HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 157 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, April 10, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, April 10, 2019

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): It's 3:30 and we have quorum.

We have two witnesses for our first panel, Mr. Ryland and Mr. Fadden.

Before I start, colleagues, we've had a couple of curves thrown at our agenda going forward and we need to give the clerks and the analyst some instructions. The meeting of the subcommittee was scheduled to start at 5:30. However, bells may ring at 5:30, in which case I would not be able to start the subcommittee meeting.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Start at 5:29.

The Chair: You're running a little tight at 5:29. I was thinking more like 5:20. We may end the current meeting at 5:20, or we can stretch it a bit to 5:25.

Unless there are other considerations, I'll call upon our witnesses to speak, in no particular order, although I take note that Mr. Fadden has spoken at this committee many times, and Mr. Ryland, I believe this is your first opportunity.

Mr. Mark Ryland (Director, Office of the Chief Information Officer, Amazon Web Services, Inc.): That's correct, yes.

The Chair: Maybe I should let the pro go first and then you'll see how an excellent witness can make a presentation.

Mr. Mark Ryland: That sounds good.

The Chair: Mr. Fadden, please.

Mr. Richard Fadden (As an Individual): Thank you, Chairman. I'll hold you to that assessment when I'm finished.

The Chair: Don't put it to a vote.

Mr. Richard Fadden: Thank you again for the opportunity to speak to you.

As I start, I want to note that in discussions with the clerk and the staff of the committee, I told them that I wasn't an expert on the financial sector, and it was suggested to me that I could make some general comments on national security and cyber, so that's what I'm proposing to do. I hope that will be helpful to the committee.

I want to comment in an odd sort of way on your order of reference, which talks about national economic security. I'm sure that careful thought was given to that, but I'd like to suggest to you—and I'm doing a bit of marketing here—that the issues you're talking about are national security issues, period. They're not a subunit of national security.

This goes to the definition of national security. I hope and think that you use a fairly broad one, but to my mind, it's anything that materially affects a nation's sovereignty. The things that the committee is talking about now can potentially very much affect a nation's sovereignty, just like money laundering conducted by a foreign state, or a devastating national security issue. That's just a small marketing effort on my part.

While I'm not an expert in financial systems, I hope and think that I can offer you a couple of useful context points. One is that context in the environment in which cyber-attacks occur, be they against the financial institutions or anywhere else, is important. These things don't occur in isolation. I would argue that you cannot deal with cyber-threats in the financial sector without an understanding of cyber-threats generally, and you can't understand cyber-threats without understanding threats generally directed against Canada and the west. We all live in a globalized world, and that certainly applies to national security threats.

I say this for a couple of reasons. Some of you may be old enough to remember the Cold War where it was fairly simple: those who were causing trouble and those who were receiving trouble were basically states. I'm oversimplifying, but it was the Warsaw Pact against the west. Some companies were affected.

I think one of the contextual points that are important is that our adversaries or instigators today are states, terrorist groups, criminal organizations—and I'll come back to that—corporations, civil society groups and individuals. I think that any of these could be causing difficulties in the financial systems that you're concerned about.

The targets, on the other hand, used to be basically states. I'd argue that they're now states, corporations, civil society, political parties, non-profits and individuals. The world is fairly complicated, and if either the financial institutions themselves or the government is going to deal with cyber-attacks against them, my suggestion to you is that they have to know and understand the context in which all of that is occurring. They just can't build walls abstractly.

I think the question of who or what might initiate cyber-attacks against our financial sector is very relevant. I don't try very hard to do sound bites, but I have one: National security is not national. It's not national in the sense that no single state can deal with these issues— certainly not a relatively small middle power like Canada—and you need international co-operation.

Second, I would argue that no federal state or nation state can deal with these sorts of things without the help of provincial or regional governments, and corporations and society generally. I would argue with you that it is a significant mistake for financial institutions to argue that they can do it all themselves, just as it is a mistake for the government to accept that hypothesis.

I talked a little bit about context and environment, so I would just like to lay out very quickly the kinds of threats to national security that Canada's facing. I think of the revisionist states, Russia and China; extremisms and extremism generally, including terrorists; the issue of cyber; the dysfunctional west; and the rogue states and issues—Iran and North Korea, come to mind.

I'm emphasizing this a little bit because I think all of these are interrelated far more than they might have been 15 or 20 years ago. They leverage against each other, and they amplify their effects. For example, Russian and China use cyber systems and benefit from a dysfunctional west because we're not fighting them together. Terrorist groups benefit from the discord caused by revisionist states, and they use cyber systems. All of them interact with one another, and I think that we need to keep that in mind when we do that.

● (1535)

One of the other issues I want to emphasize and suggest to you is that Canada is very much threatened by cyber-attacks generally and against our financial institutions. I say this, because when I used to be working, one of the things that used to drive me to distraction was the view of many Canadians that Canada wasn't threatened because we had three oceans and the United States. That view made it very difficult for governments and others to deal with a lot of national security threats. The average Canadian, absent an event, didn't think there was a great issue.

I think Canada is very much threatened by a variety of the institutions and entities that I just talked about, but why is this the case? We have an advanced economy, advanced science and technology; we're part of the Five Eyes and NATO, and we're next to the U.S.

To be honest, we're not thought internationally to have the strongest defences on the cyber side, and any institution will go to the weakest link in the chain. Sometimes we are thought to be that, although I don't think we're doing all that badly. Also, we're threatened, sometimes simply because we're hit at random.

I think it's especially important for the committee to make the point that our financial sector is indeed threatened by cyber-attacks, because I don't think a lot of people believe that.

One of the other things I'd like to talk about is who I think are the main instigators of potential attacks. I think they're nation states and international criminal groups.

What are they going to try to do? They're going to try to deny service, old-fashioned theft—and I'll come back to that—information and intelligence acquisition, intellectual property theft, and identification theft, for both the purposes of acquiring money and espionage.

Let me give you a couple of examples about states that play with countries' financial systems.

North Korea finances a lot of their operations, gets a lot of their hard currency by using their cyber-capabilities to access the financial systems of various and sundry countries. For example, they had a program some time ago that allowed them to steal money systematically from ATMs around the world. They also had a program that allowed them to claim ransoms using ransomware. More generally, they are the country that was thought to have frozen the United Kingdom's national health service a few years ago.

My point is that you can find out as much about this as I can just by Googling them. The United States has indicted a number of people from North Korea who have tried to do this, and this is just one example of a state that tries to get into western countries' financial systems.

Another one is Iran. You will have seen in the newspapers over the last five or ten years, a couple of examples of how Iran has tried to do this, in particular against the United States and banks. There are indictments against seven or eight Iranians.

I have a couple of words about Russia and China and how I don't think you cannot ignore them when you talk about this topic. I think their main objective is twofold: one is denial of service, and another is to simply reduce western confidence in our institutions. They do this systematically.

Criminal groups I think are becoming much more prominent in this area, and it's something we don't talk enough about. I hope you've had an opportunity to talk to the RCMP about this. If you look at either RCMP or Statistics Canada figures, the extent to which international criminal groups are playing with our financial institutions has gone through the roof over the last little while.

In summary, cyber-attacks on our financial system are a national security issue in my view. These attacks must be viewed in broad context if we're going to deal with them effectively. There's no silver bullet to any of this. It will only work, and we will only reduce the risk, if governments, corporations and civil society co-operate.

I think government needs to share more information with the private sector. It's something that we do far less of than the United Kingdom and United States. You can't expect private corporations to be an effective partner if they're not aware of what's going on.

The financial sector needs to report these attacks and breaches far more systematically than they do.

These issues are evergreen, and we need to talk about them more than we do.

Thank you, Chairman.

● (1540)

The Chair: Thank you, Mr. Fadden.

Mr. Ryland, you have 10 minutes, please.

Mr. Mark Ryland: Good afternoon, Chairman and members of the committee. My name is Mark Ryland. I'm the director of security engineering with Amazon Web Services. I work in the office of the CISO, so I work directly for the chief information security officer. Thank you for giving us the opportunity to speak with you today.

I suspect you all know a bit about Amazon.com, generally speaking, but allow me to add some Canadian details.

Amazon.ca has been serving our Canadian customers since 2002, and we have maintained a physical presence in the country since 2010. Amazon now employs more than 10,000 full-time employees in Canada, and in 2018 we announced an additional 6,300 jobs. We have two tech hubs, which are important software development centres with multiple office sites in Vancouver and Toronto. We employ hundreds of software designers and engineers who are working on some of our most advanced projects for our global platforms. We also have offices in Victoria with AbeBooks.com and in Winnipeg with a division called Thinkbox.

We also operate seven fulfillment centres in Canada—four in the greater Toronto area, two in the Vancouver area, and one in Calgary. Four more have been announced. Those will be coming online in 2019 in Edmonton and Ottawa.

But why am I here? What is this cloud thing? You might be wondering why we're here discussing the cybersecurity of the financial sector at all. Well, roll back the clock. About 12 years ago, we launched a division of our company we call Amazon Web Services, or AWS for short.

AWS started when the company realized that we had developed our core competency in operating very large-scale technology infrastructure and data centres. With that competency, we embarked on a broader mission of taking that technological understanding and serving an entirely new customer segment—developers and businesses—with an information technology service they can use to build their own very sophisticated, scalable applications.

The term “cloud computing” refers to the on-demand delivery of IT resources over the Internet or over private networks, with pay-as-you-go pricing, so that you pay only for what you use. Instead of buying, owning and maintaining a lot of technology equipment, such as computers, storage, networks, databases and so forth, you simply call an API and get access to these services on an on-demand basis. Sometimes it's called “utility computing”. It's similar to how a consumers flip on a light switch and access electricity in their homes. The power company sort of takes care of all the background.

All this infrastructure is created and built. There is of course physical equipment and infrastructure behind all of this, but from the user perspective, you simply call an API. You call a software interface or click a button with a mouse, get access to all this capability and are then charged for its usage.

It's all fully controlled by software, which means that it's all automatable. That's a really important point that I'll make several times, because the ability to automate things is a big advantage in the security realm. Instead of doing things manually and using.... We don't have enough experts, believe me, to do all the command typing that needs to be done, so you need the right software to automate.

As of today, we provide highly reliable, secure, resilient services to over a million customers in 190 countries. Actually, you can think of our cloud platform as a federation of separate cloud regions. There are 20 of those around the world and 61 availability zones. Each region is made up of separate physical locations to create greater resiliency.

Montreal is home to our AWS Canada region, which has two availability zones. Each availability zone is in one or more distinct geographic areas and is designed with redundancy, for power, for networking, for connectivity and so forth, to minimize the chance they could both fail. With this capability, with these multiple physical locations, our customers can build highly available and very fault-tolerant applications. Even the failure of an entire data centre need not result in an outage for our customers and their applications.

The companies that leverage AWS range from large enterprises such as Porter Airlines, the National Bank of Canada, the Montréal Exchange, TMX Group, Capital One and BlackBerry, to lots of start-ups, such as Airbnb and Pinterest, as well as companies like Netflix, which many of you have heard of, all of which are running on the AWS cloud.

We also work a lot with public sector organizations around the globe, including the Government of Ontario, the Ministry of Justice and the Home Office in the U.K., Singapore, Australia, the U.S.A. and many customers globally in the public sector area.

What are the advantages of moving to the cloud? There are three primary benefits that I want to highlight.

The first is agility and elasticity. Agility allows you to quickly spin up resources, use them, and shut them down when you don't need them. This really means that for the first time, customers can treat information technology in a more experimental fashion because experiments are cheap. You can actually try things, and if they don't work, you spend very little money. Instead of this large capital expenditure with large software licensing costs, you can do this in a much more dynamic model. Experimentation is very helpful when it comes to innovation, so that leads to greater innovation.

● (1545)

In terms of elasticity, customers often had to over-provision for their systems. They had to buy too much capacity, because only once a year or once a month was there a need for a great deal of capacity.

Most of the time, the systems are relatively idle. You have a lot of waste in this over-provisioning model. In the cloud, you can provision what you need. You can scale up and add more capacity or subtract capacity dynamically as you go.

Another advantage is cost savings. Part of what I just described also leads to cost savings. You're using only the amount of capacity you need at any one time. You can also treat your expenditures in terms of moving from capital expenses to operational expenses, which many people find very helpful.

In short, our customers are able to maintain very high levels of infrastructure at a price that is very difficult to do when you buy and manage all your own infrastructure.

The third reason, and the one that I really want to emphasize here in my testimony, is actually the benefit of security. The AWS infrastructure puts very strong safeguards in place to protect customer security and privacy. All the data is stored in highly secured data centres. We provide full encryption very easily; you just literally check a box or call an API. All your data is encrypted, which acts as controls in logging, to see what's going on and to monitor and control who has access. Also, our global network provides built-in inherent capabilities for protecting customers from DDoS and other network-type attacks.

Before the cloud, organizations had to spend a lot of time and money managing their own data centres and worrying about all the security of everything inside, and that meant time not focused specifically on their core mission. With the cloud, organizations can function more like start-ups, moving at the speed of ideas, without upfront costs and the worry of defending the full range of security threats.

Previously, organizations had to either adopt this big capital investment program or enter into long-term contracts with vendors. Really, the most difficult part was that the companies and organizations were responsible for the entire stack. Everything from the concrete to the locks on the doors and all the way to the software was completely the responsibility of the customer. With cloud, we take care of a number of those responsibilities.

What about cloud security? More and more, organizations are realizing that there's a link between IT modernization and using the cloud and improving their security posture. Security depends on the ability to stay a step ahead of rapidly and continuously evolving threat landscapes and requires both operational agility and access to the latest technologies. As the legacy infrastructure that many of our customers use approaches obsolescence or needs replacing, organizations move to the cloud to take advantage of our advanced capabilities.

Increased automation is key, as I mentioned before, and the cloud provides the highest level of automation. The possibility of automation is maximized using the cloud platform. Cloud security is our number one priority. In fact, we say that security is job zero, even before job one, and organizations across all sectors will highlight how commercial cloud can offer improved security across their IT infrastructure.

Therefore, many organizations, such as financial institutions, are modernizing their capabilities to use cloud platforms. We've been architected for the security of organizations, and for some of the most security-sensitive organizations, such as financial services.

Now, there is a shared responsibility. Customers are still responsible for maintaining the security of their environments, but the surface area, the amount of things they need to worry about, is greatly reduced, because we take care of a lot of those things and they can focus their attention on what remains. From major banks to federal governments, customers have repeatedly told us—and we have quotes that we can supply to the committee—that they feel more secure in their cloud-based deployments of their applications than they do in their on-premise physical infrastructure in their own data centres.

In sum, cloud should not be seen as a barrier to security, but as a technology that helps security and is therefore very helpful in the financial services realm as a part of a general solution for modernization and improving security.

We also have a few policy recommendations, which we'll provide in our written testimony.

One of the things is that we think there's an overemphasis on the physical location of data. Very often, people think, “I've got to have data physically here in order to protect it.” Actually, if you look at the history of cyber-incidents, everything is done remotely. If you're connected to a network and the network has outside access, that's where all the bad things happen.

Physical location of data, especially when you can encrypt everything, such as physical access to storage drives or whatever, literally is not a threat vector. Really, there should be some flexibility for banks and other institutions as to where they physically place their data, and they should be able to run their workloads around the globe, reaching their global customers with low latency and storing data potentially outside of Canada.

There are another couple of recommendations, including data residency. We believe also that centralizing security assessment makes a lot of sense. Instead of having every agency or every regulatory body separately evaluating cloud security, centralize that in an organization like the CCCS, where they can do a central evaluation and determine whether clouds are meeting the requirements. Then, that authority to operate can be inherited by other organizations throughout the government and under industries that are regulated.

● (1550)

Thank you very much for your time.

The Chair: Thank you, Mr. Ryland.

The first seven minutes go to Mr. Spengemann, please.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you very much, gentlemen, for being with us.

Mr. Fadden, it's particularly good to have you here. In terms of your former role as national security adviser, I think you have a unique perspective on how this connects to the Department of National Defence and questions of national defence. I want to start by asking you about that.

Where are the intersections, the grey zones, between what we look at as Public Safety questions and National Defence questions? These two committees have their own mandates. In that way, we're stovepiped, and perhaps there should be a joint study between the two of them.

Can you make some general comments on how much of the national defence component plays a role in good cybersecurity and how much lies on the public safety side?

Mr. Richard Fadden: Well, I tend to agree with you that drawing distinctions in this area is a little bit artificial and that one of the things that should be avoided to the extent possible is the development of these silos. We have quite enough of them as we are, and we don't need any more.

I think National Defence's main contribution is through the Communications Security Establishment and, insofar as the private sector is concerned, the Centre for Cyber Security. They tend to operate quite co-operatively with other parts of the national security environment in Canada. I would argue, in part on the basis of what I knew when I was working, but in part because I now operate a little bit in the private sector, that they certainly were a welcome development, but they have not solved all the problems of cyber-attacks here or anywhere else.

I think one of the big problems they have, and this is a Defence issue, in the sense that the defence minister is responsible, is that we talk about these things, but we talk about them less and share far less with the private sector than a variety of other countries do. I don't blame any particular government or any particular official. There's something in the Canadian DNA in that we think that national security should be dealt with and not talked about, but I would argue that in many cases we're far better off if we talk about them a little bit, without going into operational detail. It raises awareness. It allows both government and corporations to talk and to share more information than is otherwise the request, but I think the main contributor is CSE.

● (1555)

Mr. Sven Spengemann: I had the opportunity to ask the last panel about the distinction, if there is one, between state actors and non-state actors qualitatively in terms of their capacity to execute a threat. Can you comment on that? Does a state actor simply have more capacity, more hackers and more people? Or are there other qualitative differences that really put that type of actor into a different category altogether?

Mr. Richard Fadden: I think there are state actors and state actors. I think China and Russia are at the top of the league. They spend almost unlimited resources on their cyber-capabilities. They're very, very good at it. I think it's generally accepted that China uses the vacuum cleaner approach. They'll grab just about anything they can. The Russians, I think, are somewhat better technologically and more surgical in what they seek to acquire.

I think international criminal groups are not at that level, but they're getting to be very, very good. It's a very smart collection of people there, who have figured out that it's easier to enrich themselves using cyber devices than using kinetic action of some form or other. Also, there are no borders, and to the extent that there are no borders, it's far easier.

I guess the last group I would mention is terrorist groups. They're in a different category. Some of them have a limited cyber-capability. It's not really worldwide.

I guess the point I would make again is that the state actors in particular make it important that we regard cyber-defences as evergreen. I'm not talking in particular about Mr. Ryland's company, but for any protective measures that we put in place, if we have a really aggressive actor and we give them enough time and technology, they'll find a way around them. My point is, we need to constantly renew our defensive measures. We need to constantly advance our technology, mostly against nation-states, but increasingly against international criminal groups.

Mr. Sven Spengemann: I want to ask you a question about content in the digital domain, both on the civilian side and on the military side. Facebook just came out with the decision to ban a number of entities, individuals that are not meeting their standards, including Faith Goldy, who is a white nationalist and Canadian. We've also had discussions in the defence committee about Russian disinformation campaigns and deliberate false content in the social realm.

How much of an issue is content? Where do you see the trends going? Is there a trend towards, quote, unquote, “banning” content? If so, what happens? Do we push that kind of content into the dark web or are we solving some problems?

Mr. Richard Fadden: I think content is appalling, disgusting and unrealistically terrible. If you sit down some Saturday afternoon or on a rainy Sunday and, with a bit of imagination, start going through the web, you will find right-wing stuff that is as bad as the Nazis, and you will find jihadist literature that advocates the systematic killing of people. That's not talking about the dark web, which is another problem again. I think content is a real issue.

I would argue that what Facebook is trying to do is a good first step, but I really don't want Facebook to become my thought controller. On the other hand, I worry rather the same way about governments. I don't want governments to become my thought controllers by determining what happens. I think we need a bit of a national discussion on who does this.

One way that Parliament has dealt with this issue is in the area of money laundering. You may recall there was a debate years ago about how to deal with money laundering: Were we just going to make it a crime? What Parliament basically did is that they imposed an obligation on banks to know their clients. That has significantly improved the capability of everybody to deal with money laundering. It hasn't eliminated it, but it has helped it.

I think there is something to be said for government setting up a framework, either statutory or regulatory, which requires companies that play in this broad area to know whom they're allowing to access the web and then to direct them as to what they can and can't do.

Because of my old age and after 40 years in government, I've become a bit wary about being told what to think, but whether it's government or the private sector, I think there needs to be a measure of transparency so that we know both what is being done and what is not being done.

But none of this is going to work, I think, if the average Canadian isn't more aware of what's available and that average Canadian has some means of registering his or her displeasure. Right now, yes, you can call the Mounties, but they have so much to worry about that it's pretty low in their priorities.

Mr. Sven Spengemann: Thanks very much. That's very helpful.

The Chair: Thank you, Mr. Spengemann.

[*Translation*]

Mr. Paul-Hus, you have seven minutes, please.

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

Good afternoon, gentlemen.

Mr. Fadden, in 2010, you gave an interview on CBC that was reported in the Globe and Mail. You said that there was interference from foreign governments against officials in provincial ministries and in areas of Canadian politics. At that time, people from the NDP and the Liberal Party demanded your resignation. Fortunately, you remained in office.

This morning, we learned that the report of the National Security and Intelligence Committee of Parliamentarians, which has just been tabled, confirms what you said and very clearly confirms that China is a danger for Canada’s security.

In your presentation, you talked about problems, but I would also like to know about potential solutions. You talked about the “dysfunctional West”, if I heard the interpretation correctly. Could you shed some more light on what we could do? What does that mean?

● (1600)

[*English*]

Mr. Richard Fadden: Yes. When I talk about the dysfunctional west, I mean that.... I'm sure you don't want to get into a large discussion about the current U.S. administration, but they are a significant issue right now in the sense that the views of the current U.S. President are promoting massive instability. People are uncertain as to what's going on. The United Kingdom hasn't taken a major decision in a year and a half. Monsieur Macron is concerned about what's going on with *les gilets jaunes*. Germany is preoccupied with replacing Mrs. Merkel, and God knows what the Italians are doing.

My point is that while we're worrying about these major issues, we're giving an opportunity for Russia and China in particular to poke and prod in a way that they could not do if we were a little bit more together. I'm not suggesting the world's coming to an end. I really am not, but I think our adversaries—and I call them adversaries, not enemies—are very active. They take advantage of every opportunity. I think we need to start rebuilding those close ties that we've had amongst some countries since World War II.

I also think we need to realize more than we do—it's one of the pathways that I think we need to talk about—and appreciate that Russia and China are, in their own way, great countries. They've made great contributions to civilization. But right now they are fundamentally unhappy with their position on this planet and they're trying to change it, using virtually any method. I don't think we think about this very much. If we don't think about it and try to do something about it, we're really behind the eight ball.

I think the first thing is to develop a greater understanding of what's happening. Somebody asked me the other day in the media why Russia went to Syria. There's no prospect of territorial acquisition, except that they are trying to cause trouble, and they have effectively succeeded. They delayed the elimination of the caliphate. They're doing this in a whole raft of areas. They played with the elections in the United States, Germany, France, and I believe Italy. All they're trying to do is not really shift who's going to win; they're trying to diminish public confidence in public institutions.

All of this, I think, needs to be talked about more. We need to get a grip amongst particularly core western countries, about how serious the problem is. Parts of the U.S. administration consider this more important that we do sometimes. The Brits are at another level. We need a consensus in the west that we have a problem. The U.S. has just shifted their national security priorities to great power conflict, after being on terrorism for the last many years. Well, if that's the case, we need to think about what we're going to do about Russia and China, without going to war, which is not what I'm advocating. We need to be talking about it, understanding the nature of the threat and developing closer ties internationally. I do firmly believe that national security is not national, not in the way it's run today; we need to work with everybody.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

Let us go back to our basic topic, the financial sector, the banks.

We have met with a number of interested parties, various banks and various other groups. We have the banks, the government's administration system, and the political side. In terms of security, issues, potential enemies, the political side is always hesitant. The banks take their own measures.

In your opinion, is the administration, the people we do not see, the people in the shadows, currently effective enough to make up for the political side? It can be on one side or the other; I am talking generally. Sometimes, politically, we don't dare.

After the years you have spent in the political apparatus, do you feel that we are effective or that we need to be taking very vigorous measures?

[*English*]

Mr. Richard Fadden: I should admit up front that I'm probably prejudiced, having spent a goodly number of years working in this area, but I think there has been a lot of progress over the last little while and there's much more co-operation and collaboration.

But I would argue two things. One is that the world is becoming much, much more complex, and I think it could be argued that we need more resourcing. When I used to work for the government, the last thing you wanted to do was embarrass your minister by saying you wanted more money. I'm not really saying that now, but if you consider the Cold War to terrorism and the current cyber issues and great power conflict generally, yes, all of these institutions have had more resources, but the resources may not be enough today, so I would ask that.

I guess the other issue I would note is this. I was told over the years by several politicians from both sides that there aren't very many votes on national security, and that's one of the reasons why governments are sometimes hesitant to take some of the steps you've implied. However much politicians may get frustrated with officials, officials do take the lead from the political side of things, and I think we need to be a little bit more proactive sometimes than we are, because technology is moving, the threat is moving, and we seem to be playing catch-up.

I don't direct this at any government or any official. It just seems to be the way we do it, largely because, if you're the Minister of Finance or the President of the Treasury Board, the last thing you want to do is to say every two years, "Here's another quarter of a billion dollars." I'm just picking a number, but you know, there are technological changes, some of which Mr. Ryland talked about, and there are a whole raft of others. It's very hard for government to keep up with these things without a constant ongoing effort, and at the same time, you're worrying about Russia and China and North Korea and Iran. You're worrying about international criminal groups. I think we're beginning to underestimate the problem with terrorists just because we've whacked a few of them.

So, as a long answer to a short question, I think generally speaking people are doing as well as they can, but it's very difficult to galvanize everybody who works on this—political officials and the private sector—unless there's some consensus on how serious the threat is.

I would say, with great respect, there's no such consensus in Canada.

● (1605)

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

Mr. Dubé, go ahead for seven minutes, please.

[*Translation*]

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

Thank you for being here today, gentlemen.

Mr. Ryland, my first question is for you. In terms of your services, I am not sure whether you are in a position to explain to us how the responsibilities between you and your clients are separated.

What role do your clients play in ensuring the security of the data they store on your servers when they use your services?

[*English*]

Mr. Mark Ryland: It can be a very long and nuanced conversation, but just to give a kind of summary, if you look at something like what they have in the United States, there's a security control framework based on a NIST standard called FedRAMP that lists something like 250 controls—in other words, the security properties that you want in a system—and if you take that whole security framework, our platform covers more than one-third of those controls. There are simply things that we literally take care of on behalf of our customers. They don't have to worry about them at all. Roughly one-third are shared in that we take care of some of the things but the customer has to do certain configurations and make certain choices that are correct for their requirements. Those are optional because it's reasonable to do either one, but depending on what their needs are, they have to choose. Then roughly one-third are pretty much all the responsibility of the customer.

So we have decreased the scope of concern for the customer. We delineate pretty clearly, and we literally have control documents that say who's responsible for what, and then we have a lot of material—white papers, best practices documents, and what we call a "well-architected framework"—to help people with that one remaining responsibility. We want them to be very successful at that, so we put a lot of effort into helping them design secure systems.

But when you get to that level, it all depends on the needs of the application, so there's not a correct answer to some question. It's going to be "it depends". It depends on the application. It depends on the requirement.

In general, I think that's a good summary of the kind of model we use with our customers. We take care of a number of things that they normally would worry about; we describe some areas in which we do some things and they need to do others, and then we help them be successful in the remaining parts of building a secure system with lots of tools and features that make it easy to do the remainder.

[*Translation*]

Mr. Matthew Dubé: Thank you.

I want to make sure I fully understand. You said that about one third of the responsibility to configure everything appropriately lies with your clients. Does that create a barrier for people, and especially companies that might wish to use your services, by which I mean that the expertise must already exist in the company or the government agency?

Let me explain. Here is the example that comes to mind. I believe that Shared Services Canada has a contract with you. However, according to what we have been seeing in the news for some time, that organization has a quite dismal record in terms of implementing information systems.

Could the potential shortcomings or lack of expertise in a company or government agency limit the ability of a client to do business with you or with any other company comparable to yours?

● (1610)

[*English*]

Mr. Mark Ryland: It's certainly possible, in using any technology, to not use it properly. We see a big part of our mission as education and training of our customers, and we do a lot of that. A lot of it's actually free as part of the process of helping them to understand this kind of new paradigm of cloud computing.

That said, there's a lot of commonality with things they've already been doing for a long time. I'll just make up an example. Say, you're running a citizen-facing web application for a government. You already have some kind of understanding of how to secure a web system; you have an authentication system, password reset, those kinds of properties that are built into the system. If you use that similar kind of system on a cloud platform, the security properties of that would be similar to the one you've been doing historically.

It's not a completely new world. It's not a 100% new skill set that is required for security professionals, but there are definitely differences and changes. It's part of the progress of the industry, just like 20 or 30 years ago when we spent a lot of time on mainframe security. Now that's not something people focus on. There are still mainframe systems running, and they still need to be secure, but the focus tends to be on the new things, the new systems and new applications.

I think the transition to cloud computing has a similar property. In any type of modernization and use of new technology there's definitely some learning curve, but you can also get a lot more done with less labour, with fewer actual human beings. Sometimes when automation comes up it's considered controversial because, well, what if we remove people? Will we be taking away jobs from workers? In the cybersecurity area, everyone recognizes we have a huge labour shortage of skilled labourers in this area. Any type of technology that increases automation and enables a skilled worker to come up with a solution and then replicate that broadly is a big win, so everyone can get behind greater automation in the security realm.

I think that's one of the main reasons that people find the cloud platforms to be advantageous. Yes, there's a learning curve, but the ability to automate things is really quite dramatically better than using traditional technology.

[*Translation*]

Mr. Matthew Dubé: I have two quick final questions.

Here is the first one. Perhaps you are not in the best position in your organization to answer it. However, say there was a leak of data, given the shared responsibility, who would ultimately be responsible for the data in legal terms? In the financial sector specifically, if a client were to lose money, would the fault lie with the bank or with the company that allows them to store data in the cloud?

How do you see that?

[*English*]

The Chair: Be very quick, please.

Mr. Mark Ryland: Yes.

The shared responsibility also includes the line between who takes that responsibility. If there were a problem in one of our systems, we would be responsible for that. If a customer misconfigures or misuses one of our systems, then they are responsible for that.

Again, we do a lot to support customers and we have many cases in the security team that I work in where customers have an issue and some kind of incident, and they ask for our help. Although technically we're not at fault at all, we still are very aggressive in responding to help them get out of the problems that they've caused.

I'll take a simple, non-controversial example. We have systems where customers have accidentally deleted data without having proper backups, and come to us in a panic. At one level, we could say, “Well, the system was working just the way it was described. You made a mistake. There's nothing we can do”. But we will go to great lengths to help them try to figure out solutions to those kinds of problems, and similarly with security incidents.

● (1615)

The Chair: Thank you Mr. Dubé. I'm sorry about that.

Mr. Graham, you have seven minutes, please.

Mr. David de Burgh Graham: Thank you.

I'd love to continue on that line, but I'll come back to that in a second.

Mr. Fadden, I don't think anybody will disagree with your assessment that our study is really about national security as opposed to financial cybersecurity as the pigeonhole..

I would say that there are a lot of votes in national security, but only after an incident has happened.

Mr. Richard Fadden: Point taken. I appreciate it.

Mr. David de Burgh Graham: You said that national security is not national; it's supernational. Does Canada have a network backbone strong enough to handle Canadian needs? Do we have enough intercontinental connections to handle Canadian needs, and does it matter?

Mr. Richard Fadden: I think it matters a great deal.

Do we have the backbone or the intercontinental connections? I find it difficult to answer that question, because I think it's an answer that requires two parts: one dealing with governments generally, and one dealing with the non-governmental sector.

I think that insofar as governments are concerned, we have very close alliances with the Five Eyes—the United States in particular—and there's an immense sharing of information. I would argue that it's pretty effective, notwithstanding the dysfunction I was talking about.

When I was still working, the approach taken to deal with some of these issues.... It's a bit like talking about cancer. That's not particularly helpful. I notice that some of you have your cancer pins on. Talking generally about cancer is not particularly helpful, because the cure for cancers goes to the 130-odd kinds of cancer. I find that talking generally about cyber is not often very helpful. You have to break it down into its component parts.

We used to divide up the Canadian economy into strategic sectors, such as telecoms, financial, nuclear.... There were 11 or 12 of them. Quite honestly, I think the connections they have with their home offices—with each other in Canada and abroad—vary. For example, our nuclear sector is pretty well organized, and I think the general view, as sectors go, is that financial sector is not doing badly. Some of the others are less so.

I'm not trying to avoid answering your question, but I think it's difficult to just give you a yea or a nay. I think there's no one entity —government or non-governmental—that's responsible. It's just as things have evolved.

Mr. David de Burgh Graham: I'll come to Mr. Ryland for a bit more.

You talked about the over-provisioning model. You were talking about the the vast resources and being able to balance them across systems, which we couldn't have before. As an example, what's the computing power of a key fob today versus that of the Apollo?

Mr. Mark Ryland: There's more power in the key fob, probably. It's a 32-bit microcontroller.

Mr. David de Burgh Graham: When we have that kind of massive change in computing capacity, what's the security impact of that change? Is the technology changing faster than we're able to keep up with it?

Mr. Mark Ryland: No, I don't think so.

Technology changes rapidly, but there are people driving those technological changes. In general, experts who build the systems understand how they work and how to secure them. There may be a lag time in terms of broad understanding of those cutting-edge technologies, but often those experts are also designing things to make them more secure by default.

I think IoT is a great example. We don't have time to go into the details, but we've all recognized the problems in the past with the Internet of things—home devices, etc.—being deployed in a very insecure fashion. Historically, it was the cheapest and easiest thing to do. If you look at the newer technology that we provide, or that Microsoft or other large-scale providers give you, by default their systems are far more secure. They're updatable in place, which they didn't use to be. They use secure protocols by default; they didn't use to do that. You can go right down the list of how the business interests of these large providers align with building systems that are secure by default, whereas previously, that was left to the person who was building the smart refrigerator or the smart toaster or whatever.

Technological shifts can actually raise the bar across whole industries by investment and by alignment of business interests with higher security.

Mr. David de Burgh Graham: I'll go back to clouds. Does the public or even the organizations you deal with truly understand what a cloud is?

Mr. Mark Ryland: There's often a lot of confusion. First, there's this idea, what is out there? People think that there must be something out there. There's also the confusion between consumer-use cases. People think Facebook and Google are like a cloud, but provisioning IT services from a cloud-computing vendor is a completely different model. First of all, we don't monetize your data; we lock it down and never look at it. We have a totally different way of thinking about it.

The one thing they typically have in common is network accessibility. It would be able to reach them from anywhere.

There's a lot of confusion. Often when we start our presentations, we'll put up a world map. We actually have little dots on the map showing where our stuff is in that city or that region, so that people know there's physical equipment behind all of this capability.

● (1620)

Mr. David de Burgh Graham: Is AWS essentially virtual servers, or is there another system besides that? Are they virtual machines?

Mr. Mark Ryland: That's one of our core services. It's called EC2, but we literally have a hundred other services. The trend is away from using virtual machine services, because that's where the customer has to take the most responsibility. People would prefer the higher level services where we take increased responsibility and they just have to do very minimal configuration.

Mr. David de Burgh Graham: If you're not on a virtual machine and you're using the services provided, how much control can the client actually have? There's a balance to be had. As a client, could I choose what operating system to put on my virtual machine? I could put a Debian system on there, or whatever you want, but what could you put on a non-virtual machine? What are the other options?

Mr. Mark Ryland: Again, it depends on the use case. You don't care what the compute model is for a storage service, as you're just storing data. Databases are in the middle. There are a range of choices and options, but people do tend to prefer what are called "abstract services". Over time, you'll see more and more use of what those abstract services. I just upload my JavaScript function to this function as a service and the code executes whenever certain events fire. I have no concept of the operating system or anything else; it's handled for me.

Mr. David de Burgh Graham: I only have about 40 seconds left, so my last question for both of you is about the security advantages versus disadvantages of open versus closed-source software.

Mr. Mark Ryland: There's something called the "many eyes" hypothesis for open-source software. The fact that people can see the code makes it more likely that security and other flaws will be discovered. I'm not sure there's a really strong empirical backing for that, because lots of security flaws have existed in open code, but there is the big advantage that people have more control over their own destiny because you can do your own investigation. You can make your fixes. You're not dependent on a vendor to discover and fix security problems. On the whole, there are some real advantages to open-source software, but it's not completely black and white.

Mr. David de Burgh Graham: Thank you.

The Chair: Thank you, Mr. Graham.

Mr. Richard Fadden: Chairman, would you allow me to make two quick statements?

Mr. Ryland has been talking about what he does and what his clients do. If we imagine a bank for a minute, I think it's important that we not become mesmerized by the really effective things that Mr. Ryland does. If I took a device that I could probably get if I tried hard and stuck it under the desk of the executive vice-president of the Bank of Montreal, it would be a recording device. As he accessed the information and put in all his passwords, I would be able to access these from the office next door or in another city.

Talking about the Internet of things, I still don't think we've come to grips with developing a relationship with a light bulb. I think things are better than they used to be, but again, if you control the light bulb—and I'm making a joke of it.... But whatever device you want to use has the capacity for acquiring information.

The security of the systems we're talking about has two real components, the part that Mr. Ryland talked about and the environment that the financial institutions use. They're equally important, because if you get in from the financial institution's perspective effectively, either through a device that I've talked about or some other device, you can wreak not only on that financial institution but also complicate Mr. Ryland's life a great deal.

It's not just the highly complex security devices that Mr. Ryland talks about. It's a whole raft of other things as well. I would argue that the Royal Bank of Canada probably does these very well. A lowly Manitoba credit union may not. Forgive me, anyone here from Manitoba. It's the weakest link in the chain issue that we haven't really come to grips with as effectively as we could.

The Chair: Thank you.

As a result of this study, I've been paranoid talking in front of my refrigerator or my thermostat. Now I have to worry about my key fob and light bulbs.

Mr. Motz, you have five minutes, please.

Mr. Jim Eglinski (Yellowhead, CPC): You've got lots to hide.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Chair.

Thank you, gentlemen, for being here.

Mr. Fadden, when we were talking previously about combatting terrorism, you referred to our current Canadian model as more like a whack-a-mole where we suppress a problem after it has begun. Is there a mechanism to be more proactive in preventing cybersecurity attacks than just education or literacy?

Mr. Richard Fadden: Yes, I think there is.

If you look at what you can do—and I'm not an engineer, so I've reduced this to language I can understand—you can have purely defensive measures. You build something in whatever system you have: You have firewalls and whatever.

Then you have what I call "aggressive defensive": You have the capacity to know when somebody's trying to go out or come in, and you deal with that.

Finally, you have the purely offensive: You have the capacity to go out and either seek trouble or degrade somebody else's capabilities.

I think we're fairly good at the first. We're not so bad at the middle. I don't think we're so great at the third. I'm not sure that we, Canada, have to do this alone. We can do this with a bunch of other countries. However, the capacity of what I will call "cyber adversaries" to use 37 cutouts makes it very difficult for people to know where they're coming from, and whatnot.

You really do need some sort of worldwide monitoring system. I don't think we have that. I think the United States, insofar as I understand, tries, but there's a limit to what even they can do.

You've probably heard of former U.S. Secretary of Defense Donald Rumsfeld. He was ridiculed at one point, but I think he said one thing that's true, and it applies to this area: You don't know what you don't know.

I think Mr. Ryland will agree with me—

● (1625)

Mr. Mark Ryland: There are the known unknowns and the unknown unknowns.

Mr. Richard Fadden: Those are the ones I'm worried about.

Technology is moving so fast that we find it very, very difficult to stay ahead.

This is a long answer to a short question, but I don't think we're doing as well as we might do internationally.

Mr. Glen Motz: Okay, to take that further, you recently suggested that we're kind of on the margins when it comes to our ability to monitor ISIS terrorists or foreign fighters who have returned or are returning to our soil. Would you say that we are in a better position when it comes to cybersecurity?

Mr. Richard Fadden: Well, if you're dealing with the Government of Canada, I would probably say yes. I think that government, over the course of the last and current governments, has made some real strides in developing the capability to defend Government of Canada systems. They've limited the Government of Canada's systems' access to the Internet, which made things a lot easier to control.

I kept coming back to the weakest link in the chain. All you need is one weak link that allows you to access everything. Having said that, I think on the cyber side, the government is doing better than it might do on terrorism. I don't think it's doing terribly on terrorism. I was just trying to suggest that there's a limit somewhere to what you can do.

If you expand that to provincial governments, for example, there are connections between the provinces and the federal government. The provinces vary a great deal, I believe, in how protected they are. Then you keep moving on, and it doesn't take a great deal of imagination.

I'll give you an example: I read a couple of years ago that there was a mom-and-pop metal welding shop—I think it was in Arizona—that had its own little server and whatnot. A foreign state used a problem there to access an element of the U.S. government in China. The point I'm trying to make is that it doesn't take a big hole, to use a physical manifestation, to get in.

I think, generally speaking, we're not doing badly. We really aren't, but if we think that we have blocked every possible cyber-attack against us or our economy, then I think we're being way too optimistic.

Mr. Glen Motz: We have silos in law enforcement in fighting some battles, sometimes, and in sharing information. You've already alluded to the fact that in Canada, we have a lack of resources applied to this issue.

Do you see the same issue of siloing when it comes to cybersecurity?

Mr. Richard Fadden: It's not so much siloing. Some of my former colleagues will want to kick me under the table for saying this, but I don't think there's a central controlling brain to deal with cyber issues in the Government of Canada.

I think CSE has a real role. I think Public Safety has a role. The military looks at things slightly differently. GAC has a role in dealing with things internationally. ISED—I think that's what it's called—is involved in the regulation of the Internet and how we play with them.

I don't think the American practice of creating a czar is necessarily the issue. I would suggest, at least on the basis of when I was the national security adviser, that we could have used more coordination, and maybe at some point, more direction. It's a very complex field and departments worry first about themselves.

The machinery of government is the Prime Minister's prerogative. He or she will organize things as he or she wants, but this is one area that I think is so global in its manifestation, so complex, that simply saying to various departments and agencies they have to cooperate may not be enough.

● (1630)

The Chair: Thank you, Mr. Motz.

The final five minutes go to Mr. Picard.

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

Mr. Ryland, my understanding of the cloud is that it is a centralized structure for which security measures and safety levels are so high that clients whose data you store feel pretty sure that they are 99% safe against outsider attacks.

Mr. Mark Ryland: I think that's a very fair summary. They certainly feel that they have a leg up in building proper defences, because we're taking care of a lot of things they would otherwise have to worry about.

Mr. Michel Picard: But you just said to Mr. Graham that you had no knowledge about the content stored on your server, because it's not your business to know what your clients put on your server, so how safe is your system from a Trojan horse?

Mr. Mark Ryland: It's very safe, because we constantly build and test our systems to assume that we have hostile customers. We assume we're being attacked by our customers, and we take that into account and make sure that the isolation properties of the system are very strong.

Mr. Michel Picard: So there's safety on both sides, from attacks from outside as well as from those from inside.

Mr. Mark Ryland: Yes.

Mr. Michel Picard: Excellent. Thank you very much.

Mr. Fadden, this study brought us on a journey. We had no clue where we were going, because it's so vast, big, wide and diversified. We totally understand the relevance of any action to be taken on this, especially on my side, with financial institutions. From your knowledge of government and your experience, where would you say we should start in establishing policies, and what are some of the recommendations you might have?

Mr. Richard Fadden: I think, Chairman, I would go back to one of the points I made earlier. I think Parliament legislatively has to impose obligations on financial institutions, in much the same way it has done with money laundering. It has to require them to do a variety of things. Right now, most of the things are done in the self-interest of the financial institutions. They tend to be pretty good, but we should up, significantly, our reporting of breaches and attempted breaches. There's a regulation, if I remember correctly, that requires that now. It's not as fulsome as it might be.

The Americans and the Brits, in particular, have severe penalties for institutions not reporting breaches. I don't know how we can expect to deal effectively with breaches if we don't know when they're occurring. I think it's better than it has been, but still.... So I would say imposing clear obligations on the institutions and reporting of breaches. Again, some of my former colleagues are going to kick me under the table, but I don't think we share enough classified information with the private sector. I think we do far better than we did 15 or 20 years ago, but if you take the most senior technological official in the Royal Bank—which happens to be where I bank, but I'm not trying to promote it—and you ask them to collaborate on cyber issues, and the Canadian official isn't authorized to share any classified information, I don't see how you can have a real dialogue. The States and the U.K. clear, from a classified information perspective, people in the private sector. I don't mean to suggest that we don't do any of this, because we do. I'm just arguing that we don't do enough of it. I would say those three things.

Mr. Michel Picard: When you mentioned that we might be tempted to ignore or forget about Russia and China because we are focusing somewhere else, I was surprised. I thought we were focusing so much on Russia and China that we were forgetting about real threats coming from other countries, satellite countries working for those main states. When we looked at Cambridge Analytica at our committee, it was obvious that at the end of the day it might not be Russia, but with so many satellite offices in other countries in action, where should we put our focus?

Mr. Richard Fadden: That is, I think, Mr. Chairman, the $57,000 question.

Voices: Oh, oh!

Mr. Richard Fadden: Part of the problem is you can't ignore Russia and China. We can't ignore those things that you just listed. I think we ignore international terrorist groups at our own cost. We have a whole bunch of civil society groups that muck around with cyber. I could probably go on, but the truth is we can't ignore any of them.

That's why I think there needs to be more collaboration, more sharing and more efforts to get us to a point that one of your other members suggested. We need to try to get ahead of the problem more than we have in the past. I don't have an answer except to say that while you may well be right in this six-month period, maybe in the next six-month period things are going to shift. We need to be fleet of foot. Again, after working for government for 40 years, I can say that's not one of our strong suits. It's true of governments generally, but I think we need to be fleeter than we have been to deal with all of the topics you're talking about.

● (1635)

The Chair: Thank you, Mr. Picard.

Before I suspend, I just want to thank our witnesses. Usually "fleet" and "government" don't go in the same sentence.

With that, we're going to suspend for a minute or two. Thank you for your presentations.

Mr. Richard Fadden: It was a pleasure.

Mr. Mark Ryland: Thank you.

The Chair: The meeting is suspended.

● (1635)

(Pause)

● (1635)

The Chair: We'll manoeuvre around the vote call at 5:30. We'll probably stop around 5:20, as opposed to 5:30. I'll stretch it as far as I can.

With that, we're back on and I'll ask Mr. Drennan for his presentation.

It's for 10 minutes. If you look up, I'll give you an idea of when you're getting close to the 10-minute mark.

Thank you, Mr. Drennan for appearing.

Mr. Steve Drennan (Director, Cybersecurity, ADGA Group): Thank you. I am Steve Drennan and I'm pleased to be here today representing myself and ADGA in the cybersecurity domain and financial sector in Canada. Thank you for the invitation to provide testimony to the public safety committee at the House of Commons today and for all of your time.

For a bit of background, ADGA is a one hundred per cent Canadian company that has delivered strategic consulting, professional services and world-class technology in defence, security and enterprise computing for over 50 years. It provides high-end solutions, engineering and staffing in the government and commercial spaces. ADGA has a lot of insight, given all of this, and expertise into domains such as cybersecurity. ADGA also has strong views, as do I, on coast-to-coast security requirements and evolution and on our being abreast of the landscape and strategic partners. ADGA has a strong converged security capability with lots of cyber assessment design and compliance background. That's just to give you a feel of where I'm coming from today.

From reviewing previous testimony online, I saw a theme that the committee already had a lot of feedback on cyber-attacks, challenges, ranges and faults in the domain. Given all of that, I thought I'd focus today on cybersecurity solutions. There isn't a silver bullet to it, but there is a lot of capability that can be deployed on scale and a lot of other parts that can be developed to really increase what we do and strengthen the Canadian financial sector.

I like to think of it as critical infrastructure. You probably think of power stations and dams and classified systems as critical infrastructure, but the financial sector certainly is critical infrastructure. It's one large interdependent system that ranges across lots of different entities, like the Bank of Canada, Payments Canada, Interac—who I know were presenting—the Receiver General, merchants, small and large commercial entities and also consumers. Those are a lot of end points. There are a lot of things that can go wrong there. It's all the data, too, that is in transit and in storage. If you've been hearing and thinking about one network, one piece or one solution, it's not the whole story.

There's a shift occurring in cyber. It's shifting to socio-political attacks and brand manipulation, along with small and large volume financial attacks. Given what's at stake and the ability of cyber criminals to hide, obfuscate, and launch attacks on a non-stop basis, Canada needs to have an updated approach to cyber defence in the financial sector. The days of hiding behind walls, actual walls or firewalls, are past. It's a very interconnected space out there.

It's important to understand the adversary too. I think you've been well briefed on that, but cybercriminals and nation states have massive sets of resources. They'd be a very large country by GDP if all the cybercriminals put their wealth together. They are often physically unreachable because of where they come from.

One stat, a brief example, and I won't get into too many, from a recent Mandiant report—Mandiant is the cyber arm of FireEye, one of our strategic partners—is that the global median dwell time is 101 days. Dwell means the time that malware lives in a network until it's found and stopped. Just think about that for a second. That's an incredible amount of time for something to be sitting there exfiltrating and taking data before it's even found. Sometimes it goes up to 2,000 days before it's found. While the cyber problem is complex, it can be tackled in a way that is simplified for users, merchants, businesses and banking organizations. That's what I want to focus on today, that is, on some of the ways we can address this.

I'll focus on cyber solution themes that can address large-scale cyber-threats to the Canadian financial sector. Theme one that I'd like to go over is what I call “convergence of cyber data and protection capability”. Think of this as next generation solutions that could be deployed on scale for everyone to use and take advantage of. The concept is that one organization could actually lead this effort and put this capability in a central location so that it would be turned on for all of the entities I was just speaking about—everything we've been thinking about.

● (1640)

There's really fantastic new technology. One of them is linking ideas around centralized artificial intelligence, machine learning, advanced analytics, threat hunting—if you haven't heard about that, you can ask me questions about it later—and security orchestration. You can actually create semi-automatic cybersecurity detection and response. It can be fairly automated. Sometimes you do want somebody to be able to make decisions on key points and react when you sense a cyber-threat, especially if you're shutting down part of a network.

Smart buildings and networks can also be a part of this. It's not just green. Green is good, but when you introduce all kinds of Internet of things sensors, you're introducing a whole bunch of data, and that data can then be compromised. If we have an ability to sense across the physical data—operational data, sometimes called OT data, and the IoT data—we can have solutions that can better sense when there's a problem. For instance, if there's an environmental problem or an attack against a building or data centre, you'd probably want to know about that in the cyber-world and be able to respond to it. Today it's not very merged, but it can be.

There's the notion of moving forward on cyber-active defence or even offence, and that is linked to legislation and what the rules are. When you know you're being probed and attacked, the ability to respond to it, to determine where it is and to shut it down to at least protect yourself, is a very important capability.

The securing of domain name service, which is at the heart of the Internet, has standards around it called DNSSEC and others. That's really important because, if you can't trust your address resolution and where you're going to for data, that's really important.

Cyber-threat intelligence, which we touched on earlier, is really interesting because it can be done vertically. You could have just Canadian data and banking information, so you would see trends in attacks in the Canadian market space, and you'd be seeing them before they hit most of your end points, and then you'd be able to react to it in advance. You'd be able to make decisions and do updates before it became a widespread attack. That could be zero-day attacks or APT attacks, but the ability to see and respond before they become a problem is very important.

● (1645)

The Chair: Excuse me, Mr. Drennan. The antiquated system that we have around here is intruding into a very impressive presentation on cybersecurity. I'm told we have.... Is it not 15 minutes?

Mr. David de Burgh Graham: Don't use ParlVu.

The Chair: Initially I thought it was a quorum call, so I didn't say anything, but then the time was running, but it's not. We're going to leave it as a quorum call.

Mr. David de Burgh Graham: You could save yourself 45 seconds by looking at ourcommons.ca instead of ParlVu. You get a direct feed that way.

The Chair: I'm having what he looks at.

Mr. David de Burgh Graham: You're looking at the wrong thing. Get faster.

The Clerk of the Committee (Mr. Naaman Sugrue): I'm looking at both.

The Chair: Okay, we just blew 45 seconds. I apologize for that.

Thank you, Mr. Drennan, for your patience and understanding. Go ahead.

Mr. Steve Drennan: Thank you.

On the last point about capability, something that could be introduced on scale, as we were talking about in this theme, could be supply-chain and life-cycle management. CSE, the Communications Security Establishment, which also has the cyber centre, used to run a program called the "evaluated products list".

When we talk about Huawei, people have issues and we talk about them. We have to think about everything that gets introduced, all the software that's built—it's often virtualized and put in the cloud—the hardware and the chips. Where do the chips get manufactured? Where do they come from? You can have a complete cradle-to-grave program so that you evaluate that equipment and that software so that you know you can trust it. The government is the right entity to be able to manage that program.

The second theme I'd like to go over is leveraging a secure public cloud. I think the speaker before me was from AWS, so I'm sure you heard plenty on it. I'm here to say, too, that it's a good idea. When you're trying to bring all of these different groups together, one of the best ways to do that is with a secure Canadian public cloud, and I think we need to start thinking more about that. I know a number of banking entities that are looking at moving that way.

When you have networks inside, that's a private cloud, or a hybrid cloud as you move out to the public cloud, but leveraging a secure public cloud on scale is really important because that would be a great way for the whole community and all of those consumers to speak to each other. If you set up the right security, and policies and filters, everybody will have the same security. There are operators who have true failover within Canada, so if you have a failure, which you have to expect and count on, then, when you have disaster recovery, it stays within Canada. That's really important for the residency and custodianship of the data itself.

Cyber-agility is a piece that's really important here. It lets you move and launch new applications.

The Chair: You have one minute left.

Mr. Steve Drennan: All right; I'll move faster. The third theme would be about establishing a lot more trust around critical data. The banking and key banking groups could actually become the trusted single source for registration, authentication and credentials.

My fourth theme is about user awareness. Let's not lose sight that our weakest link is still the user. We could have more specific mandates and more training so that people are more aware of what to click on, what's good behaviour, what's good hygiene.

In conclusion, there are next-generation cyber solutions on scale that can be used to stabilize and empower the financial community, but it's going to take the right funding and drive to make that happen.

● (1650)

The Chair: Thank you, Mr. Drennan.

Colleagues, we have about a half an hour. If I go with seven-minute rounds, that will pretty well use up the half hour. If I drop it to six-minute rounds, I could get one more question in. Is that fine?

Some hon. members: Agreed.

The Chair: Okay, we'll have a six-minute round. We'll have Ms. Dabrusin, please.

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

I wanted to start with your fourth theme because that's something that has really caught my attention since the beginning of our hearings when someone talked about having a really secure system delivering information between two cardboard boxes, and the individuals at either end being the cardboard boxes. When you were talking about user-awareness, I know that you didn't get a chance to finish what you were going to say about that, but perhaps you could talk more about it now. What are the specific things we could do better as a government and for public awareness, and how do we increase cybersecurity, cyber hygiene, whatever we call it?

Mr. Steve Drennan: Good. I'm glad I get to talk more about it. I don't think there are a lot of standards. When I look at the Treasury Board guidelines and MITS and its requirements, it's not very clear. It doesn't really define what you have to do to train users and to provide a lot of cyber guidance. It's a bit passive. We have our cyber-safe websites. We have places people can go to learn, but are we actively promoting enough information? We could have more campaigns. We could have more learning through games and monthly meetings and themes to raise an awareness. I'll take one example on spear phishing. Has that been well covered here?

Ms. Julie Dabrusin: I don't believe so.

Mr. Steve Drennan: Has phishing been covered?

Ms. Julie Dabrusin: Yes.

Mr. Steve Drennan: Spear phishing is more accurate phishing. If it looks like the Hon. John McKay is sending a message to all of you and he tells you it is urgent and you have to click on it, you may think about clicking on it because it looks like it's coming from John McKay.

The Chair: That's a bad example.

Voices: Oh, oh!

Mr. Steve Drennan: Well, it was one example. If it looks like it's coming from a position of authority and looks like it's your style of writing and mentions things that are typically in the messages you exchange, it would seem more likely that you should just click on it. They can use pressure. We'll see sometimes formatting problems, misspelled words, but you have to look. How often do we just pull out our devices and work really quickly to click through the messages?

A bit of training, though, and awareness around spear phishing can help, and you can't just do it once. You actually have to do it several times. One of the ways to do that is to do an anonymous type of analysis spear phishing campaign and you actually send almost everyone in the organization a spear-phishing type of email. You're the ethical person, so it's okay. There's a link, and if they click on it all it will do is register anonymously that someone clicked on it. At the end, you end up with a statistic of how many people clicked on it. And it's not going to be good the first time. Then you say, "By the way we ran a spear-phishing campaign. Come and visit at lunch and learn and we'll explain why you shouldn't have clicked on it." So many people did. The next time you do that, because you do it a second time and a third time, the awareness gets raised. You start raising this awareness with your users and then your users are much better. They're never going to be 100%, but getting the percentage a lot lower is much better.

Ms. Julie Dabrusin: That's helpful. That's something an organization can do. I guess what I'm trying to figure out is this. When we're looking at what recommendations we can make, how can we build our role from that?

I note that one issue that came up with one of the witnesses was passwords. We already have a prompt now when you enter a password. It tells you that you need a certain number of characters, capitals, and different numbers, whatever. What it never prompts you for is whether or not you have ever used the same password before. Apparently, a big weakness is that people use the same password over and over again. That's fairly usual. Just having a pop-up box to ask whether you've used a password before would seem simple, but it would mean that the password you were about to use was not a strong one even if it met the other markers. When we're looking at the financial industry, people signing up for online banking and these types of things, are there things that we can try to put out as recommended standards?

Mr. Steve Drennan: Yes. I think there are two points in here. There's the cyber-awareness training and the passwords, so we'll talk about both.

For the passwords, yes, there should be more standards. They're actually easily set by policies. You should set more policies on it. That can be mandated in legislation. It would be more clear. When I look at MITS or at requirements, it's not always clear what the password guidelines are. It's not prescriptive enough.

Absolutely, that's just one example. You probably want to do away with common and known passwords that people choose often. You want to try to make sure that they don't choose dates that are reflective of their own personal history and that an attacker might also already have.

There are ways of making sure that gets legislated and then enforced. That's a very good example—

● (1655)

Ms. Julie Dabrusin: Can I just jump in quickly on that? I don't have much time.

Mr. Steve Drennan: Yes.

Ms. Julie Dabrusin: Do any countries have that? Are there any examples that we could look to for that type of thing?

Mr. Steve Drennan: Not that I'm aware of, but Germany and Europe tend to have a lot more legislation around this. With GDPR and other standards, you might see it there. I'm not a hundred per cent sure.

Ms. Julie Dabrusin: You can continue. I just wanted to get that in.

Mr. Steve Drennan: I would say that the other thing, though, is that there are too many passwords, too many different passwords. How many systems does everyone in this room have that they log into just at work?

You can actually have a lot of those passwords synchronized, and then make it two-factor or add biometrics on top of that to create a stronger but more consistent password. That's actually a lot more effective. When you back it up with the ability to audit your users and look for behavioural issues that you might see on the network, it's a much stronger approach than everybody here having 15 passwords that they have to recycle all the time.

The Chair: Thank you, Ms. Dabrusin.

Mr. Motz, you have six minutes, please.

Mr. Glen Motz: Thank you, Chair, and thank you, Mr. Drennan, for being here.

As you indicated, your group works with government, industry and law enforcement on issues of security, including national security. Last year, one expert in our security study noted that he had "Zero confidence" in Canada's readiness for emerging technology threats like AI and quantum computing.

In your experience with your work in Canada, how ready do you think we are with respect to that statement?

Mr. Steve Drennan: We are not as ready as we need to be, but we're not at zero. I would say that, unfortunately, it might vary a lot depending on which group you're looking at. For instance, at the Canadian Centre for Cyber Security they're focusing on analytics and the sharing of indicators of compromise and that sort of thing, where they could play a bigger role and probably will over time in terms of their capabilities and how that can be shared.

There are other organizations, too, that have varying capabilities because they have different security technology deployed. Some of them would have Fortinet firewalls and some other people will have, say, Check Point or Cisco firewalls. Some of those firewalls will have different kinds of capabilities enabled, and some of it is next generation and some of it is not.

Unfortunately, there's a lot of variation in terms of what we can respond to. You mentioned AI, machine learning and quantum. As the attacks become more sophisticated, we do need to have more sophisticated countermeasures on scale, and that's why I was talking about the use of a public cloud. For the financial sector, if it were run from a common place, that more advanced capability would be there for almost everybody connected to that source. That's one way of bringing the level up for everyone.

Mr. Glen Motz: Canada, and I guess the world, for that matter, is said to have major gaps in talent with respect to cybersecurity. What is your group doing to try to develop more talent? How and where are you investing in skills and target groups in what is certainly an emerging field?

Mr. Steve Drennan: Yes, that's at the core of what is very important to ADGA.

ADGA is led by a female CEO. We're very proud of that and of our proud Canadian history and diversity as well. We invest heavily in co-op programs and bringing in people who have emerging skills to get them into cybersecurity—because that's what we're talking about today—but also into other fields as well.

There's a lot of work that we all play.... Recruiting is a function that we can get involved in at the university and college level. We can help with the actual programs they're taking. For instance, at Algonquin College, they have a very good program on cybersecurity. There are a number of cybersecurity parts that are being built out now at the university level as well. That's just here in Ottawa. We take an active role in that. We work with other colleges as well.

It's important to purposely recruit diverse talents and diverse skills and have a big diverse population, I guess, in terms of the people you have. We in Canada have to make sure that we maintain that talent. Keeping people excited and energized about the work is a responsibility for all of us. If there's a lot of cyber-work this year but none next year, where does all the talent go?

● (1700)

Mr. Glen Motz: Last week, I believe, we had a gentleman here from Ryerson. Some could argue that there might be some gaps in what they're going to try to roll out as far as their academic program is concerned. Does your group, or do groups like yours in industry, sit down with educational institutions and help them develop curriculum that will help to develop the types of employees and skill sets that you want coming out of our schools?

Mr. Steve Drennan: Yes. We actually have that opportunity. I've been involved in giving feedback to Algonquin's program in the past. There's also Willis College. We've talked to them. They have a program, and I've given feedback on how much cybersecurity is in there, on what should be in there, and on the Government of Canada security clearances they should get for their students as they go through, which will enable them to have better careers and stay in Canada. We have influenced and we do work with the universities on the programs—for instance, the programs for all the engineering students. We regularly meet with these groups. We're directly involved. We do get an opportunity with the faculties in academia to set those agendas.

Mr. Glen Motz: Can you explain the difference, if there is any, between cybersecurity in the defence sector and cybersecurity in the IT sector? Is there even a difference?

Mr. Steve Drennan: I can think of a few key differences. One of them is that it's like a dam bursting. In cybersecurity in Defence, they are just waiting to move from what's called “defence” to “active defence” to “cyber-offence” as the legislation gets moved forward, because it's a critical enabler. Cyber is now seen as a whole new area; just like having naval or air force, cyber is its own theatre of combat. It's pretty critical that we move that legislation forward so that National Defence can do more on the cyber landscape. As they deploy troops and as they're in theatres of operation, they can now win and lose battles based on cyber. That's one difference. They're held back a little bit. They also have a whole bunch of classified networks and other elements that all have to be brought forward. That has to do with funding and large changes that are being looked at right now.

In the private sector, there aren't as many rules. We talked about cyber-threat intelligence earlier. You will see the large vendors being able to gather that data across the world from the nodes they have in different countries, because it's less restrictive on how they operate. That's actually very positive, because then they're able to share that data with government and industry.

The Chair: Thank you, Mr. Motz.

Mr. Dubé, you have six minutes, please.

Mr. Matthew Dubé: Thank you very much for being here.

I want to go back to the labour issue that was raised by my colleague and look at a different aspect of it. Does the industry get hamstrung by the fact that when it comes to security clearances, these are based on things like where people are from and things of that nature? You're involved in procurement on the cyber side, but in traditional procurement, if that's the correct term, around the actual building of fighter jets, helicopters, military equipment and what have you, there have been issues in the past where, depending on where our allies are on a particular issue, or where we're at on a particular issue, different companies have been disqualified and missed out. They have highly qualified people working there, and perhaps the ideal equipment to serve, say, Canada's military, but the U.S. has an issue with a particular country or something like that. Are you seeing this issue play out in the same way in the cyber field? If so, what can we do to address that?

Mr. Steve Drennan: Yes, we are seeing that issue. For commercial clients, they're much more flexible. If your company has the right reputation and if you have the right people and skills, you can get those cyber engagements. We do a lot of security assessments and design and cloud security work. The message in terms of what you're able to do with the commercial sector, which is very sizable in Canada, is much more straightforward.

It is a challenge. I have lots of security clearances. It's been simpler for me, but for others, if they don't have enough residency in Canada, they can't get the security clearance. Typically, “secret” is required for most things. It can be “top secret”, but “reliability” isn't often the requirement. You need, I think, a five-to-10-year residency in Canada, and often to be a Canadian citizen. It might be good to look at mechanisms on how we could also do other security checks that would get people to secret and how we could make it much more uniform. There's probably no reason that every government department needs its own clearance process and its own rules. If you're trusted, you're trusted. If the company is trusted, it's trusted.

These are things that probably could be reformed over time. We probably should look at other ways to clear individuals. We have a bit of a brain drain in Canada. We should be recruiting talent from other countries. As we get those people here, we need to be able to get them busy and onto important projects and still give comfort to the government and banking that they have the right clearance and the right background.

● (1705)

Mr. Matthew Dubé: I appreciate that. In keeping with this issue, is there a particular issue for cyber, though? If you're a company that's building helicopters, you're not selling helicopters to the Department of Finance, but to DND. However, if you're operating in cybersecurity, Finance needs cybersecurity as much as DND does. Is there an issue there even where our traditional sort of military alliances make it easy to cut off people for security clearance when it comes to traditional military procurement, but it's more challenging when...? Is there an issue where, if you're involved in cybersecurity for the Department of Finance, let's say, and you're using a company that has skills coming from people who might not be recognized on the defence side? Do you see what I'm getting at?

You mentioned that security clearances are different. As Canadians, are we losing out on having proper protections, say, for the finance department because we're applying the same rules we would apply in defence because we're trying to create that uniformity where the alliances might be different and how it plays out in terms of—I mean who cares what the Americans have to say if we're protecting the Department of Finance, for example, unlike the military where we actually have an alliance with them?

Mr. Steve Drennan: I don't think the discrepancy is the issue. I think the issue is time. Now you're losing a year or two years sometimes before you can get key people in on engagements. For some of the cyber knowledge you want, you could take a group of people—I think we talked about how people can be accelerated and there's been witness testimony on how we can get people started quite quickly into cybersecurity, entry level positions and others. If you have a key group of people whom you can clear based on adding some people who are trusted from companies—and sometimes you need subject matter experts, let's say, from the U.S. So comparable clearances and moving quickly on it is fundamental. Sometimes what happens is that it's more about the time that we lose because of all these different clearances and that the impact of that is direct to national defence and to other groups that can't get teams meaningfully started for a year or two sometimes. The Department of Finance might not require as many clearances. DND requires what's also called a VCR at each site, but other entities don't do that. It's about having the same standards applied to everyone. If the data is more sensitive, that's what the clearance should be for everyone.

Mr. Matthew Dubé: With the 20 seconds I have left, I'm just wondering if you believe that we shoehorn or pigeonhole ourselves rather too much by looking at the traditional alliances and some of the countries that are comparable to Canada and that might have the expertise, but because they're not part of the traditional paradigm that we look at, we're maybe missing out on some of that talent.

Mr. Steve Drennan: Yes and no. I think we can go to the Five Eyes community and get a lot of that talent and have comparable clearances, but yes, we should also look at extending to other countries. How do we have a fast track clearance process from other countries so we can trust individuals for information, and how can we do it quicker?

The Chair: Thank you, Mr. Dubé. That was interesting analysis. The analyst here whispered in my ear, “That's exactly one of the big problems, just getting those clearances”.

Mr. Picard you have six minutes please.

Mr. Michel Picard: It's nice to see you again. You provide services to financial institutions, is that right?

Mr. Steve Drennan: Yes.

Mr. Michel Picard: What was the comment you made about the fact they would be the trusted company or the guardian of this critical information? What was that again?

● (1710)

Mr. Steve Drennan: It's a really key point. I just didn't have enough time to go into it too much, so thank you for the opportunity.

We all trust when we walk into a bank, and we all trust when we walk into the Bank of Canada, or one of these trusted places like the Department of Finance. That is something that can be leveraged in a very positive way. One of the things we talk about is passwords. When you're setting up credentials online, you have to be able to trust how you set that up. I think we should be leveraging that space and those personas and organizations more. That can establish more security for those online credentials and it can play a broader role. It can be more uniform as well. That's a key thing. We can set up stronger credentials that are more uniform that could be used in a more specific way for cybersecurity.

Mr. Michel Picard: Doesn't that create an awkward situation where a bank would be the guardian of my critical information instead of the bank having access to some third party being responsible for that information, because you put the customer in a vulnerable situation where he has to deal with the bank, being secure of course, but at the same time the objective of the bank is to make money, not to guard my information? That puts the customer in a weak situation with the bank.

Mr. Steve Drennan: The main thing would be that the bank would play a role called a “registration authority”. The bank doesn't have to have the data.

I think you've been briefed on tokenization. The data wouldn't have to be held by the bank; the bank could be the enabler of saying, “You are who you are, we know it, you've come into a bank, we trust you, you trust us, we've done a registration check.” It would be a function in support of setting up the online identity rather than holding the data.

Mr. Michel Picard: You were quite positive about the earlier comments of AWS about centralized structure and an iCloud type of system where everything is at the same place.

There are two things. First, does that mean you support any initiative towards open banking where everything is in the same place?

At the same time, we talk about those centralized systems with such trust in their security that we don't feel the necessity to discuss an insider job or human risk factors. It's as though they don't exist anymore.

Mr. Steve Drennan: Yes, I am in favour of using secure public cloud. That would mean large data storage, but the ability, then, to detect attack correctly when it's happening and protect the data better.

In terms of protecting that data, there are lots of mechanisms that can be used. For example, there are good products for cloud that enable you, at the field level, to encrypt data whenever you need to. If you have an insider threat and there's a breach, the data that's stolen is encrypted data. It's protected because it was protected properly as you stored it.

What we don't do a lot sometimes is organize our security design correctly, so when we're breached, we're not protected properly. We don't detect it fast enough and we don't know how to respond. To your point, if we organize ourselves and there is an insider threat, the data can be protected and we can more quickly detect and respond to the event, too.

One example I'm sure everyone is aware of is Snowden. He actually had a lot of access, and then was able to give himself more access. That's not exactly the paradigm you want to have in an environment. There are better ways of doing that.

Mr. Michel Picard: I'll leave the rest of my time to Mr. Graham.

The Chair: Mr. Graham.

Mr. David de Burgh Graham: Thank you.

Mr. Drennan, in the three minutes that Mr. Picard has been asking questions, I logged into a server, and using raw SMTP, sent myself an email from god@heaven.org. I think this brings to a big part of your spear phishing discussion the question, why is it that we are still using protocols that are completely hackable like that?

There's no authentication whatsoever in SMTP. I can put any spoofed address that I want. SMTP SSL is not universal, but it doesn't prevent spoofing in any case. Therefore, is there a role for, say, PGP signing our emails as a standard, or is there something we can do to sign cryptographically? Is that an approach we should be looking at?

For whatever reason, that has not taken off in the 25 years it has been around.

Mr. Steve Drennan: I'm speaking from some first-hand experience, but it's probably because PKI, or public key infrastructure, can be a bit of a big hammer in actually deploying certificates. Then what assurance of certificates are you deploying, and are they proprietary?

S/MIME was very good, but the point is that there are ways of establishing identity and having digital certificates, or proof of the message originator and who sent it and whether it has been tampered with, that can be added and done better.

Absolutely, there are technologies. If we standardized on one, that would be good. I don't know if we need full public key infrastructure. We have to be careful about what digital certificate approach we take, given the massive community that would be involved in the financial community.

● (1715)

Mr. David de Burgh Graham: What system would you suggest we use to authenticate? Email is the greatest source of all vulnerabilities as far as phishing, and so forth, is concerned, so what should we use?

What do you use?

Mr. Steve Drennan: Well, we're moving away from email. That's more for productivity reasons. Email is not necessarily being used for what it was created for. There are things such as Slack and other tools that can create more efficient conversations.

Earlier we talked about user awareness. People need to know how to use email and what to click on. Just because everything is encrypted doesn't mean a bad actor didn't send an encrypted email to you, so it still comes down to that point.

There are ways to do it. If we wanted to have a portal service where there would be secure emails kept in a location that you could pull down, that would an option. There's time-to-live encryption, so that when you send messages, they're encrypted, and then if you don't open them fast enough, they expire and disappear.

There are some options to look at.

Mr. David de Burgh Graham: Like key signatures.

The Chair: Thank you, Mr. Graham.

There are four minutes left. Are there any questions on the Conservative side?

Mr. Eglinski, do you want to use four minutes?

Mr. Jim Eglinski: You were talking about security along with Mr. Dubé. At your company, which works a lot with many government agencies, what security level do you look at for your people, or do you have to get them a secret or a top secret level?

Mr. Steve Drennan: In our cybersecurity team in the organization, we have a lot. We have the ability to hold and process top secret information. We have classified environments. We all get top secret clearance and these extra clearances that we were just talking about. We do that because it enables us to be able to do the contracts we were talking about earlier. We know we have to do it. It affects whom we can hire as well, and that's an unfortunate byproduct because we always want to get as much diversity as we can. But we get all the top clearances for sure. And some other parts go with it for —

Mr. Jim Eglinski: You seem to be a little on the negative side. There seems to be a lot of.... I used to do top secret investigations for security clearances, and a lot of work is involved in them. But you think that we should be reducing our level or our standard?

Mr. Steve Drennan: No, creating more consistency.

Mr. Jim Eglinski: More consistency?

Mr. Steve Drennan: So that all government departments can have the same clearance. If an entity or a person is trusted to a level of information or a caveat of information, they should be trusted equally wherever they go. They shouldn't need different clearances for different organizations inside Canada.

Mr. Jim Eglinski: There's no standard with a national set of rules that you have to meet to get to a certain level?

Mr. Steve Drennan: Absolutely.

Mr. Jim Eglinski: Okay.

I have one quick question; I think I've got about two minutes left?

The Chair: Yes.

Mr. Jim Eglinski: You spoke briefly about artificial intelligence. I've studied it in a couple of different committees other than this one. Do you think that in time artificial intelligence will be able to do cybersecurity better than we can do it personally ourselves right now?

Mr. Steve Drennan: I think the interesting way to look at artificial intelligence—hopefully it's not one of those bad movies that we've seen—and the way I've seen it being deployed now is that it can assist the operators. So when you have a security operations centre and you have operators who are very hard to recruit, build and keep, and you only have so many of them, they can make it a lot easier by reducing the datasets that you need to deal with and pre-making decisions, populating and making it very easy for you to make key decisions. So if you think of them as cyber assistance to help you get through all the terabytes of data and make your job easier and more focused, that's the way I think artificial intelligence machine learning is at its best for cyber.

Mr. Jim Eglinski: You don't want to feed them so much.

Mr. Steve Drennan: You can feed them everything; just don't let them press the button on everything.

The Chair: I want to thank Mr. Drennan on behalf of the committee for a very fascinating period of time and discussing things that Mr. Graham is pretty well the only one who understood.

Mr. Steve Drennan: Thank you.

The Chair: Thank you again.

Colleagues, the subcommittee will start in two minutes.

The meeting is adjourned.