HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 154 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, April 1, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Monday, April 1, 2019

● (1600)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Ladies and gentleman, we have quorum, and we have lost half an hour.

I'm just going to ask all the witnesses to come up to the table directly.

My proposal, colleagues, is that we mash the panels. I've spoken to all the witnesses and asked that they be prepared to speak for less than 10 minutes. My thought is to give the panellists seven minutes each to make their presentations.

The first round of questions will be six minutes, and the next round, four minutes. We'll just run as long as we can.

I think there's another vote. We're not sure.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Are we not going all night tonight?

The Chair: Did you bring your cot?

An hon. member: Oh, oh!

The Chair: Okay, with that, the meeting has come to order.

I'll simply call the witnesses in the order that we have on the agenda, which starts with Mr. Green from Mastercard, followed by Mr. Davies from EY, Mr. Finlay from Cybersecure Catalyst and Mr. Gordon from Canadian Cyber Threat Exchange.

With that, Mr Green, you have seven minutes, please.

Mr. Ron Green (Executive Vice-President and Chief Security Officer, Mastercard Canada): Good afternoon, and thank you for the opportunity to be here today.

First, I want to praise the committee for launching this study. Cybersecurity is one of the greatest challenges governments and businesses are facing at the present time, with serious implications for national security, financial stability and consumer protection.

I also want to congratulate the Government of Canada for launching its national cybersecurity strategy and establishing the Canadian Centre for Cyber Security. I had the opportunity to meet with the leadership of the centre today, and we at Mastercard look forward to supporting their work however we can.

Cybersecurity is a top global priority for Mastercard. Safety and security are foundational principles for every part of our business and the innovative technology platforms and services we enable. We know that secure products and services are essential to the trust our customers, cardholders, merchants and other partners place in us. Let me contextualize this.

As you probably know, Mastercard does not issue credit cards or have a direct relationship with consumers. That is the purview of the banks that issue our cards.

Mastercard is a technology company. We provide the network that allows consumers to use their Mastercard virtually anywhere in the world, in more than 210 countries and territories, and have those transactions processed in seconds, connecting 2.5 billion cardholders with tens of millions of merchants.

For us to provide value to banks, merchants and consumers who use our network, we must provide safety and security. We cannot afford to have any interruptions in the operations of our network.

We are also investing in innovation: enhancing our capabilities in-house; acquiring cutting-edge technology companies; and nurturing our Start Path group of curated start-ups, including five in Canada, connecting with our issuing partners to grow their business. Just last month, Mastercard entered into an agreement to acquire Toronto-based Ethoca, a fraud solution powered by collaboration between banks and merchants.

At a very high level, that's what we're doing. Please let me now turn to our advice for government, which falls into six main areas.

First, in a networked, interconnected digital world, we need cybersecurity solutions tailored to small and medium-sized businesses. Cybercriminals will seek out the weakest point in the system to launch an attack. Therefore, we need to provide a framework for small businesses to protect their operations. Mastercard is playing a leading role in defending SMEs as we stand up our Cyber Readiness Institute, which emphasizes the practical application of tools for small and medium-sized businesses. The institute also facilitates the workforce development needed to implement these cybersecurity risk management tools.

In addition, keeping with this focus, in February, Mastercard and the Global Cyber Alliance released a new cybersecurity tool kit specifically designed for SMEs. This is a free online resource available worldwide. It offers actionable guidance and tools with clear direction to combat the increasing volume of cyber-attacks. There are operational tools, how-to materials and recognized best practices, all with an action focus. This tool kit will be updated regularly.

Second, global companies frequently confront an expanding and overlapping set of cybersecurity regulations in different jurisdictions. Those need to be harmonized using a baseline framework. We understand good trilateral progress was made here in the context of the NAFTA renegotiation, developing a common framework to align and manage cybersecurity risks, which is encouraging.

Third, there is a need to improve identity management and authentication as more devices are connected online. We need a robust identity ecosystem to enable easier and more secure digital interactions and transactions that safeguard the privacy of our cardholders.

Fourth, with the Internet of things there will soon be 30 billion connected devices. This creates enormous opportunities for the digital economy, but it also increases cyber-risk. Therefore, governments and the private sector should develop standards to improve the interoperability and cyber-threat detection and prevention while removing friction from commerce.

Fifth, as cyber-threats grow, governments and the private sector face a shortage of employees with cybersecurity skills. The world needs to start training the next generation of cybersecurity experts, and government has a role to play. If you have kids or grandkids, get them hooked on cybersecurity and they can make a lot of money in their lifetime, because right now the needs are there but the qualified security personnel are not.

Finally, collaboration, information-sharing and bringing all stakeholders to the table are required to fight cybercrime. President Obama commissioned an expert task force on cybersecurity on which our CEO sat. The task force issued a series of recommendations. The CRI, which I mentioned earlier, is a direct offshoot of the task force's emphasis on securing SMEs.

I believe this issue is so fundamental to the future of our economy and society that it needs attention from leadership at the highest levels. Mastercard is ready to lend its expertise to the Government of Canada in much the same way.

I could talk for hours on the subject but I will stop here and happily take questions on the areas that are of most interest to you. I have tried to provide a snapshot of what we are doing and what we think governments should be doing.

Thank you again to the committee for having me here, and I look forward to your questions.

● (1605)

The Chair: Thank you, Mr. Green, and thank you for respecting the time.

Mr. Davies is next for seven minutes, please.

Mr. Thomas Davies (National Financial Services Cyber Leader, EY): Thank you for inviting us to this session to provide insights and field questions on cybersecurity in the financial sector.

My name is Thomas Davies, and I am the National Financial Services Cybersecurity Leader for EY in Canada. I'm also a special adviser for financial crime for the firm globally with a focus on insider and outsider threats. Prior to joining EY, I spent eight years as a director of Scotiabank, supporting all three lines of defence.

Cyber-attacks are on the rise and the financial services industry is considered a high value target globally. The number of individuals, organizations and nation states with access to advanced tools has grown exponentially as service offerings for hacking have been developed and optimized by criminal organizations. Attacks on financial services are not limited to cyber-breaches. They can quickly move to fraud and money-laundering activities, which then create a strain on the talent and financial resources of any organization. These concerns are exacerbated by the shortage of skilled professionals across financial crime domains. A successful breach of payment systems, transaction networks or customer data could have a material impact on the economy.

Consider for a moment the implications of not being able to use your debit or credit card for a day or even a week. Imagine over one million Canadians trying to withdraw cash to pay for groceries, gas or medicine. Many global regulators consider the resiliency of financial services against a cyber-event to be a top priority for ensured economic health, as exhibited by new security requirements in Hong Kong, the United Kingdom and New York.

As Canadians demand greater access to financial services through digital platforms such as open banking, we need to consider embedding security and privacy principles into the design phase of a solution. In doing so, we will help to build customer trust, encourage adoption and proactively reduce the likelihood of costly fixes later. Implementing preventative measures such as training and awareness, access management, system hygiene, third party risk and corporate governance will reduce both the attack surface of these platforms and the maintenance required to support them.

Canada has an opportunity to become a global leader in security and privacy while continuing to be a great innovator of fintech. Through the continued support of shared intelligence, the development of talent through early and continuous education, and by enhancing public awareness of cyber-threats leading to financial crime, we can ready ourselves against this growing threat.

Thank you.

The Chair: Thank you, Mr. Davies.

I encourage colleagues to take note of the way in which these presentations are made in a timely fashion.

Mr. Finlay from Cybersecure Catalyst, please.

Mr. Charles Finlay (Executive Director, Cybersecure Catalyst): Chair and members of the committee, thank you very much for the opportunity to speak with you today.

Cybersecure Catalyst is a new centre for cybersecurity activities that was established last year by Ryerson University. It is permanently located in Brampton and will open its physical footprint in Brampton later this year. The centre will collaborate closely with governments and government agencies at all levels, private sector partners and other academic institutions across Canada to drive growth and innovation in the Canadian cybersecurity ecosystem.

We will deliver programming in four pillars. We will provide cybersecurity training for existing cybersecurity professionals, and introductory cybersecurity training for newcomers to the sector. We will support scaling-up Canadian cybersecurity companies through a unique commercial accelerator program. We will support applied cybersecurity R and D partnerships between academic institutions and private sector partners. Finally, we will deliver public education in cybersecurity, focusing on private citizens and small businesses.

In developing the mandate of Cybersecure Catalyst, Ryerson University engaged in a lengthy consultation process with industry and government, including a number of financial institutions. I think the results of this consultation process are important for our discussion of cybersecurity in the financial sector as a national economic security issue. When we asked major financial institutions and other private sector entities what they needed most from a university-based cybersecurity centre, the answer wasn't some specific technological tool or identified advance in the science. The overwhelming answer was more people. You have heard this from other witnesses before the committee today. In particular, we heard from financial institutions that they need their existing personnel to be upskilled to meet emerging threats, and they need more people to come into the sector to staff entry-level positions within their organizations. Every one of the major financial institutions in Canada has many current openings for cybersecurity personnel.

The anecdotal evidence taken from our consultation process is supported by the empirical evidence. As you have already heard from other witnesses in this hearing, in July of 2018 Deloitte and the Toronto Financial Services Alliance released a report that estimated that the demand for cybersecurity personnel in Canada was increasing by 7% annually and that 8,000 cybersecurity positions need to be filled by 2021.

It is important to note that this shortage is not just a security problem; it is an economic development problem. The lack of trained cybersecurity personnel creates staffing challenges for the regular operations of these financial institutions, but it also impacts these institutions' ability to create new and safe products and services for domestic and international markets. Crucially, the lack of trained personnel seriously impacts the ability for small and medium-sized Canadian cybersecurity companies to grow.

An interesting way to see the Canadian labour market problem in cybersecurity is to travel to Israel. Israel is generally acknowledged to have the strongest cybersecurity technology ecosystem in the world. The Israeli government has established a new major centre for cybersecurity activities in a small town in the Negev Desert about an hour by car from Tel Aviv, called Beersheba. In January, I travelled Beersheba to meet not with Israeli companies but with representatives of Canadian financial institutions that have established offices at Beersheba because they can find cybersecurity talent in Israel much more readily than they can in Canada.

That is the bad news. The good news is that this problem is well understood and efforts are being made to address the issue. This federal government's investments in cybersecurity in the 2018 budget were significant, in particular with the establishment of the Canadian Centre for Cyber Security. The centre is already acting as an important partner and voice for the cybersecurity sector in Canada. In the recently released 2019 budget, this government made cybersecurity a priority, allocating $80 million to post-secondary institutions to expand the pipeline of cybersecurity talent in Canada, among other measures.

Of course there is always more to do. In our view, training programs should focus on two key cohorts: young people in K to 12 and demographic groups that are seriously under-represented in the cybersecurity sector. Young people are not necessarily inclined to view cybersecurity as an interesting or exciting field of study or future employment, but this can change with the right engagement.

● (1610)

We will not solve the labour market issue of cybersecurity for financial institutions or for any other institutions if we don't open the cybersecurity sector to more women, racialized groups, new Canadians, indigenous Canadians, veterans and to those who have been displaced from legacy sectors. Efforts should be made to focus specifically on opening training and industry placement opportunities to individuals from these groups, and we will focus on that at Cybersecure Catalyst.

Finally, as our economy continues to transform, we see exciting opportunities to build talent pipelines between sectors where human labour is being displaced, and the cybersecurity sector where the need for qualified personnel is growing.

Thank you very much.

I'd be pleased to take your questions.

The Chair: Thank you, Mr. Finlay.

Mr. Gordon, you have seven minutes, please.

Mr. Robert Gordon (Executive Director, Canadian Cyber Threat Exchange): Thank you, Chair.

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

I'm the Executive Director of the Canadian Cyber Threat Exchange, CCTX. I'll highlight the work of the CCTX because I believe it has a direct bearing on the current focus of this committee's inquiries.

The CCTX is a not-for-profit organization established by the private sector with two broad mandates. First, we operate a cyber-threat information exchange to deliver actual intelligence to our members. Second, we provide a collaboration hub for the sharing of best practices among cybersecurity professionals. We're a relatively new organization, having commenced basic operational capacity just two years ago. I'll provide a few additional comments on our services in a minute.

The founding principles of the CCTX make it unique. First, our aim is to attract members from all sectors of the economy, not just those from critical infrastructure. We currently have members from accounting companies, law firms, the health sector, construction firms, entertainment companies, airport authorities and technology companies, among others.

Second, the large companies that founded the CCTX made it clear that the CCTX cannot be just for large organizations. We need to attract small and medium-sized organizations. In every sector of the economy, all sizes of organizations are experiencing cyber-attacks. We've grown from the initial nine founding members to just under 60 today, with additional applications being processed weekly.

In January this year, we changed our membership and fee structures to make membership more attractive to small and medium-sized organizations. Those changes have been really well received. Small organizations now represent 28% of our membership, and we're working to ensure this number grows significantly. As we increased the number of small organizations, we were developing cybersecurity reports and services specifically tailored to meet the needs of the small business owner.

I'll briefly highlight two of the service delivery areas.

We operate a cyber-threat information-sharing hub. Threat information is provided by participating member organizations. The threat intelligence received does not contain personal information, and the source of the information is anonymized.

The CCTX also receives cyber-threat information from the new cyber centre. We're pleased to be the first organization to sign a collaboration agreement with the new cyber centre. This is an important partnership for the CCTX and the government. We believe we will benefit from the full cybersecurity capability the government offers, and the government is going to benefit by our being able to extend the reach of what they're doing to small parts of the economy they no longer service, particularly those areas outside the core critical infrastructure.

The CCTX also offers its members an opportunity to provide threat-related information to the government, while keeping their identities anonymized. As we continue to grow, we'll provide the government with a broader understanding of how cyber-threats are impacting the entire Canadian economy.

This committee previously heard from witnesses on the importance of developing the cyber workforce required to defend the Canadian economy. The CCTX plays a role in assisting the private sector in developing and retaining the skills they require. Our cross-sector collaboration capability provides a variety of forms to bring together cybersecurity professionals to share best practices and ideas. Practitioners get together to discuss new topics such as the new techniques that are being used by attackers, new defence technologies and strategies, and changes in the legal landscape that companies should be aware of. We deliver this capability through monthly webinars and in-person collaboration events. The time employees devote to participating in these events contributes to their retention of their professional certifications.

Financial institutions understand the importance of collaboration, which is why all six of Canada's largest banks belong to the CCTX. The banks recognize that through collaboration they can raise their own defences and make it more expensive for the attacker. We provide a unique cross-sector sharing forum. As an example of the beneficial and unique relationship of the CCTX, work is being done through our portal between the financial institutions and telecommunications companies on a very specific cyber-threat.

Banks have built an impressive capability to defend their networks from cyber-attack, and they are now launching a new initiative through the CCTX. They would like to share their expertise with SMEs and are working with us in helping to raise the maturity of SMEs in every sector's supply chain, not just those relating to financial services. Each bank has identified an area of expertise and presentations have been developed that focus on the needs of small and medium-sized enterprises. We're currently working on the delivery mechanism for this important initiative.

● (1615)

Collaboration starts with building a trusted relationship. The CCTX provides an environment where the trust can flourish. We're building a community where members don't have to be operating in isolation. When a crisis occurs, they have a community to which they can reach out for assistance. Creating this organization that shares threats and best practices across sectors and all sizes of companies is a key pillar to achieving the desired level of security in order to protect Canada's economic prosperity. Collaboration means you don't have to do it all yourself because “none of us is as smart as all of us”.

I look forward to your questions.

The Chair: Thank you, Mr. Gordon.

With that, Mr. Spengemann, you have the floor for six minutes, please.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Chair, thank you very much. I'll be sharing my time with my colleague, Mr. de Burgh Graham.

My question is for Mr. Green.

Thank you for being with us. Thank you for your expertise. I'd also like to thank you for your past service as an officer in the United States Army. I also serve on our Standing Committee on National Defence, and from the perspective of our armed forces I just want to let you know how much we value our friendship and alliance with the United States.

● (1620)

Mr. Ron Green: Thank you.

Mr. Sven Spengemann: You had a chance to visit the Canadian Centre for Cyber Security. My interest is in small and medium-sized enterprises. From your perspective, having clients that are SMEs, how much of a structural obstacle do you think cybersecurity is for start-up companies in Canada? What should the Government of Canada do more of, or do better, in terms of facilitating access to market entry points for those companies that are data-centric and depend on cybersecurity?

Mr. Ron Green: As someone who has visited a number of small start-ups, I can say that for many of them security may not be top of mind. It needs to become part of everything we do, not just for small businesses, but just as people.

When you leave your house every day, you lock your door. You need to have a certain level of cybersecurity hygiene in your everyday life. For businesses, especially those that have data available to them, it needs to be a part of what they do now. We're at a point in time where we need to help them with that, through best-practice sharing and access to experts. That is one of the reasons we engage with Global Cyber Alliance. We are part of many groups that provide best practices and how-tos, but it's about making tools available to small businesses to actually help them do something, rather than just telling them, “These are the things you should think about.” Give them the tools and access to the expertise.

At the cyber centre, they're certainly working on ways to provide information to small businesses. They'll never have intelligence organizations like I have, but certainly, you can break down the information enough to help them on the journey to get more secure.

Mr. Sven Spengemann: That's very helpful.

I'm going to hand it over to my colleague.

Mr. David de Burgh Graham: Thank you.

Mr. Davies or Mr. Green, I'm not sure which of you can answer this. How does liability work for financial institutions that have losses related to cybersecurity?

Mr. Ron Green: With cybersecurity incidents and breaches, there's a place where the victim can be victimized twice. You have the threat actors that steal the money, and then you have the ensuing civil and criminal cases that take place afterwards. Sometimes, depending on the company, they are then taxed more, or they spend more time on it.

From our perspective, we work with a body comprised of our lawyers, the acquiring company's lawyers and the merchants that are involved in the issuing. We work out a reasonable compensation between all of the impacted organizations. That's for payment card breaches. It may differ depending on other breaches that take place.

Mr. David de Burgh Graham: Are the financial institutions insured for cybersecurity? Is there a separate insurance for that?

Mr. Ron Green: There is cybersecurity insurance. I guess it depends upon which country you are in and the insurance that's available to you. I go through a rigorous review annually with our insurance providers to make sure that I'm maintaining a proper level of security for the organization, so that we can then take advantage of the insurance opportunities that the company provides for us.

Mr. David de Burgh Graham: This question is more open. When you're hiring cybersecurity professionals, what level of vetting is done for these people? It's not a normal job interview, or is it? Do you do vetting to make sure they are not going to introduce vulnerabilities rather than fix them?

Mr. Thomas Davies: I can take that one.

We do a technical review of most...in our community. It's a small community, so we benefit from the fact that we typically know someone who has worked with these individuals before. It's a plus and a minus, a pro and a con, but we often look at references and understanding the environments that they worked in before and how that work has gone. Then we go through a technical vetting process to understand. It's usually a longer cycle, which also has its negatives, in that it takes us longer to board secure professionals in this area.

Mr. David de Burgh Graham: We're talking, Mr. Finlay, about the need to expand the number of people in cybersecurity. We're trying to make sure that as we go into a massive expansion—as we saw in 1999 with the technology bubble—we don't introduce a whole lot of people whose intentions are not necessarily what we're looking for.

Is there an intention to make a degree in cybersecurity separate from a degree in computer science at some point?

Mr. Charles Finlay: Cybersecure Catalyst is going to focus on training for existing cybersecurity professionals, and introductory training to bring new professionals into the sector. We are not going to focus on giving a degree right now out of Cybersecure Catalyst. Degree programming in cybersecurity is being developed by many post-secondary institutions. Many post-secondary institutions, including Ryerson, have courses in cybersecurity. Our particular focus is on the professional training, because candidly, that's where we feel we can make an immediate impact within the next couple of years, so that's our focus.

There are all sorts of different models of degree programs that are offered by different institutions across the country.

● (1625)

The Chair: Thank you.

Monsieur Paul-Hus, you have six minutes, please.

[*Translation*]

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

Mr. Green, I like what you said in your presentation. I see that Mastercard has really established priorities, in addition to identification, protection, detection and response methods. I also like your relationship with the different companies.

In your presentation, you also gave advice to governments. You mentioned the need for coordination among the different countries. I want to know where Canada stands. What are Canada's strengths, and, above all, what weaknesses should it address?

[*English*]

Mr. Ron Green: I think, fortunately, Canada does lead the way in cybersecurity technology development. I just mentioned Ethoca. We also acquired a company called NuData, which powers a lot of the security control features that we enable within mobile devices. I think there's an opportunity to continue that effort to develop new cybersecurity solutions that can help the marketplace, the fintech environment. I think that is a strong place to come from. You are also, just being at the centre, very open to working more collaboratively with the private sector, so there's the ability to share intelligence information.

There are things that we have an opportunity to see globally that may be of interest to your teams, and hearing from your teams about new threats that are out there gives us an ability to more proactively stop things from happening. That's a big interest for me.

[*Translation*]

Mr. Pierre Paul-Hus: There are different threats. Some threats come from individuals who try to hack into a system. However, rogue states, such as China, also attack our systems.

As a private company, how do you respond to a cyber attack carried out by a state? Do you expect the Government of Canada to take action? Should government resources be involved? You'll take the first steps, but do you expect anything from the government in the event of an attack carried out by a state?

[*English*]

Mr. Ron Green: We have to defend against all comers, individuals all the way through nation-states. We think about all potential threat actors that there may be, and we implement layered defences in order to overcome delay, and prevent such attacks from being successful. However, if such actors were successful, we would depend very much on our government partners to help us with the mitigation of the effect, but then also, depending on what the attack may be, take other actions. I only defend—that's my lot in life—but if something else needed to happen, it would have to be with one of our government partners.

[*Translation*]

Mr. Pierre Paul-Hus: Okay, thank you.

Mr. Finlay, we now see that all stakeholders must work together. This includes the government, private sector and university sector. We're talking about workforce training in cybersecurity.

Do you have any advice to help us ensure that all these stakeholders work together? Since everything moves very quickly in cybersecurity, speed is key. We mustn't get bogged down by excessive administrative measures. Do you have any advice for us?

● (1630)

[*English*]

Mr. Charles Finlay: I frankly think that the establishment of the Canadian Centre for Cyber Security is a fundamental improvement in the Government of Canada's position in respect of cybersecurity and in bringing all the partners together.

You properly identified industry, the academy and government having to work together.

I mentioned Israel in my opening comments. What's interesting to me about that ecosystem is how closely those three pillars of civil society, if you like, work together on the cybersecurity problem. I think that the Canadian Centre for Cyber Security acting as a convenor in bringing all those parties together is very important. In terms of advice, I think that the government's and the administration's opportunity to counsel all parties to work closely together is very important, and that it should be made a repeating theme, in terms of your discussions about cybersecurity, that everybody needs to work together.

[*Translation*]

Mr. Pierre Paul-Hus: My next question is for all the witnesses.

At this time, do you think that Canadians in general are naive about cybersecurity?

[*English*]

Mr. Thomas Davies: I wouldn't say naive. I think we're a little bit more numb to cybersecurity events than other cultures. I think we're a little bit quicker to let it go. That would be my comment.

The Chair: Go ahead, Mr. Green.

Mr. Ron Green: I think about when we adopted things like the automobile into the environment. There was a period of time where no one understood, no one knew what it was, and we're all lucky to be alive because none of us had car seats or anything like that. If you look at cars today versus cars a long time ago, you will see lots of maturity, lots of improvement. We're in that same kind of cycle. We're not naive. It's just that we're still innocent about these things. We have to pick this up.

The Chair: Thank you.

Monsieur Dubé, you have six minutes.

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

Mr. Green, this whole notion of not being a card issuer is something that I recently was helped to understand by folks in your company. It adds a lot of wrinkles, I think, to how this process works.

I'm just wondering if you could walk me through a few things.

Mastercard is in charge of the payments, the transactions themselves, and then you have a card or a device or a website, sort of these third party things out there if you're using Apple Pay or something like that. And then there's the bank, which would be the card issuer.

Through that triangle, if I could put it that way, how would the accountability work, let's say in terms of my information? In other words, if I'm using my phone to pay for something and there's an issue, then is it incumbent on the banks, the card issuers, is it incumbent on Mastercard, is it incumbent on Apple because they caused a problem with Apple Pay? How does that work?

Mr. Ron Green: A lot depends on the particular incident, with respect to who's more responsible for the issue that occurs. First and foremost, an attacker is always the first person. They are the ones who did the wrong thing, but within the four-party model, there's an issuing bank, an acquiring bank, and then you have the merchant and the cardholder.

The cardholder reaches out and works with the merchant, and I would say a lot of times we encounter issues with the merchant because there's some sort of security issue, there's something wrong there. Maybe information is captured or stolen from this point.

We're doing a lot to remove the value of any information that the merchant may have with tokenization. If you use your Apple Pay, there's not a PIN, there's not a 16-digit number that you're most comfortable with. We provide a token that can only be used a certain way. You can't steal it and then make it usable on another device or a computer. There's a token that's on your Apple Pay. We power the token that's in Apple Pay. We're taking that tokenization—

● (1635)

The Chair: Mr. Green, for the edification of the chair and possibly other members who might not heard of tokenization, I wonder if you could give a brief explanation of what that means

Mr. Ron Green: The 16 digits that make up your card are what we call a PAN. It's a certain number that you're most common to use —you know it and you see it because it's on your plastic card. A token is something we create. It actually works throughout systems, but we can create them and throw them away, then reuse them.... It's not as fixed as just that 16-digit number.

So when we create a token, like in the case of a merchant where... we replace PANs and we work with them to place tokens. If they are breached and the tokens are stolen, it doesn't matter. We'll just make new tokens. We will take away the value of the PAN—the credit card number—and replace it with a token, so we can just create more tokens.

Mr. Matthew Dubé: That's interesting, because it sort of leads me to wondering about AI and biometrics.

I'll use lay terms, if you'll forgive me. You're enabling, in a temporary way, different payment methods. The question then becomes, if AI or biometrics are being used in different ways—to understand the types of transactions people are doing, when they're doing them or things that are occurring on a device—isn't there inevitably a more concrete connection that's being made than just sort of this throwaway stuff?

Again, I'm trying to see it through a layperson's lens, this notion, because it seems to me there would be a stronger connection at that point if you're enabling that type of data collection.

Mr. Ron Green: It's not all about data collection. It's about having the right data at the right times.

I don't want to make this too difficult, but in the future, identity stores will be less important than the ability to get the identity information when you need it.

When you want to make a transaction, we can connect to the identity stores to pull in the information to identify you, Matthew, when you need to make that transaction. Then when you're done, it all goes away. There's no need to store it. We just want to reach out and make sure the information is there when you need it.

Mr. Matthew Dubé: Is there not a landing point for something, at some point? We had a witness a couple meetings ago who said, “it sounds silly but the cloud's not actually a cloud”. There's a space where the data is being stored.

Mr. Ron Green: Yes, it's in a computer somewhere.

Mr. Matthew Dubé: Absolutely. This data is landing somewhere.

Even though there's a protection for Apple Pay, let's say, with this token, there's still a transaction taking place and then something's landing somewhere and staying there, without any....

Mr. Ron Green: It can be transitional, so it's there for a period of time. It's not there for always. It's there when you need to do the thing that you're trying to do, and then when it's no longer needed, it's gone.

Mr. Matthew Dubé: I'll kind of walk through to what I was asking the banking association representatives about when they were here.

If I'm using a banking app on my phone to pay my credit card, inevitably I'm doing it through the bank, but there is information that has to go to the credit card company in that case.

Mr. Ron Green: The information that we transact is a PAN—the 16-digit number—and the date, time and the amounts. We don't hold cardholder information. Your issuing bank does.

We see just that the 16-digit number did a thing. The merchant asks, “Can the 16-digit number pay for it?” We ask the issuer. We don't actually know the cardholder, but the issuer knows the cardholder. The issuer says, “Yes. That 16-digit number that belongs to Matthew can pay for that”, and then we pass that information back to say, “Yes, they can pay for it”. Then a charge goes back.

It's all information that passes from one side to the other. Depending on what you're asking for....

Mr. Matthew Dubé: In other words, you would have the merchant name, the card number and the amount, essentially.

Mr. Ron Green: Yes.

Mr. Matthew Dubé: That's not necessarily stored in Canada, so is that subject to protection from Canadian law?

Mr. Ron Green: We have to be compliant with Canadian law for the data for Canadian citizens. Right now the majority of transactions take place at our St. Louis or Kansas City facility. There are other locations that also do work for us. The data needs to remain local only. From where I sit globally I can see threat actors attempt to work against the payment system no matter where they are. But as countries localize or look for localization of data, and that data can't be used in other places, the ability for me to analyze and see where the threat actor moves becomes more difficult.

The threat actors don't care about borders. They're willing to attack Latin America or Europe or Canada or the U.S. If I can see their attacks taking place in Latin America, but I'm not allowed to use that information to help protect another country, the attacker can then move without my using the learning to protect the other, so attackers can continue to attack different places without my using the information to help protect it.

● (1640)

The Chair: Thank you.

Mr. Picard.

[*Translation*]

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

Mr. Davies, you provide consulting services to financial institutions. In business, one challenge is to properly manage security investments and risks. It's about balance. When it comes to investing in security measures, we must consider whether paying for any possible damage would be cheaper than or equal to the cost of investing in security.

For a long time, the perception was that financial institutions limited their investments in security and chose to pay for damage that occurred as a result of incidents because it was more beneficial. Is this type of resistance still encountered or has the market changed with regard to security?

[*English*]

Mr. Thomas Davies: I would say that they are investing heavily in protection in cybersecurity. There is brand and reputational risk. While in the community we talk about not competing on security itself, I believe the financial institutions do compete on customer trust.

The biggest issue the financial institutions have today is actually having the individuals necessary to deploy the capital. They have robust budgets and they set aside adequate funding, but to try to get through as many projects as they do with the limit in skill shortage becomes a challenge.

[*Translation*]

Mr. Michel Picard: It should be noted that third parties that have access to financial institutions may not have the financial means or tools to protect themselves from risks. As a result, they may represent an access risk to the financial system. Do the industry's security investments still protect the market?

[*English*]

Mr. Thomas Davies: Third parties that service financial institutions are considered one of their greatest risks. The financial institutions develop a really strong security program but then can be weakened by an external party. Third party risk is something taken very seriously by the financial institutions.

I think one of the issues is that people believe that cybersecurity is an overly complicated domain when a lot of breaches occur due to the basics being missed. I think that proper education, in terms of what the basics are and how to go about resolving them, can greatly mitigate that risk. We are seeing financial institutions start to basically mandate that their third parties have certain minimum controls inside of contracts and that there is an assumption of risk along with them. In Canada we have OSFI that regulates the banks. If a third party is the reason for a breach, OSFI doesn't really care that it was a third party. It still holds the bank liable, so the banks are taking this very seriously and are going through heavy risk programs to mitigate this issue.

[*Translation*]

Mr. Michel Picard: My next question concerns human resources, and it's for Mr. Davies and Mr. Green.

From a consulting perspective, the focus is on recruitment, while from a client perspective, for example at Mastercard, the focus is on the risk posed by human resources.

I want to share an anecdote. A number of years ago, I filled in a credit card application form properly—I won't say which card. When I received the card, the credit limit had already been exceeded. Obviously, I contacted the security department. The problem wasn't caused by me, but by the security department when the card was issued. The problem came from the inside.

In a previous life, I attended Canadian Bankers Association meetings, where we talked about payment terminals that were impossible to break into. However, the terminals were broken into within three weeks. We think that there's still a risk of inside jobs.

How is this human resources risk, which seems to lead to a dead end, managed for both the client and the consultant?

● (1645)

[*English*]

Mr. Ron Green: We do a great deal of background checking on our employees before we bring them on, but we also have insider threat programs. We know what the correct or usual behaviour is, and then we look for anomalies. I had an opportunity to take my board through what we have in our insider threat program, but we have a way of sensing when people are acting abnormally.

When those triggers are set, then my team will launch an investigation to see if the employee is acting in a way that is not in the best interests of the company.

Additional to that, we have employees who have high-risk roles. The things that they do allow them the ability to make or destroy machines, or things like that.

We have an increased level of monitoring, so my guys watch what it is that they're doing. It's all in behind the scenes, but it happens to make sure they they're doing the things that they are supposed to. If they're not, then we respond to it.

Mr. Thomas Davies: I'll add that the insider threat is the number one concern of most chief risk officers, because of the magnitude of the event when it occurs. You know, the Edward Snowden discussion comes up often in terms of national security. The idea that an insider has access to privileged information is always a concern.

There is a discussion around enhanced monitoring under what we call powerful users, people who have—to Mr. Green's point—powerful privileges inside the organization, and making sure to mitigate the risks.

So one account is frauded, that's a mitigated risk, and there's a certain risk tolerance you have to have internally. You can't guarantee that nobody will do a bad thing, but you can minimize the impact and do some basic training and awareness.

When I was a member at Scotiabank the code of ethics, business conduct, know your customer, and anti-money and laundering training were mandatory. It is important to have that be a mandatory component and to at least give everybody the sense that you're here to do the right thing.

The Chair: Thank you.

Mr. Motz, you have four minutes, please.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Chair, and thank you for being here, gentlemen.

Mr. Gordon, we've heard from previous witnesses to this committee that countries like Australia and Israel have pretty effective information-sharing networks between industry, government and academia. We haven't heard necessarily that the same exists in Canada. Could Canada improve in this regard, and if so, how should we go about doing that?

Mr. Robert Gordon: I think we actually are improving. I think one of the big steps was creating the new cyber centre to do that. It's one of the reasons why we're working so closely with them to do that linkage between what the private sector is doing and what the government's doing.

As a matter of fact, we're working with some Australian organizations to create an organization in Australia similar to the CCTX, to do that cross-sector piece. It's one of the ways of bringing together all of the companies, all regardless of size or what they're doing, and bring them forward in a way they can start to interact with the government.

The government's going to be looking after the cyber centre, a fairly narrow window into the critical infrastructure—that's what they are going to scale to—and they're looking at us to expand that out to all the those sectors and areas that aren't going to be covered by what they're doing. The government can be providing some general advice, but a lot of it is taking the general advice and saying, we need to do something in technology, but as an individual within a company, how do I actually do that?

It's a little bit of the skills development that Mr. Finlay was talking about. We're trying to bring that along, to take the knowledge the government is providing and then translate that by getting individuals who are going to execute on using that technology to sit down and figure out how you actually do some of these things.

● (1650)

Mr. Glen Motz: Your organization has a platform that's now more accessible to the smaller markets, to small and medium-sized business, and they're taking advantage of that.

Have you observed any attacks in those start-ups, in those smaller enterprises, that have grown from there?

Mr. Robert Gordon: On the companies that we have, no, but that's been happening.

A lot of examples come out of small companies. Part of the supply chain is being the source of the target into the much larger organizations. It's one of the reasons—and it was said previously—the banks are so interested in looking at their third parties and what they can be doing to try to enhance the cyber-resiliency of that third party, because they're all hooking into their systems.

It extends beyond that into literally every sector. For example, when dealing with the owners of large buildings who are now worried about all the tenants of their building hooking into them, you're only as strong as your weakest link. Every sector is going through the same issue.

Mr. Glen Motz: A previous witness to this committee said that Canada is often the first victim of attacks, and it's partly due to the fact that we have fewer resources than our friends to the south have.

In your exchanges and with the allies, have you seen that to be so?

Mr. Robert Gordon: That we're being attacked first, or...?

Mr. Glen Motz: You have a lot of interaction with our allies.

Are you seeing that Canada sometimes might be the first point of attack on some of these issues, as opposed to some of our allies?

Mr. Robert Gordon: Yes. The attackers will come after countries for a variety of reasons.

In some instances, we may be the only target of an attack coming in, and other times we'll be a jumping-off point for attacks starting here and going elsewhere, or we can be the second country going down, where the attack starts somewhere else and then comes over to Canada. We get hit in all three areas.

Mr. Glen Motz: That's perfect.

Mr. Davies, in your view, what are the biggest cybersecurity shortcomings that you see or experience in the Canadian financial sector?

Mr. Thomas Davies: The biggest issue they have is legacy sprawling systems, and proper hygiene over those systems is still extremely challenging. Security tooling doesn't really exist for a lot of older systems, where they have to build what we call a ring fence to protect that asset. It's still the number one issue. It sucks time.

Mr. Glen Motz: I have a follow-up to that, because it's important to that issue.

You're right. If you're old like John and me—

The Chair: Thanks very much.

Mr. Glen Motz: Our bank data is old. Wouldn't financial institutions—rather than trying to build, as you called it, a ring fence or protection around that—transfer that to software, to mechanisms, that could now secure it better, as opposed to just trying to protect it in the medium that it's in?

Mr. Thomas Davies: Yes. They would love to simplify that environment. It is challenging based on some of the old systems that are still required for the branch network and for other systems throughout their global network. It's certainly on their radar, but incredibly challenging and incredibly resource expensive.

The Chair: Thank you.

Ms. Sahota, you have four minutes, please.

Ms. Ruby Sahota (Brampton North, Lib.): Thank you, Mr. Chair.

On this committee, we've been hearing quite a lot about the collaboration that's needed among the government, private and academic sectors.

Mr. Finlay, you spoke about your visit to Israel and the need for us to gear up and be able to provide the type of training they do. Can you explain a little more about Cybersecure Catalyst, how it compares to some of the training that's provided in Israel, and what the similarities and differences are?

Mr. Charles Finlay: There are a number of different things that are interesting about how the Israeli cybersecurity ecosystem trains its people. It obviously has a unique national service characteristic, with military service in Israel that is different from the Canadian context.

One of the interesting and powerful things that they do is start young—K to 12. We think that is a very powerful way to get at the root of the cybersecurity labour market issue, by making young people very interested in cybersecurity and engaging them in cybersecurity careers. Ryerson, in partnership with Royal Bank of Canada and Carnegie Mellon, one of the leading universities in the United States in cybersecurity, ran a hack-a-thon called CanHack in 2018. It's an online game where high school students engage in monitored, supervised, safe cybersecurity tasks. Our projection was doubled in terms of the number of students who engaged in that program.

We think the opportunity there is extraordinary. That's piece number one, in terms of young people. Piece number two is engaging demographic groups that are under-represented in cyber and workers who are being displaced from legacy sectors. There's an opportunity to introduce workers who are being displaced from some sectors that are losing personnel, to train them up so that they can enter the cybersecurity sector at an entry level. We think that's a very exciting proposition.

Those are two things we hope to do and those are analogous to things we have seen being done in other countries, including Israel.

● (1655)

Ms. Ruby Sahota: You spoke about meeting some Canadian companies while you were there that have either temporarily or permanently shifted over in order to receive these types of services, training, for their personnel. What companies or what types of companies are you referring to and do you envision these companies coming back and perhaps setting up near Cybersecure Catalyst?

Mr. Charles Finlay: Yes, we do. At Beersheba there are the major Canadian financial institutions. The major Canadian banks have offices there, and they are there because the skilled people are there. We believe we can create an ecosystem where we're training people. Industry is there to acquire that talent, companies are scaling up through the accelerator program, and university-based researchers are also working with entrepreneurs and with the trainees and the industry. What we saw in Israel exists in other countries too. But what's particularly conspicuous there is they have this alignment among industry, academia and government, and we believe that pulling those pieces together at Cybersecure Catalyst will create that ecosystem.

The Chair: Thank you.

Mr. Dreeshen, welcome to the committee. You have four minutes, please.

Mr. Earl Dreeshen (Red Deer—Mountain View, CPC): Thank you very much, Mr. Chair.

Thank you to the witnesses.

Just a couple of things I've been thinking about as I've been listening to some of the discussions. There are a lot of institutions and businesses that have been attacked, and people have gone after their information or frozen their information. Various universities... there would be ransoms that are set up there. That's important when it comes to how businesses are going to be able to move forward, but also smaller businesses start to fear that.

I'm just wondering what types of investigations are taking place and how successful those investigations are in taking care of that particular problem. A lot of small companies worry about the way they might be attacked and being held ransom.

Mr. Thomas Davies: Sir, I can take a first stab at it.

There's not a great job done today of disclosing the nature of breaches in the general public. The banking group does share information in order to try to protect each other from getting hit by the same issue, but outside of that, that information is pretty private and can have a material impact on your operations and the reputation of your brand, so it's largely kept internally.

In the U.S., I believe it's the FBI that has a little more detail in terms of business email compromise and other ransomware and other types of events that happen. To collate that data in Canada, to give an idea of people...the themes that we're seeing, we can talk about them here and talk about access management and system hygiene and training and awareness, but to prove it with real data would be helpful.

Mr. Ron Green: I think also with the crypto-locking or the ransomware attacks that you're mentioning, a lot of that comes back to some basic hygiene stuff. Knowing to update or patch your systems would certainly relieve a lot of the problems. Having antivirus software would relieve your problems. Being smart about phishing.... The Verizon data breach report says that 93% of the breaches that took place were because of a phishing attack. I can tell you that we take it very seriously at Mastercard. We have a "three strikes and you're out" rule. My phishing stats for February were 0.4 fail rate, and consider that 20% is about standard.

It's helping those smaller businesses understand the basic things that you need to have and, in case it all goes wrong, backing up your stuff so if it is locked up you restore it and then you can overcome your problem.

● (1700)

Mr. Earl Dreeshen: There's a lot of money that's being made in the fear factor. I think back to Y2K and the way everybody was so concerned about what was going to happen to the computer systems and so on. A lot of people were making money solving a problem—you folks maybe know whether it was serious, but lot of others thought it was simply a hoax.

Maybe you can comment on that, but I guess my concern, too, is on protection of intellectual property, the concern that people go to all this work trying to develop...and then have other actors, whether they be people, other countries or other companies.... How are you able to determine how best to protect or how people should be trying to protect themselves?

Someone can talk about Y2K if they want.

The Chair: If you're going to talk about it, be very brief.

Mr. Robert Gordon: I'll skip over Y2K, then.

One of the challenges for companies is getting them to actually identify the critical information in their systems that they need to protect. If you don't know what's critical, you can't protect it all, so you start to layer it down on the things that are more important, then you can start to control who gets access to it.

One of the interesting challenges for a lot of companies, particularly when you're talking about ransomware and small companies, is that they traditionally think they haven't any big trade secrets, nothing that somebody wants to steal.

The problem with ransomware is that they don't want to take anything; they just want to deny you access to whatever you have that's of value to you. For a lot of small companies, that's quite a mind shift to get around, because once they get around that, then they can start to realize why they now have to be taking an interest in ransomware, both in terms of the defence of things—there are some things that can be done—and if it happens how they actually recover from it.

The Chair: Thank you.

Ms. Dabrusin, you have four minutes, please.

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

Perhaps I can get some direction from the chair, because I'm also on for the next seven-minute block, so do I have 10 minutes, which I can share with someone?

The Chair: My thought was that because of the efficiency of the witnesses we have, that efficiency has actually spilled over into the members. We therefore have about half an hour, so we merged this. My thought was that, after Mr. Dubé does his final three minutes, the chair might exercise a little prerogative and ask a couple of questions, but we would open it up for three-minute rounds to run out the clock.

Ms. Julie Dabrusin: Thanks.

I was looking at the Cybersecure Catalyst website earlier, and I saw that there was something on it that said that the annual growth rate in trained cybersecurity professionals labour demand in Canada was 7%.

I was wondering where that figure comes from. Is that something that you've seen as a trend year over year? Do you anticipate in that same range?

Mr. Charles Finlay: Yes, that comes from a report from Deloitte and the Toronto Financial Services Alliance 2018, where they estimated that the growth rate was 7% year over year.

Ms. Julie Dabrusin: We've been talking about the need for training and having a skilled labour force for this. What is the kind of training time period you're talking about? If you have high school students who graduate and say “I'm interested in cybersecurity”, how long is it from the time those students graduate and complete all the programs to the point that they're hireable in cybersecurity?

● (1705)

Mr. Charles Finlay: It's a terrific question. There are a bunch of different pieces. We are looking at continuing education, so essentially we are working with employers to upskill their existing personnel. The time frames depend on exactly what skill set those employers need. That's a particular issue in cybersecurity because the threats and the technical frameworks are changing all the time. That's in respect of the executive education base.

In the introductory training for under-represented cohorts, we are looking at six months of programming. In our view, a six-month intensive course can take an individual with relatively little technical training to an introductory entry-level position and make them eligible for entry-level internships and secondments into industry. Then there are undergraduate courses in cybersecurity and computer science, which follow the typical undergraduate pieces. An undergraduate cybersecurity course could be three years; an honours course could be four years. Those are the different frameworks. All sorts of continuing education in cybersecurity of different lengths of time are being offered.

Ms. Julie Dabrusin: I'm just trying to figure out so that if I'm trying to explain to kids when they're graduating from high school, they have an idea of the timelines. They have to think about it. If they're thinking about student loans and everything they're going to be putting aside to get an education, if we're telling them this is a great career, there's a huge demand, it's helpful if we can at least give them a bit of a map of what that looks like. That's what I'm hoping someone on this panel could help me with. If I'm talking to a high school student, what am I giving them on how much time it would take, what are the degrees needed to get into this industry?

Mr. Ron Green: From my perspective as a guy who hires folks. I have members of my team who haven't gone to university or college. They had just tremendous interest, and they spent a lot of time in their high school years working on and understanding computers and developing a sense of security. They demonstrate themselves in our interviews and our tests, and we can see they will be a good person to bring onto our team. They'll be strong in the technical sense, but eventually they'll run into a roadblock because they don't have some of the background you'd want for management.

Right now it's hard to find people coming out of college with a cybersecurity degree. I look for someone with a technology degree, and I can train them on security in my security operations centres. I can give them on-the-job training. What is hard and what we look for in a lot of the roles is experience. We're looking for people who have the college degree. They may have a master's in cybersecurity, but then they have field experience, so your military folks, or people who defended large networks. They're few and far between. I've had roles that have taken two years to fill because it's hard to find the person.

The Chair: Thank you.

Mr. Dubé, you have three minutes, please.

Mr. Matthew Dubé: Thank you, Chair.

Mr. Green, you'll forgive me for harping on this. I'm just trying to walk through my understanding of it. When we left off, we were clarifying my question.

You talked about the local inability to identify a threat that's not necessarily going to recognize borders. I guess the concern can be flipped as well in terms of that type of information being accessible, say, to national security agencies or law enforcement. The specific example I'm thinking of is the concern that's been raised by the Privacy Commissioner here in Canada. For example, Canadians might now legally purchase marijuana with their credit cards. As it is illegal federally in the United States, if the border patrol were so inclined, that information could potentially see a Canadian being barred from entering the U.S.

If that information is there somewhere, for good or for ill, there's always going to be a risk of it being used. I'm just not clear on the accountability that exists, both in law and otherwise, for information for me as a Canadian dealing with a Canadian bank that might be stored on a server located in the U.S., or anywhere else.

● (1710)

The Chair: This is not a personal question.

Voices: Oh, oh!

Mr. Ron Green: There are a couple of things. We don't store you; we know a 16-digit number that belongs to an issuing bank. The Canadian bank would actually understand who Matthew is; all we know is a 16-digit number. We don't have any kind of open...our data is available to—

Mr. Matthew Dubé: Sorry to interrupt, I just want to jump in to understand. I recently moved and I changed my address. It got pushed back at me because it was not updated in the system. Whose system is that? Is that yours or the bank's, which is the card issuer?

Mr. Ron Green: Where are you having the challenge? Is it the zip code or something like that?

Mr. Matthew Dubé: I was trying to confirm a payment for an online purchase. I was asked for the name of the cardholder as it appears on the card, the three numbers on the back of the card and the address. Because I had changed it that same day, I ended up calling the helpline and was told I would have to wait until the system reset for the address to be up to speed. Is that the issuer?

Mr. Ron Green: Did you call the number on the back of the card?

Mr. Matthew Dubé: Yes, that's the issuer, right?

Mr. Ron Green: That's the issuer. That's your bank.

Mr. Matthew Dubé: If I'm dealing with PayPal, for example, and using a credit card, if I'm putting the number and the address, the number is going to you for validation, and then the address, the cardholder's name, etc., is going to the bank.

Mr. Ron Green: Right, and we use that number to talk to the issuer. Is this good information for us to allow the transaction? It comes through us by the 16-digit number, we pass it to the issuer—that's your bank, which knows you—that information passes and it says, "Yes, and he has the money." Then we pass it back to the inquiring merchant to say, "Yes, they have the money; go ahead and do the transaction." Then we pass the amounts back through to the issuer.

The thing that passes that helps us to make a transaction work is the 16-digit number, and that's the data we use.

The Chair: Thank you.

I have a couple of questions, and then I have Mr. de Burgh Graham and Mr. Paul-Hus, for three minutes, and anybody else. That should run the clock right down. No questions for Mr. Motz—ageism.

You know, part of this study is precipitated by virtue of the 5G controversy, and particularly the 5G controversy with respect to Huawei, Nokia and Ericsson. You three in particular are on the front lines of defence, and so my question is this. If this is coming down the track—and it is—how are you preparing for that, or are you preparing for that, and how would your preparations change what you've just said today, if in fact it would change what you just said today?

We'll start with Mr. Green and work to the right.

Mr. Ron Green: Sure, no matter what the communication vehicle is—mobile or 5G or Wi-Fi or even plugged-in networking—when our folks are in environments where they're leveraging those things, we provide a secure pipe so that it pipes through. Be it 5G, be it mobile, we will secure the data that transits that for our employees. A lot of what powers our network is that it's a private network. We aren't on the Internet; the things that enable commerce to happen are on a very private network that we control. If I'm using a 5G network, I'm going to secure a pipe so my people can communicate securely. The network that we ride, where we do all our work, is our own private network.

The Chair: Really, is the entire Mastercard processing around the world a private network?

Mr. Ron Green: It is a private network that we enable out to the edges. That's some of the reason it's difficult to do the things we do, because it's taken us time to build this private network that we have.

The Chair: Mr. Davies.

Mr. Thomas Davies: Sure, we try to focus on protecting data from end unit to end unit. While it's in transit, no one else should be able to read it. That is the goal, depending on whether people have the technology to be able to intercept and change and whatnot.... That is advanced technology. It is possible, but by taking the basis that only one entity can read and send, and then once it enters its exit phase, it is then decoded and read again, it's exactly what Mr. Green just said. It can be done by private network or it can be done by public network, but that is the focus.

● (1715)

The Chair: Your clients would not have a private network, would they?

Mr. Thomas Davies: It depends on what kinds of systems they are using. For example, there are private networks between the banks for SWIFT messaging, wire transfers and such, and then there are public networks for dealing with their customer bases.

It depends on what criticality of asset they are resolving. For example, in a lot of cases they will have dedicated private networks for their third party service providers as well.

The Chair: We had one security person describe it as secure here, secure here and a cardboard box in between.

Wouldn't a number of your clients have exactly that issue whether the cardboard box is here, or there, or in between it's still unsecure?

Mr. Thomas Davies: To reduce that is the goal. It's like coding a message when we used to send messages back and forth during the war in indigenous languages so they couldn't be read midstream. We do the same thing today. As a message is being sent through the wire, you try to keep it as decoded as possible, but once it gets to its destination, someone has a token or a key to unlock the information and understand what's there.

The Chair: Mr. Gordon, do you want to add anything?

Mr. Robert Gordon: From the very narrow perspective of the CCTX, it's not going to matter because that responsibility will reside with each one of our members having to deal with it. Depending on the type of member we have, they will be dealing with it from the financial institutions or they will be relying on the public network.

The Chair: What do you mean it doesn't matter?

Mr. Robert Gordon: I'm not monitoring their networks so I don't see what all of my members are seeing. What I get is the result of what they are looking at on their network, and when they see anomalies coming in, that's what I actually see. I'm not sitting and watching what's going on inside their network.

The Chair: Thank you.

With that, Mr. Graham, for three minutes, please.

Mr. David de Burgh Graham: Mr. Green, just to put Mr. Dubé's questions to bed, PayPal is in the U.S. I think the point of the question is your private networks might be private networks all you want. If they go through the U.S., they are still subject to the USA PATRIOT Act. I think that's the concern at the core.

How do you address that?

Mr. Ron Green: I still don't know who you are in my network.

Mr. David de Burgh Graham: You said you have a 16-digit number. It's not hard to de-index a 16-digit number. If somebody gets their hands on that number to get to know who you are, if they figured out how to get into your system to get that number, they are going to figure out who you are. So I don't buy that argument necessarily. Do you see my point?

Mr. Ron Green: You're saying if they have some other way to reverse-engineer the 16-digit number...because it would have to be by legal process. I'm not just open to the U.S. government to come in when they choose to, and look at stuff, and I don't share that way.

Mr. David de Burgh Graham: But it's in that cardboard box that John likes to talk about through which your VPN runs. I'm assuming it's a virtual network. You talked about your private network. You're not running your own fibre line across the world so those are virtual networks, right?

Mr. Ron Green: Right.

Mr. David de Burgh Graham: But you're still running over a public access wire.

Mr. Ron Green: I encrypt, though. I don't just run open.... I have the second biggest HSM footprint next to the Department of Defence so I have a lot of cryptology that happens across my network.

Yes, there's still a private network that may go through a third party, but it's still encrypted for me to all of my end points, and the transactions that cross it are encrypted.

Encryption's not trivial. As to whether a nation-state has some way of breaking through the encryption that I'm not aware of could intercept what it is we're doing, that's possible, but not to my knowledge.

Mr. David de Burgh Graham: Mr. Gordon, when I got my first root password about 22 years ago, we followed a thing called rootprompt.org. You might remember it. It was a website that did effectively what you're doing now with CCTX, monitoring all the current vulnerabilities and posting them so we as system admins could stay on top of them. Then one day rootprompt.org got rooted, and there was no more rootprompt.org.

What organizations do you not want in CCTX? What are the vulnerabilities you have? How do you address that?

● (1720)

Mr. Robert Gordon: What organizations do I not want?

Mr. David de Burgh Graham: Yes, because you said you want lots of organizations to join. What organizations do you not want?

Mr. Robert Gordon: I want organizations that do two things. I want organizations that are interested in collaborating, so sharing what's going on, and also honouring the agreement we have, and what they are going to use the information for. I want organizations that are going to use the information to defend their networks.

Somebody who is going to use the information for a purpose other than that—I prefer they go and join something else.

The Chair: Thank you.

[*Translation*]

Mr. Paul-Hus, you have three minutes.

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

Mr. Green, since Mastercard is an international organization, your network is linked to a number of banks in different countries. Are Canadian banks well equipped, compared to European or American banks? You work directly with the banks because you use them for your transactions. Are Canadian banks well organized, compared to banks in other countries?

[*English*]

Mr. Ron Green: I think the Canadian banks are actually in relatively good stead compared to U.S. or European banks. I have seen banks in other places that I'm not so....

[*Translation*]

Mr. Pierre Paul-Hus: Our study concerns the Canadian banking system and the insurance company system. Your company works directly with banks around the world. According to you, Canadian banks are among the well-protected banks in terms of cybersecurity. Is that what you're saying?

[*English*]

Mr. Ron Green: I think they're well protected. There are a number of banks that we converse a lot with. We see it as an opportunity to make sure that we're all working together. I think about wildebeests. When we're together, we're less of a target. If we're alone, we're more of a target. I've had a number of Canadian banks come out—even Canadian Tire—and look at our fusion centre, work with us and build up a collaboration channel.

[*Translation*]

Mr. Pierre Paul-Hus: I have one last quick question.

Mr. Green, does Mastercard have cyber defence strategies to protect itself against attacks from the dark web?

Mr. Finlay, are these topics regularly studied in the university sector?

[*English*]

Mr. Ron Green: We have an intelligence team that looks for threats in the dark web. We pay providers to look at different things within the dark web. We have different government partners that are also looking at things within the dark web to find out how they're attacking and what's different so that we can prevent that. We also share that information with our customers.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

[*English*]

The Chair: Madam Sahota.

Ms. Ruby Sahota: All of this has been very fascinating today but being an MP from Brampton I have a particular interest in Cybersecure Catalyst, which is already partially set up and will be in full swing, thanks to Ryerson. I am happy to see that in budget 2019 there is a commitment made to Cybersecure Catalyst.

I want to know, more particularly, what types of certifications you'll be providing through the training. Are these certifications internationally recognized? Are they comparable to other training programs available anywhere around the world? Also, how many people do you anticipate will reskill or skill up, and how many introductory courses do you plan on being able to complete once you're in full swing?

Mr. Charles Finlay: With respect to certifications, it's our goal to deliver a suite of internationally recognized certifications from established third party cybersecurity training organizations. These are well known in the marketplace. These are entities like SANS, EC-Council and Palo Alto. There are lots of different providers that offer these and we are engaged in developing partnerships quite intensively with SANS and EC-Council to deliver these courses.

This really goes to the posture of Cybersecure Catalyst, which is industry-focused. We are very much interested in supporting the Canadian cybersecurity industry through the partnerships that we've discussed with academia and, obviously, through collaboration with the government. The cybersecurity sector in Canada promises to be one of the best in the world, and it can be one of the best in the world. We're going to work extremely hard to support that. We are aiming for those kinds of industry-focused certifications.

In terms of numbers, we have a five-year model out with respect to the introductory courses, that is, bringing demographic groups that are under-represented in cyber into the sector. We're looking at approximately 500. In terms of the work that we're going to be doing with our private sector partners, that will be in the thousands. In terms of engagement with young people, that will be, we hope, in the tens of thousands. Cybersecurity is a big problem and the numbers that we need to reach in order to have a material impact on this issue are large.

That's the ambition for this centre.

● (1725)

Ms. Ruby Sahota: Thank you.

The Chair: Colleagues, I have four minutes, and then we do have to vacate because there's a subcommittee meeting here.

Being the nice guy that I am to Mr. Motz, in spite of his ageism cracks, the time is split between Mr. Picard and Mr. Motz.

You have two minutes each.

Mr. Picard.

Mr. Michel Picard: I have just one question.

Mr. Davies and Mr. Green, what is your understanding of open banking and what is your position from a securities standpoint?

Mr. Ron Green: Open banking will provide a lot of great new opportunities but we have to approach it in a way that security is enabled with the new technology that comes from; the new providers that we'll see. I think the government can help with making sure they're holding to a good standard as they deploy their capabilities.

The Chair: Mr. Motz, you have the final question.

Mr. Glen Motz: I'm going to continue with that.

Michel, thank you, that was a great question.

I wanted Mr. Davies to answer.

The Chair: Oh, sorry. Did I cut somebody off? I apologize.

Mr. Thomas Davies: No, it's all right.

I know the Department of Finance is working on a special paper right now on open banking both from a deployment regulation and a security standpoint. As Mr. Green said, to embed security from the outset will be important. The U.K. has already done quite a bit of open banking so it would behoove us to look at what they've done today and the lessons learned.

The Chair: On behalf of the committee I want to thank each of you for an excellent presentation. It was very informative.

What that, the meeting is adjourned.