory Smolynec: We have a small lab to conduct experiments offline to protect our networks and government networks.

Mr. David de Burgh Graham: If these experts take apart a phone, for example, and find a significant privacy vulnerability in it, what would be the course of action?

Dr. Gregory Smolynec: It depends on the context in which it is happening. If it's in the context of an investigation, which is often the case, as we do a lot of support for investigations, that information—evidence, so to speak—would become part of the report of findings of our investigation.

Mr. David de Burgh Graham: You work with outside organizations such as the Electronic Frontier Foundation, which is one of my favourite examples. They are constantly doing this type of work, putting that work out there, validating it and vice-versa.

Dr. Gregory Smolynec: Yes, we have networks of external partners, not the least of which are our international data protection authority partners, our provincial data protection authority partners, as well as privacy commissioners across Canada and around the world.

Mr. David de Burgh Graham: We've heard a lot in the past in this committee and other committees about anonymization of data. At the industry committee, there was a very brief discussion of a StatsCan study on banking data, for example. It's very possible to anonymize this type of data. Is it possible to “de-anonymize” this type of data?

Dr. Gregory Smolynec: Yes. One of the things we're looking at is standards. In fact, as we speak, the acting director of our technology analysis directorate is in Israel for a meeting of the International Standards Organization on de-identification. The problem, however, is that data sets can be combined to reidentify individuals. So it's a very complex area.

● (1655)

Mr. David de Burgh Graham: Thank you.

The Chair: With that, we'll have to close this session. I want to thank both of you on behalf of the committee for your testimony. We are now suspended.

● (1655)

(Pause)

● (1655)

The Chair: Colleagues, we're back on. Mr. Foster has been very generous and waited patiently for us. Can I get some guidance from you as to how much time we can have with this panel? If we end at 5:30, that will be 35 minutes.

Mr. David de Burgh Graham: A reduced quorum...?

The Chair: Is the vote at 5:45 or is it six o'clock?

Mr. Matthew Dubé: It's at six o'clock. They are half-hour bells—

The Chair: Half-hour bells, so the bells are going to start ringing at 5:30. Do I have a general consensus that we push it past 5:30 . for at least 10 minutes?

Mr. Pierre Paul-Hus: So that's 5:40.

The Chair: Is that good? Is everybody fine with 5:40?

Some hon. members: Agreed.

The Chair: I'm assuming that you can stay past 5:30.

Mr. Glenn Foster (Chief Information Security Officer, Toronto Dominion Bank): I can stay. No problem.

The Chair: Thanks, Mr. Foster.

As you know, you generally have a 10-minute opening statement. The committee would not be upset if that were less than 10 minutes. So with that—

Mr. Glenn Foster: I'll do my best.

The Chair: It's an opportunity. Please, go ahead.

Mr. Glenn Foster: Thank you.

My name is Glenn Foster. I'm the senior vice-president and chief information security officer of TD Bank Group. I'm responsible for TD's cybersecurity program across all of TD's activities globally.

TD is the sixth-largest bank in North America by branches and serves more than 25 million customers. We rank among the world's leading online financial services firms.

I'm here to talk to you about cybersecurity and its impact on financial services, Canadian consumers and national security. Traditional banking services have continued to become more digital. A recent CBA poll found that 76% of Canadians are using digital channels, both online and mobile, to conduct most of their banking transactions.

More than half of those polled say this is their most common banking method. This is true for TD customers as well. We have more than 12.5 million active digital customers and 7.5 million total active mobile customers. We complete 1.1 billion digital transactions per year in North America, and we have the highest digital penetration of any bank in Canada, the U.S., the U.K., and other parts of Europe.

Meanwhile, cyber-threats continue to become more sophisticated, driven by the commoditization of crime in the underground economy; the loss of top secret nation state intelligence technologies, when made available to bad actors; innovative technologies that spur advances in automation; geopolitical tensions and increased activity against global financial service participants and payment systems.

Recent economic sanctions have further increased tensions and have motivated retaliatory actions, cyberespionage campaigns, and attacks on financial services and critical infrastructure globally by nation state actors.

The proliferation of data breaches has significantly exposed consumer data and places pressure on banks' ability to authenticate customers.

This exposure of consumer data has also led to new automated attacks in which criminals leverage stolen account credentials and test them against online banking sites at a significant rate, an attack that's known as credential stuffing.

At TD, we have invested heavily in cybersecurity as one of our top priorities to ensure that we can protect our customers and live up to the high expectations of trust they place in us. We have a strong history of information sharing and collaboration with other Canadian banks through the Canadian Bankers Association, and across sectors of the Canadian economy through the newly formed Canadian Cyber Threat Exchange. We understand how critical it is to share intelligence on threat actors, and we consider it a best practice to combine our defences, as our ability to prevent, detect and contain cyber-attacks increases significantly when we work together as opposed to individually.

The effectiveness of our information sharing is limited based on current privacy laws and legal barriers. Legislative reforms allowing for safe harbour provisions for proactive protection could benefit our efforts. We support the government's creation of the Canadian Centre for Cyber Security under the Communications Security Establishment. We've been a long-time proponent of centralized authority for collaboration with the private sector.

Working with the Canadian Cyber Threat Exchange, we have established a solid structure for public-private partnerships and sharing. The critical part of the centre's mission should be not only information sharing and intelligence but also developing and implementing national strategies for cyber resiliency, preparedness and response.

The centre should be effectively resourced to engage with the private sector in establishing and measuring minimum security baselines for critical infrastructure sectors. The public and private sector would also benefit from coordinated resiliency tests and response capabilities verus systemic cyber events for critical infrastructure, which will prepare the centre to be the central point of coordination with the private sector in response to a national security threat.

It is important to note that cyber protection and safety are the responsibilities of not only financial institutions and government but also Canadian consumers.

Security practices fail when individuals do not understand their personal accountabilities and do not practise due care in their digital lives. Therefore the new national strategy is focused on educating Canadian citizens on cyber safe practices, which is vitally important to increasing their literacy with regard to risks and expectations.

The ever-increasing cybersecurity demands require a robust and highly skilled workforce. Various external benchmarks suggest an unmet demand of over one million open positions for cyber talent in North America alone.

At TD, a premier employer in Canada, our focus on talent is a top strategic pillar of our cyber program. We face increasing competition for cyber talent in Canada, and we are collaborating with academic institutions to create strategic partnerships such as the one mentioned in our announcement last year of our partnership with the cybersecurity institute of the University of New Brunswick.

We have also expanded our geographic footprint to the United States and Israel to meet talent demands. We are committed to growing the next generation of cyber talent here in Canada and encourage the federal government to accelerate the development of robust educational programs at Canadian universities to provide for the cyber workforce of tomorrow.

● (1700)

I am pleased to be here to discuss Canada's approach to cybersecurity, and I look forward to our discussion.

The Chair: Thank you, Mr. Foster.

Mr. Picard, we will go with the six-minute rounds again.

Mr. Michel Picard: Welcome, Mr. Foster.

In how many countries can we find TD bank offices or branches?

Mr. Glenn Foster: I don't know the exact number. I would have to get back to the clerk.

We're primarily a North American bank with other securities investments firms overseas.

Mr. Michel Picard: Is the network that you use for your transactions in Canada a private network, or is it the Internet—the web in general? How is the security managed when you have access to your bank from outside Canada through your branches or offices?

Mr. Glenn Foster: We have various connection methods based on the products or the stores or branches themselves, but the majority of our transactional traffic is through our online and our mobile applications, which will be coming in over the Internet.

Those connections are based on both browsers and our proprietary mobile applications that customers very commonly put on their smart phones, and they use standard PKI-based encryption to protect those transmissions from end point to end point.

Mr. Michel Picard: Is the information related to Canadians only for personal identification or information all in your server in Canada, or can some of that information be found or copied elsewhere in your branches in foreign countries?

● (1705)

Mr. Glenn Foster: All of TD's data centres reside within Canada.

Mr. Michel Picard: So outsiders, i.e., TD bank outside of Canada, or any other third party talking to your server, then enters into your server in Canada in order to have access, if possible, to the information that you have.

Mr. Glenn Foster: Yes.

For our core banking systems, there would be direct connectivity to us within our data centres in Canada. Now, TD does have external third party service providers for various banking services and customer services. Those services may reside within other countries, such as the United States.

Mr. Michel Picard: We cannot compare your system with other companies', of course, because it's private, but we are talking more and more about open banking. What is your take on that?

Mr. Glenn Foster: As a security professional for a number of years, my opinion is that the integrity of any security scheme is reliant on a closed loop between the consumer of services and the service provider of the banking services. Any intermediary that's in between inherently weakens the security scheme.

Mr. Michel Picard: With the concept of open banking, do I understand it correctly when you say that if there will be a third party, that's a vulnerability to the system?

Mr. Glenn Foster: Yes.

Mr. Michel Picard: Do you need a unique system then?

Mr. Glenn Foster: When it comes to authentication of credentials, a third party would inherently have to have access to those credentials for online banking. Of course, there are various models. There's the U.S. model, which is very much market driven, which allows us, as banks, to contract with these third parties and provide certain assurances over their security. The U.K. model is very much open; therefore, anyone could consume those services.

Mr. Michel Picard: If or when you are a victim of a hacking or an attack, do you declare this to an authority, and how long do you do it after the fact?

Mr. Glenn Foster: I'm sorry. Could you repeat the question?

Mr. Michel Picard: When you are a victim of a hacking aggression, do you declare that to an authority somewhere—to the government—and how long after the fact do you declare that?

Mr. Glenn Foster: Our primary regulator, which is OSFI, provides very prescriptive guidance on reporting requirements. The requirement is 72 hours, based on a described severity scale.

Mr. Michel Picard: Thank you.

I had six minutes.

The Chair: You have a couple of minutes left.

Mr. Michel Picard: I have plenty of time. Do you want a coffee or something?

Some hon. members: Oh, oh!

Mr. Michael Picard: Should we regulate the announcing of an attack not only in terms of time, to make it as fast as possible, but also use this information and spread it all over the market to inform everyone, protecting the information of the person or the company, but doing it in a way where this information may be helpful somehow?

Mr. Glenn Foster: As for privacy information and the protection of the consumer PII, I believe the privacy laws and reporting time frames are adequate. As a bank or large institution, we go through various security scans, looking for malicious activity on a daily basis. The question really comes down to finding the threshold of abusive activity, whether some activity is actually a problem. My view would be that the reporting we do at our primary regulator is adequate.

The typical things we see at TD Bank relate to attempts at customer-based criminal activities against our online banking systems. One of the things I mentioned in my opening remarks was credential stuffing. If you look at all of the data breaches that exist now from Marriott, Yahoo, etc., we have millions, in some cases billions, of credentials. Yahoo reported 3.5 billion sets of credentials. Criminals are scripting attacks against various banks, looking for consumers who reuse their user names and passwords throughout the institution. The volume of that traffic is significant, and it forces banks and corporate defenders to invest in leading technologies to remediate that traffic. That becomes business as usual for us, no different from fraud losses within a period of time.

The Chair: Thank you, Mr. Picard.

[*Translation*]

Mr. Paul-Hus, you may go ahead for six minutes.

Mr. Pierre Paul-Hus: My colleague asked you a question about data storage. As you pointed out, TD Bank generally stores its data in Canada but may also store some data in the U.S.

On Monday, we heard from Mr. Green, the head of cybersecurity at MasterCard, and he told us that banks were the ones keeping the data on file.

You work with Visa. Do you store the data related to TD Visa cards here, in Canada, or in the U.S.?

● (1710)

[*English*]

Mr. Glenn Foster: The core processing is outsourced and that data actually resides in the United States.

[*Translation*]

Mr. Pierre Paul-Hus: I see.

I'd like to come back to the oft-mentioned ethical hackers.

What you do call them again?

Mr. David de Burgh Graham: The term is white hat hackers.

Mr. Pierre Paul-Hus: Very good.

In 2017, TD created the red team, a group of ethical or white hat hackers that work for the bank and spend 24 hours a day looking for holes in the system.

What kind of service contract do you have with those individuals?

[*English*]

Mr. Glenn Foster: Good question. Even prior to the development of the red team, we had our own internal ethical hacking team as well. The purpose of that team was to support our system development activities and make sure a credit system was secure before we placed our trusted data in it, or exposed it to customers. The red team, specifically to your point, is made up of ethical hackers who test our production systems on a daily basis. Those are internal employees. We augment those resources with experts in the field. We do that not just for capacity, but also for shared expertise, because the way to strengthen this industry is by constantly bringing in new skills, new talents, and continuously testing our systems.

[*Translation*]

Mr. Pierre Paul-Hus: I'd like to talk about the trust relationship between the bank and the group. At their core, they are people who enjoy hacking. What they do is slightly criminal, but you hire them to work as the good guys, if you will, helping the bank and supporting its system.

How do you make sure you can always trust them?

[*English*]

Mr. Glenn Foster: Obviously, these employees go through our pre-employment screening. We do background checks, etc. They are part of our insider risk program, and they're aware that because of the sensitive position they hold in are testing production systems where customer data may reside, they will be continually monitored beyond the level that average employees are subject to. They will go through a periodic screening on an ongoing basis.

[*Translation*]

Mr. Pierre Paul-Hus: You said that TD had a cybersecurity office in Israel. We heard from two witnesses who cited Israel as their preferred location.

Why is Israel so important from a cybersecurity standpoint?

[*English*]

Mr. Glenn Foster: Israel has a unique ecosystem in regard to their mandatory military service. They were very early adopters and had early recognition of the importance of cybersecurity. The availability of talent and high skills in that location are very desirable. That said, we are very selective about the positions we place over there. We look at security innovations, security intelligence, and monitoring for potential risks to TD Bank or our customers. In some cases, we run proofs of concept for rapid development of cyber-tools and products.

[*Translation*]

Mr. Pierre Paul-Hus: You mentioned Israel's ecosystem with respect to military service. Ultimately, Israeli culture offers a certain way of looking at the world. Security is a huge issue for them. We've heard a lot about Israel. How can Canada follow in Israel's footsteps to make sure young Canadians are better equipped for the challenges or take an interest in the issue?

You brought up the military. I served in the armed forces. It may be beneficial to look to Canada's military as well. Cybersecurity plays a big role in military operations, but it's done in a bubble. Is there a way to work with the military in that regard?

[*English*]

Mr. Glenn Foster: Their mandatory military service gives them an advantage, not just from the mindset they have but the networks they create. What's unique of their small ecosystem is that they leverage those military networks throughout their careers. Somebody could be working for Intel or somebody could be working for IBM, and they're working on a unique problem. It spurs very interesting collaborations. In some cases, it spurs a lot of the start-up nation mentality that you hear.

● (1715)

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

[*English*]

The Chair: Mr. Dubé, you have six minutes, please.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

[*English*]

Mr. Foster, thank you for being here.

I want to talk about artificial intelligence. It has been raised a few times. In particular, it's being used by bad actors to learn how to attack weaknesses in systems. My understanding is that more and more we're seeing it being used also as a protective measure, learning how to protect.

I think TD acquired an AI start-up last year. I'll start with the security perspective and I'll get to other aspects of it.

From a security perspective, for both defending and your perception of those who are attacking, what's your sense of the current state of affairs?

Mr. Glenn Foster: I'll start with the attackers.

Although we're highly concerned about adversaries leveraging artificial intelligence to attack us, we haven't seen many examples of that in practice. Given that it's an evolving space, it's one that our threat intelligence team monitors very closely.

On the defence side, it's a significant asset and tool for us. Traditional security products were very good at a period of time where attacks were very repeatable. You could define signatures; you could block them.

Current attacks are very sophisticated. They're evolving on an almost daily basis. From the time of zero day out in the public to the time the commercial vendor can patch, to the time that large institutions can patch those vulnerabilities, the window, although getting so much shorter, is still significantly greater than the speed at which adversaries can develop scripting and start scanning everyone on the Internet. Part of that automation, in some cases using AI to be more rapid in how it identifies these vulnerabilities, is becoming a much more significant problem for us.

How we detect the more sophisticated actors in some of those regards, where they know how to get around our traditional security equipment, is through AI and machine learning and big data.

Mr. Matthew Dubé: Thank you for that. That's the security side.

From a business or marketing side, AI can also be used to advance the needs of a business, to identify customer needs, and so forth. Layer 6, which you acquired, actually even says in their mission statement that they use machine learning technologies to help businesses better anticipate their customers' needs, which is a laudable goal. Those of us who use banking apps see these things being incorporated, where they're trying to predict spending trends or things such as that.

How does that get used? I know it's a broad question, but I want to understand. If data is being collected inevitably, how does your organization, your business or your bank, go about culling that information and making sure you're not gleaning things that maybe shouldn't be gleaned or that haven't been consented to, at least not explicitly?

Mr. Glenn Foster: In regard to data protection, not just for Layer 6 but for any technology system within TD Bank, we go through a very robust accreditation process that we call our "secure SDLC" program. That really starts in understanding basic requirements, risk assessments and privacy impact assessments, and then providing prescriptive measures on how that data is supposed to be protected. We have a very robust data classification standard. Then we leverage various schemes to protect that data.

The first strategy, of course, is if you don't actually have an explicit need, you don't get the data. Then there are various techniques, from tokenization obfuscation to encryption, to protect that data.

Mr. Matthew Dubé: I appreciate that.

The other aspect I wanted to go to is with regard to apps. Earlier, I was asking the Office of the Privacy Commissioner about this notion that when you install an app on your phone you're sort of giving broad permission. Some of the time it's explicit and other times it's less so in terms of such-and-such app wanting to access your microphone, your camera, and this, that and the other thing.

When your organization is developing the app, I'm wondering how you reconcile what's going on within the application for the banking activity of the client and the fact that there might be a variety of flaws that exist within, whether it's the firmware or other flaws that are being exploited within the mobile device itself. How does that work? What do you see as recommendations going forward?

● (1720)

Mr. Glenn Foster: All I can tell you is how we approach the security with the TD Bank for our applications.

You're right. Our application has to live in an ecosystem. No different from your computer, it's dependent upon the underlying operating system and the firmware. We build those applications with a couple of principles in mind. One is least privilege. Of the data that's in there, we try not to persist any data on the device itself. That way, if there are any inherent weaknesses, there's no data there for it to actually access.

We make sure the application is hardened. I mentioned the ethical hacking team that we have, in addition to the red team. Their role within the bank is that prior to the launch of any of these products, they perform very robust security testing, to make sure the application adequately insulates the application from the other things that are going on within the device itself.

Mr. Matthew Dubé: Thank you.

The Chair: Mr. Graham, please, for six minutes.

Mr. David de Burgh Graham: Thank you. I'm going to follow up a bit on Mr. Dubé.

How secure is an app on a jailbroken phone?

Mr. Glenn Foster: How secure is an application on a jailbroken phone?

Mr. David de Burgh Graham: Yes.

Mr. Glenn Foster: It's not very secure at all, which is why we have jailbreak detection in our applications. We will actually suspend services for that application if it is jailbroken.

The issue, obviously, is that malicious code could end up very easily on that phone. Also, we've talked about encryption from point to point. Data could potentially be exfiltrated as a result of malicious code running on the device.

Mr. David de Burgh Graham: Right, because you said before—

The Chair: Mr. Graham, I'm sure there is somebody else on this committee who doesn't know what "jailbreak" means. Could you explain that?

Mr. David de Burgh Graham: I can explain it to you if you don't count it against my time.

The Chair: I'm not counting your time. I'm sure this is all for greater edification.

Voices: Oh, oh!

Mr. David de Burgh Graham: How do I explain this in 10 seconds?

Do you want to explain what a change of jail is and what a jailbreak is?

Mr. Glenn Foster: The simplest way to explain jailbreaking is that when you get your phone from your provider, you can only load applications through their approved app store. Jailbreaking is essentially a hack that you can find on the Internet to allow you to sideload applications around what was already approved by your service provider.

Mr. David de Burgh Graham: It allows you to use your phone as a computer. It's much more usable, but much less secure, so it's a trade-off.

The Chair: Okay. I see. Thank you for that.

Mr. David de Burgh Graham: The reason I wanted to get to jailbreaking a little is that you talked earlier about PKI: public encryption, public key systems. If you have a jailbroken phone, your private key can be compromised, and therefore everything you are doing is very easily compromised. Is that a fair assessment?

Mr. Glenn Foster: It's not quite as easy as that. There is a risk there. The risk to that device actually increases, and then obviously we want to know if that phone is jailbroken so we can make risk-based decisions on that user or any transactions they're trying to perform.

Mr. David de Burgh Graham: Okay.

I have a financial institution-specific question, fortunately, for you. Last fall, my wife lost her credit card, and of course it got used quite a bit. There was nothing we could do about it because they used the tap function, and there's absolutely—

Mr. Jim Eglinski (Yellowhead, CPC): I'm older—

Voices: Oh, oh!

Mr. David de Burgh Graham: It took her two days to notice that she'd lost it, but anyhow.... We don't have to put that in our Hansard.

The point is that there is no security on these tap cards that I can see. What is the method to secure PayPass and payWave, the RFID technology that we're using now? Is there anything we can do to actually make it secure?

Mr. Glenn Foster: EMV payments are using fairly advanced cryptography. I wouldn't say they're insecure.

Mr. David de Burgh Graham: They're secure so long as you have them, but if you lose them, there's nothing to authenticate that the person using it is the person who's supposed to be using it, which there is with PINs and, to a certain extent, with the numbers on the back of card. There's none whatsoever for tap.

Mr. Glenn Foster: All I can say is that within the banks we have various fraud strategies and limits on EMV payments as a result of that. I'm sorry to hear about your wife's experience.

Mr. David de Burgh Graham: They didn't refund it because we hadn't reported it missing. We didn't know it was gone until we got about $200 in charges in that time. My point is only that this can happen and there's no practical system to stop it.

It depends on your goodwill as a bank to refund it, but it isn't ultimately your fault. I'm wondering if there's any way around that, but there doesn't seem to be.

Mr. Glenn Foster: Again, I'm the technical security person for data and systems. I'd have to follow up with our product folks and product people.

Mr. David de Burgh Graham: Fair enough.

When I travel around the world, for example, and I use my credit card or my debit card in different places, does TD track where and what I'm doing with it for any purpose other than [*Inaudible-Editor*] the transaction?

Mr. Glenn Foster: No, only for fraud purposes.

Mr. David de Burgh Graham: Fraud purposes. There are no marketing purposes whatsoever at any stage of that?

● (1725)

Mr. Glenn Foster: Your transaction data and the point of sale transaction is what ends up within the systems within TD. Is that your question?

Mr. David de Burgh Graham: Let's say I go to the bank across the street here, and then I go to Saskatoon and then I go to Taipei. You now know that I'm travelling and you know roughly what I'm buying. Is that data used for anything other than security tracking?

Mr. Glenn Foster: Again, I'd have to defer to the product folks who do that type of target marketing.

Mr. David de Burgh Graham: Are passwords obsolete?

Mr. Glenn Foster: In my professional opinion they still have some value—that's "something you know"—but the value of that credential is dramatically decreasing year over year.

Mr. David de Burgh Graham: What is the alternative?

Mr. Glenn Foster: The alternative is various forms of biometrics. You still want some form of something you know, or something you have, along with the biometrics themselves. That's really the "something you are" in the scheme they refer to as "multifactor authentication".

I think if you look at the thumbprint readers today and at some of the facial recognition technologies in the marketplace, they're becoming far more robust. In most cases they're a more powerful authenticator than a customer's username and password.

Mr. David de Burgh Graham: That's fair. If your biometrics are compromised, is there anything you can do?

Mr. Glenn Foster: We bind a biometric to a user, so we can then suspend that and re-enrol the user. We don't retain your entire.... With a thumbprint, for example, none of these devices actually retain your entire thumbprint. They all have their own proprietary algorithm of points that they take, and they actually retain that data only. Schemes vary from device to device.

Mr. David de Burgh Graham: I have a....

Mr. Glenn Foster: Your thumb is safe.

Mr. David de Burgh Graham: The thumb has to have temperature to it, too. It has to have blood flowing, so that's another whole issue.

Mr. Jim Eglinski: You just hold it in your hand for a while.

Mr. Matthew Dubé: You've thought about this.

Mr. Jim Eglinski: Put it in the microwave.

Some hon. members: Oh, oh!

Mr. David de Burgh Graham: On a slightly lighter note, in Monday's meeting the topic of Y2K came up briefly—I don't remember why—and I didn't have a chance to come back to it. Is TD Y2K38-ready?

Mr. Glenn Foster: Is TD Y2K38-ready?

Mr. David de Burgh Graham: If we have the Y2K38 bug.

Mr. Glenn Foster: We haven't performed a robust assessment on that yet.

Mr. David de Burgh Graham: Do you have anything left with 32-bit?

Mr. Glenn Foster: No.

Mr. David de Burgh Graham: Okay, then you're fine.

Thanks.

The Chair: Mr. Motz, did you know, as an ex-police officer, that there was something else to jailbreaks than what you thought?

Mr. Glen Motz: Yes, as a matter of fact, I was aware of that particular—

The Chair: You were aware? I'm very impressed.

Mr. Glen Motz: We used to hack into phones all the time.

The Chair: I see.

Mr. Glen Motz: Anyway....

The Chair: Four minutes, Mr. Motz.

Mr. Glen Motz: Legally.

Mr. Michel Picard: Of course.

Mr. Glen Motz: Under judicial authorization, Mr. Chair.

I want to get back to a conversation we started on Monday with some of the other groups that were here. We heard there are some longstanding issues around legacy systems, specifically in the banking industry, for example software that's no longer supported. I'm led to believe that some of our ATMs still use and operate under the Windows XP platform, which is no longer supported.

As a financial institution, are you facing these challenges right now? What are you doing to ensure that your systems are secure and that old data is being transferred or made more secure?

Mr. Glenn Foster: Like all large enterprises, we have currency issues. We spend a significant amount of our budget on upgrading those systems, including the ATM fleet. Likewise, we operate within a system of layered controls to make sure those networks are a closed loop, that we have adequate encryption from a device back to our systems themselves, and then we have layers of detection to identify any potential misuse to maintain that we're balancing risk along the way.

Mr. Glen Motz: Okay.

We've been talking at this committee and in the House—and nationally, really—about whether or not to accept Huawei, for example, into our critical infrastructure moving forward. With 5G now on the horizon, is your bank prepared to use servers that are built in whole or in part by foreign entities that are controlled sometimes by foreign governments? How are you navigating that process?

● (1730)

Mr. Glenn Foster: We're currently undergoing an assessment on that, so we haven't arrived at a conclusion, nor have we published a policy on it.

Mr. Glen Motz: How do you vet your software and hardware now, then?

Mr. Glenn Foster: On the hardware side, we have an acquisition process that is likewise a security accreditation process, prescribed for any internally built or deployed software. On software acquisition, where you commonly reproduce commercial off-the-shelf software, we also go through an evaluation prior to its acceptable use.

Mr. Glen Motz: You make sure that it doesn't have any backdoor bugs in it.

Mr. Glenn Foster: That is correct.

Mr. Glen Motz: All institutions are subject to cyber-attacks. The banking industry certainly isn't immune. In your experience with TD, where do most of your attacks originate and what kind of information is being targeted?

Mr. Glenn Foster: The majority of the attacks we see are commonly disguised to look like they're coming from within Canada or within North America more broadly. Where we can trace the original traffic, they're mostly coming from Eastern Europe, Russia or, in some cases, China or North Korea.

Mr. Glen Motz: What are they targeting, and are you guys using any proactive measures to protect your own infrastructure?

Mr. Glenn Foster: Yes, we have a dedicated threat intelligence team that monitors the dark web. We collect threat intelligence and indicators of compromise from multiple source providers. We have a very robust sharing capability through the CBA, and more globally with the FS-ISAC and the U.S., where we get significant intelligence on what the community is seeing. We then use that data to look at actual traffic that is coming in and out of our network.

We proactively block known malicious destinations, so that if anything were to get into our enterprise, it would essentially be quarantined right away. We have layers of control and detections throughout our network and our infrastructure, where we can both identify potential bad-actor activity and quarantine devices in real time.

The Chair: Thank you, Mr. Motz.

Ms. Dabrusin.

Ms. Julie Dabrusin: When you made your initial presentation, you talked about personal accountability being an issue. Our systems were described earlier as being like armoured cars going between two cardboard boxes. That really stands out as an issue.

To what extent does the bank, for example, create pop-ups when people are putting in their passwords or logging in to advise them, "Hey, if you've used this password somewhere else, you've compromised your security?" Do you have anything where you're informing people about the need to come up with new passwords?

Mr. Glenn Foster: As an industry, we don't present pop-ups within the log-in transaction. We all provide guidance on our online banking websites about what strong passwords are. We do proactively disable accounts if we suspect there's nefarious activity, or we've identified these credentials on the dark web or what have you. That would force a customer to go through their password reset flow and reauthenticate themselves through other means that they are legitimately who they say they are. Then we reinstate their accounts.

Ms. Julie Dabrusin: I'm just trying to think about my sense, and what other people have said, and it doesn't strike me as being untrue that people might use a certain number of go-to passwords. That is one of the biggest compromises of their personal cybersecurity.

Mr. Glenn Foster: [*Inaudible—Editor*] usually gets passwords or password reuse. It's commonly obtained through various breaches at less sophisticated companies.

Ms. Julie Dabrusin: I know that when you sign on to different sites, they all say, "You need stronger passwords." You've used a capital letter and thrown in some type of symbol, a number sign or something, and a certain number of characters, but there's nothing I can picture that says, "Hey, have you used this password before?" Is that not a simple way to at least jog people's memory? Sure, you're doing this because it's convenient, but you're reducing your security. Is there not something you could put in there, as part of those eight symbols or letters, or whatever thing you prompt people on?

Mr. Glenn Foster: We obviously can look at additional ways to educate customers and consumers along the way.

Ms. Julie Dabrusin: Thank you.

You talked about the need to have more programs to train people. What hasn't been clear for me is what training is required. It seems there are different types of standards and that some places might hire without a person's having a specific cybersecurity degree, and some places might not. What do you need as training for your workforce? What are you looking for, as training?

● (1735)

Mr. Glenn Foster: It would be to have more academic institutions offering cyber-related programs, and that goes to your point on different depths. Some are on basic security operations, as offered by local colleges, or basics of cybersecurity and networking. You could talk about the ethical hackers or the white hats that we talked about before. Moreover, there's the far more technical level of security that we commonly refer to as "application security". That would be beneficial.

If you look at the number of schools that offer these types of programs, you see that although we have some leading programs within Canada, they're not as broad as they need to be, and the number of students going in there is not what we need it to be.

I see talent, over the next decade, as probably being the number one crisis within large institutions in how we're going to meet the growing cyber-threat.

The Chair: We have about four minutes left, and I'm sure Mr. Spengemann would appreciate the generosity of Mr. Eglinski to split that four minutes.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Sure.

The Chair: You can have one question each.

Mr. Jim Eglinski: I have three questions, but I guess I'm going to have to work really quickly.

You talked about Israel and how collaboration works very well there because a lot of these people came through back-door military training and such.

Do you have a collaboration among the other major lending institutions in Canada? Do you work together and feed information back and forth, for example on what's a bad thing, a good thing, etc.?

Mr. Glenn Foster: Yes, we do.

Mr. Jim Eglinski: And in your system, do you have the capability of finding out if someone is hacking the customer's system at home? Can you let your customers know through your ability to check them?

Mr. Glenn Foster: On the first part of that question of whether we share information with each other, yes, there is a threat-intelligence working group under the CBA cybersecurity specialty group, which all the banks and CSE attend and provide updates to as well, which we find very helpful.

We share indicators of compromise. These are technical indicators on the types of threats and bad actors that we see and how to identify them. We find there's a great strength in doing that. We know that adversaries, criminals, share very broadly in the dark web and in other chatter about vulnerabilities they find in institutions and banks. I think likewise, we should take advantage of that.

On your second question of whether we see vulnerabilities that occur in the customer's home, no, we do not. Typically all we see is the transaction as it comes into our servers.

Mr. Jim Eglinski: Did that sound like two minutes?

The Chair: Almost, but Mr. Spengemann is going to appreciate your generosity. He might even send you a birthday card.

Mr. Jim Eglinski: Thank you. That's very nice of you, Mr. Chair.

Mr. Glen Motz: I'll send candles.

Mr. Sven Spengemann: Thank you, Chair, and thank you, Mr. Eglinski.

Thanks very much, Mr. Foster. As a former employee of TD, it's a pleasure to welcome you.

I'll roll my questions into one. We have the privilege of having you here as the chief information security officer of a major bank. Can you give us some insights into how your role is structured, what your responsibilities are and how you intersect with other major parts of the bank?

In the same breath, can you give us an appreciation of how much room there is for a major bank to be creative to develop its own security platforms? To what extent are you really constrained by the realities of the use of digital technology in limiting, first of all, the percentage of expense on security, but also the options that exist in terms of what you do to protect daily operations?

Mr. Glenn Foster: Where I sit organizationally, I report to the head of enterprise operational excellence, who reports to our group head, who reports directly to our CEO. My group has a head of innovation technology and shared services at TD Bank.

We felt that for strong governance, it was important to separate the CISO role from the technology organization, both for objectivity and as a reflection that cyber is really a business risk, not a technology risk.

We find that business engagement, in terms of process and products and how we engage our customers, is paramount to the success of our cybersecurity program.

As far as your other question is concerned, I had a bit of difficulty understanding whether you were talking about a percentage of spending or caps on spending.

● (1740)

Mr. Sven Spengemann: It was on the cost of providing security. In other words, are your options effectively prescribed or constrained by the current marketplace, or are there creative options and even differences among the major banks in terms of how much they spend on security as a percentage of total operating costs?

Mr. Glenn Foster: I think there is variability among banks, partly because we're not necessarily all organized exactly the same way. If you look at any information security organizations, it's the 80-20 rule: 80% of us have the same things in our organization, and 20% may be federated or decentralized in other areas. It's very difficult to track apples to oranges.

At TD bank, cyber is the top risk. Getting budgets is not a problem for me. We have top executive support, we have board support, for the program. Any constraint I face would probably be in the form of two things.

First is the amount of change the organization can go through in a given year. This is a fast evolving space. My spend has been growing at a compound annual growth rate of about 35% to 40% year over year. That's a lot of change to try to push into the organization.

Second is the availability of commercial products. The explosion, as I would call it, of security products within the industry is a lot to weed through to decide what's more hype than legitimate protection. I would find that for the most advanced organizations—we talked about big data and AI—the most uplift in the coming years would be in investments in our own skills and our people with data science and to be able to solve the problems of our bespoke applications as opposed to the general use vendors.

The Chair: Thank you, Mr. Spengemann.

Unfortunately, we have to bring our time with Mr. Foster to a close.

I want to thank you for your patience with us.

With that, the meeting is adjourned.