HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 146 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, January 30, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, January 30, 2019

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Colleagues, let's bring this meeting to order. We are already past 3:30, and I see that we do have quorum.

This is the 146th meeting of the Standing Committee on Public Safety and National Security. We're undertaking a study on cybersecurity in the financial sector as a national economic security issue.

We've been advised that our other witness is stuck in his own security line, but I imagine that will clear with some time.

I see that Mr. Kabilan is here. I'm sure he is knowledgeable about appearances before committee, so without further ado we'll ask you for your 10-minute presentation, sir.

Dr. Satyamoorthy Kabilan (Vice-President, Policy, Public Policy Forum): Good afternoon.

Thank you very much for the invitation to speak to you today. The topic you've asked me to cover is the issue of cybersecurity, and in particular how it applies to the financial sector.

I think it would be useful to start with a very quick bit of background information when it comes to cybersecurity, in terms of why the financial sector is of interest, who the actors might be who might be interested in attacking, compromising or otherwise getting into the financial system, and some of the challenges that go with trying to protect the financial system and why.

I did provide my speaking notes beforehand, and the cover is just some very, very big numbers. Essentially, we're talking about the rate of breaches per day. It's in the hundreds, if not more, and it just keeps going up. People are very interested in attacking organizations from a cyber or Internet perspective because it's easy. You can be anywhere in the world to do it. In particular, when we think about those who might be interested in the financial sector, I would bucket them into four categories.

The first category is very easy: people who like the challenge. I sometimes refer to them as thrill-seekers. Financial institutions represent probably the toughest nut to crack when it comes to cybersecurity, so the kudos that goes with successfully breaching systems is very high in the hacker community. In many cases, this sort of action may be harmless and may be more reputational, such as changing the graphical interface on a web page, but nevertheless it's a group with interests in the financial sector.

Second are the hacktivists, those who have a social or political cause and see the financial sector or some of those it supports as being part of the challenge they face. Hacking helps them to further their cause or further their message. Again, I think it's very straightforward. Everyone has heard of Anonymous, though they're not very anonymous anymore.

Third are the criminals. Again, this is very straightforward in some ways. In the financial system, there's a direct monetary return that can be gained by criminals, but it's not just the direct monetary interest that criminals have, and I think this is very important to emphasize. You could hack into a system and try to siphon out money, but it's not just money that's in the system—it's information. It's personal information and information about the dealings of companies, all of which can be monetized in other ways. When we think about criminals, it's not just about direct monetization off the attack; it's also about the indirect benefits they can gain.

Finally—and I think this is where some of the biggest challenges are coming from—there is the issue of nation-states. You might ask the question, why would another state be interested in our financial system? If you think about it for a moment, in terms of the challenges we face in today's world, economic competition is as stiff as it ever was, and understanding the financial system, because everything flows through it at one point or another, gives you a very strong indication of not only how the country is doing, but also potentially how some of the corporations within the country are doing.

When it comes to having the upper hand in the economic challenge sphere—I shouldn't say “warfare”—from nation to nation, understanding the financials of a nation becomes very useful. If you think about that further and you're talking about nation state-sponsored takeovers, that information becomes even more useful. Ultimately, if you think about modern warfare and modern threats, think about the financial system this way. At the end of the day, our financial systems are literally based on confidence. Anyone who is able to infiltrate that and affect that confidence will affect our markets.

We've seen time and time again how markets change just on the basis of what people think is going to happen. For those nation-states, in terms of a leg-up, in terms of a new hybrid warfare option, that becomes a target of tremendous interest, because the consequences can be quite significant if you manage to undermine confidence in the financial system.

If we take a look at those four actors and then look across the financial system, I think there are five key challenges we have to think about.

The first is—I think this has been mentioned time and time again—that we think about the threats we face in terms of regulation and legislation. We think that if we put in the right rules and the right standards, we'll be able to stop bad things from happening.

I don't know how many of you have the 60-day or 90-day password rule change. Just to let you know, that was invented in the days when it took between 60 and 90 days to compromise your account from when someone had your password, but this is an ISO standard, and in many cases it's a requirement for companies.

● (1535)

First and foremost, standards are actually struggling to keep up. By the time a standard comes into place, we've gone well beyond it. I think the first big challenge we face, particularly in the financial sector, which is heavily regulated, is that if we just depend on standards and regulation, which cannot keep up with the threat, for me they're just the table stakes to get into the game. It has to go far beyond that.

The second issue, which is certainly as pertinent in the financial sector but it cuts across everything in cybersecurity, is the issue of information sharing. If I'm company A and somebody has tried to attack me by going after a very specific piece of software and no one knows, it's a zero-day vulnerability. No one yet knows this vulnerability exists, but the rest of the financial sector, maybe 70% of it, depends on the same software. Do you know what? It's embarrassing to admit that I've been hacked, so I'm not going to tell anyone. That's the typical story we hear about cybersecurity. The information about what's happened is rarely, if ever, shared or made available. Now, this is not about embarrassing anyone. This can be made available anonymously. Some nations like Australia, for instance, are pushing for more and more disclosure when it comes to breaches or attacks. Having that intelligence and information shared actually has a crucial role to play in cybersecurity, and it's something we have not gotten right yet.

The third challenge is that whenever I say “cybersecurity”, someone brings up a smart phone and says, “Yes, it's about securing this.” Cybersecurity is not just a technology problem. In fact, if you look at the latest breach statistics from the Australian privacy commissioner and work it out in terms of the different categories they use, over 60% of it comes through humans, either malicious or non-malicious, making mistakes or being socially engineered. That's 60% or more. This is not just a technology problem; it is very much a human problem.

I would say this to you as well: If I wanted to hack your bank, I wouldn't hack your bank; I would hack you. It's far easier to engineer a person than it is to get through the protections that a financial institution or a large organization might have.

The fourth thing, which is kind of an extension of that first piece about technology, is users. I think there was a news story a few weeks ago about a user being compromised because they were taken in by a scam and they were actually paying out large amounts of money. Unfortunately, that security, as one expert once described to me, is like armoured vehicles with armed officers taking money between two cardboard boxes, and it's the cardboard box at the end that we worry about, because the user at the end may not be as well defended, or may not understand things as well as the bank or the financial institution or the provider of the services might.

My biggest nightmare was when my father got an eBay account and a PayPal account. Not everyone is familiar with the digital world, and therefore there can be attacks against them, and while you and I may look at those and laugh and say we know they are scams, not everyone will. So the user at the end of the chain is another piece that we need to think of.

Going back to the comment I made about confidence, it may not be a financial institution's fault, but if enough of those users, particularly as people age, start suffering these attacks, think about what that does for confidence. They tell their friends; their friends tell their friends, and that spreads. There's a problem with the system, but it's not the system; it's the user, at the end of the day.

The last piece, which I think is a very big challenge and certainly it's pertinent in today's headlines, is the issue of supply chains. This might sound a little odd in cybersecurity, but think about it this way. We buy equipment; we buy bits and pieces from all over the world, and we integrate those into our systems. If we look at the earpieces we're using today to the translation systems, to the audio systems, there will probably be anywhere between three and 20 countries involved in constructing all of those. There's a direct supply chain, but it's not even in the equipment we're using directly. For those of you who remember the infamous Target breach, it was the HVAC system that they went after. They went after the HVAC company, and through that breached the system, and from there got into Target.

Supply chains have become very complex. They involve not just the bits and pieces we buy, but also the organizations that provide services to us. Again, I wouldn't attack your company; I would attack whoever services your company. When we think about cybersecurity, all of these elements add up to a very dangerous picture, which is, what does that do to confidence? If enough of these incidents keep happening, will they affect confidence, which is ultimately what underpins our financial system? That's why cybersecurity in the financial sector is a major concern and continues to be a major concern today.

● (1540)

The Chair: Thank you very much.

Apparently, colleagues, our second cybersecurity expert is tied up in security, which is a problem. I propose that we commence our questioning. When he arrives, we can interrupt the questioning to hear the testimony.

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

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Mr. Chair, thank you very much.

Thank you, Mr. Kabilan, for being with us today.

One of the lenses I would like use in exploring this topic is the premise that good cybersecurity is good for Canadian business, is good for foreign investment, is a social good. Where do you see the Canadian system being positioned vis-à-vis, say, the Five Eyes allies we talk to a lot? You mentioned Australia. How are we doing specifically with respect to the banking sector? What concrete challenges do you see that this committee should be looking at?

Dr. Satyamoorthy Kabilan: First and foremost, to the assertion that good cybersecurity equals good business and good opportunities for Canada, I would wholeheartedly agree. In an era when data has become so important, and the ability to operate on a virtual basis has become the core or fundamental for almost every organization today, it has become almost an infrastructure requirement to have good, concrete systems that are safe and secure.

To the question around where Canada is now, that's actually very difficult to judge. I would go back to my previous statement about information sharing. There are some overt pieces where I think we may not be doing as well. One key overt piece is the issue around information sharing on cybersecurity breaches. We don't have a requirement to do that. There have been attempts in the private sector to try to remedy that—the Canadian Cyber Threat Exchange is an example, and I believe you'll hear from Scott Jones later on—but I don't think we do very well on that.

In terms of actually acting, one of the things we need to look at is how we get that information back out. If you've been breached, or if you suffer from an issue, it's not to embarrass you or cause problems from a shareholder perspective; it's just so that intelligence can go back into the community and say, “Here's the vulnerability. Here's something to do about it.” While it's hard to judge where we are, we certainly don't have something robust in place that makes us share that information and ensures that all organizations can get access to that type of basic information.

Mr. Sven Spengemann: That's very helpful.

Do you see the tendency to under-report cybercrime as being limited to the stigma of being embarrassed about reporting a breach, or are there other factors that the committee should know about?

Dr. Satyamoorthy Kabilan: Certainly embarrassment is one, but it can have financial repercussions as well. Those can be direct—i.e., fines for loss of personal data—and also indirect, such as from the reputational damage that goes with it. You can also have, of course, direct impacts on shareholders, for example on share price. There's a whole range of impacts that go with it.

When I was in my previous role, we did a piece around information and intelligence sharing. There's another little piece in here that I don't think we've addressed but that may help—namely, the misperceptions between the public and the private sector around what can and cannot be shared and around what will and will not be protected. For example, as a private company, if I were to share some of this information with the Government of Canada, technically that would be privileged. That should be protected from being disclosed under ATIP. Again, it's private information and it has commercial implications. That's not always well understood: where that information resides and how it's protected.

On the flip side to this, some reports have looked at the challenge within government of understanding what they can share back the other way. The constant riposte we get from the private sector around clearances is “I may have a secret clearance, but I can't have a secret conversation or secret data actually shared with me.” There's still the caveat that regardless of whether you have that clearance or not, the information flow is still very much dependent on relationships that you might have and not so much on whether or not you have the clearance to have it.

Mr. Sven Spengemann: Thanks very much. Again, that's very helpful.

You're speaking just about financial institutions, the cornerstone of our economy, the large institutions that have capacity to look after their own cybersecurity infrastructure. I want to shift the lens a bit and ask you about your thoughts on small businesses and start-ups. This government is very focused on creating an environment that encourages entrepreneurship and start-ups and innovation. For smaller businesses, the cost of having to provide their own cybersecurity infrastructure is....

I'll put it over to you. Is it prohibitive? Are there specific challenges we need to look at for small business? If so, what augmented role could governments take to provide that platform of good security?

● (1545)

Dr. Satyamoorthy Kabilan: I don't have any in-depth research on this, but certainly from the little bits that my team has looked at in the past, it's not so much the cost that would be the first thing I would address, though that is an issue. For some things, such as making sure you have up-to-date systems, etc., there is a cost involved, but a lot of it is down to education. How do I actually protect my systems? What is actually necessary, and how do I quantify the risk that my company faces? Is the risk I face because I have a food truck and I take credit cards? Is that the same as the risk I might face if I ran a small boutique store and I was taking personal information because I wanted to create a loyalty scheme? Are the risks the same? Is the data going to be looked at in the same way in terms of actors who might be interested in attacking my organization?

I think the bigger challenge is not so much the cost; it's a more fundamental issue. It's around education and it's around getting small businesses to understand where their risks are and what simple steps they can take to actually deal with them.

Mr. Sven Spengemann: I'd just like to take the remaining minute and a half I have to ask you about what levers you see in the hands of government, other than regulation, and specifically about your thoughts, if you have any, on public-private partnerships in augmenting our baseline security infrastructure for the private sector.

Dr. Satyamoorthy Kabilan: Certainly the public-private partnership route is, I think, one that needs to be explored, because no one sector, on its own, has all the answers.

Again, organizations like the Canadian Cyber Threat Exchange have attempted to do this. They have brought government in, and they've tried to work with the private sector. But it's bringing the two together.

There are some capabilities in government organizations like the Communications Security Establishment. They have some fantastic capabilities and knowledge, but equally—and you mentioned this—these large financial institutions are investing in cybersecurity, so they do have knowledge and they do have capabilities of their own. If those can be brought together, the sum of the whole will be much greater than the individuals acting on their own.

Mr. Sven Spengemann: Thank you. Again, that was extremely helpful.

Mr. Chair, do I have any time left?

The Chair: You have 15 seconds.

Mr. Sven Spengemann: I think I'll pass it over.

Thanks very much.

The Chair: In those 15 seconds, I'll ask you one question. When I was in NATO last week, a presenter talked about the Norway model, in which all of the information comes to one location. Are you prepared to comment on that?

Dr. Satyamoorthy Kabilan: I'm not 100% familiar with the Norway model, but if you're talking about a central hub where everything comes in and everything is scrubbed or protected, on the one hand, you have a great advantage in making sure you have central control over everything. The flip side to it is that if that hub goes down, everything goes down.

The Chair: Good. Thank you.

Mr. Motz, you have seven minutes.

I hope our security people have a really good reason for why our witness is not here.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): I just sent Sean down and he said he—

The Chair: I sent my Shawn down too.

Mr. Glen Motz: Okay, Sean and Shawn should be able to handle it. He said he should be here in a couple of minutes, so hopefully—

The Chair: It's been a long couple of minutes.

Mr. Glen Motz: I can start my questions, if I may, Chair. I could slightly adapt Mr. Leuprecht's questions as well.

Sir, thank you for being here.

One of the questions I have for you, given your background, is whether you can explain for us some of the vulnerabilities that exist currently with the IoT technology, the Internet of things technology. I don't think people really understand the vulnerabilities that exist there. Can you explain those for us?

Dr. Satyamoorthy Kabilan: The Internet of things is a rather interesting phenomenon. Just to go back a little bit, what's happened here is that it has become cheaper and cheaper to basically put a microchip into things—

The Chair: Mr. Motz has very graciously said he'll defer at this point, so we'll restart Mr. Motz's clock when Professor Leuprecht settles himself in.

I'm sure you have some negative commentary on our level of security.

Dr. Christian Leuprecht (Professor, Department of Political Science, Royal Military College of Canada, As an Individual): We all make do with the resources we have, right?

The Chair: All right.

You are a veteran witness before this committee and others. We look forward to what you have to say in the next 10 minutes.

Dr. Christian Leuprecht: The submission is more than 10 minutes, so I'll just highlight a few points. I tried to make sure I circulated it beforehand so we can go into some of the other issues.

[*Translation*]

As always, it will be my pleasure to answer your questions in both official languages, but I will be making my presentation in English.

[*English*]

There are five different elements that I was asked to comment on in regard to the range of cyber-threats that are facing the financial sector.

Here particularly, I highlight the ones that derive from the Internet more generally, including online banking, financial transfers and whatnot, and also the threats in particular to the SWIFT network: the vulnerability of the Internet as a whole, all the electronic transfers, and then the vulnerability of banks in particular to detect money laundering—know your customer—and the large-scale financial money-laundering issues that we have. I list some of those here in my brief. There are also the dangers that emanate from the SWIFT network, with Canada obviously being tied into the SWIFT network.

There are some recommendations here supporting the cybersecurity needs particularly of small and medium-sized financial institutions, something that I think is often overlooked as we focus only on the large entities.

Also, Canada must develop a policy response for rebuilding the financial system's technological infrastructure in the case of a major failure. I think we have not quite figured out the relationship between government and private industry if the entire system did go down and we actually needed government intervention and the expertise of some of our colleagues around town in order to bring the entire system back up.

We need the ability to publish warnings of retaliatory attacks and to pursue hackers in all available avenues under domestic and international law, all of which I think we can be much more aggressive at.

Second, I'll comment briefly on the sector-specific vulnerabilities and mitigation efforts.

The banking sector in particular is vulnerable to insiders. This applies not only to physical insider threats, but also to people who provide insider threats inside the organization with regard to moving and laundering money. It's estimated that about $2.5 trillion is laundered around the world each year, much of this electronically, including—as you know from our own case in Vancouver in recent days—a substantial amount through our own country.

Banks need to take responsibility for the consumer losses, as they do, but they have significant incentives not to do as much as they can. In the trade-off between convenience and security, they'll always go with convenience, because that's what the customers want, and we're not convinced that banks are being forced by government to pay sufficient attention to that trade-off. When banks are robbed in a cyber-attack, they have currently no incentive to disclose it, which means that everyone else is vulnerable to the same sort of attack. There are also reputational risks.

With regard to recommendations, they include developing a policy framework to mitigate consumer losses from risky behaviour, both at the institutional level and at the individual level; supporting the nascent cybersecurity industry in Canada, where I think there's a lot more that government can and should be doing; developing policies to incentivize data analysis of bank data for cybersecurity purposes; and encouraging more government collaboration among law enforcement, FINTRAC and financial institutions, including bestowing an enforcement capacity on FINTRAC.

Third, there are infrastructure interdependencies. These arise through the fact that the Internet does not respect boundaries, so information held by businesses such as banks is particularly vulnerable to data outages, data breaches and interruptions to communications in other countries, which are either accidental or deliberate. The SWIFT network, for instance, has had multi-hour outages. Financial institutions are motivated to keep data about customers and transactions in national repositories, and it's difficult to ensure this with the way the infrastructure is currently set up. Because of how distributed the infrastructure is, Canadian data are vulnerable to data breaches in jurisdictions outside of Canada, where regulations are weaker.

Bank infrastructure of communication systems.... The nature of the current system, with considerable extension such as 5G, means that vulnerabilities can only be hardened but not avoided. The recommendation here is that Canada should pursue a sovereign data localization strategy, reinforced by legislative and tax incentives to require critical data to be retained only in Canadian jurisdictions; set clear standards and expectations for the resilience of Canadian communication infrastructure; monitor that resilience; and impose penalties on critical communication infrastructure players who fail to adhere to standards or fail to make adjustments without which they would be left vulnerable.

● (1550)

Fourth is the role of communications service providers in threat detection and threat mitigation. This is where telecoms play a particularly important role. I cite here also the example of the deep packet inspection that CSE, for instance, uses to protect government infrastructure. Two issues prevent this from being fully exploited. First, the level of detection is so expensive that there's little incentive for telecom providers to get into that business. Second, telecom providers consider that amelioration, once detected, legally problematic. One of the interesting curiosities is that telecom providers in Australia have been much more willing to be proactive, even though their legislative regime is almost the same as Canada's. These widely different outcomes between Canada and Australia, I think, warrant further examination to see what can be learned in order to achieve the outcomes that Australia, under the same legal regime, is achieving.

The recommendation is that government should clarify the opportunities and obligations of telecom providers with respect to detecting and ameliorating communications that have the potential to do harm. Government should devote more resources to cybersecurity research. We already have a number of world-class capacities, including in quantum computing and cryptography, but there's much more need. The demand for highly skilled personnel vastly outstrips the supply. Unlike Australia, there is no strategy in this country on how to generate those human resources in terms of highly qualified personnel.

Finally, there are issues relating to entities participating in the Canadian economy and telecommunications infrastructure that may be subject to extraterritorial direction from foreign governments. Two parts of the information infrastructure contain inherent unfixable vulnerabilities—the network switches that form the backbone of the Internet and the consumer devices themselves. The network switches necessarily see all the traffic that they direct. If this traffic is not encrypted or is weakly encrypted, such switches may be able to detect everything that passes through them. Even if the traffic is strongly encrypted, the patterns of communication cannot be hidden from the switch. This traffic analysis is revealing. Switches can also control how they manage communication by delaying it, by cutting it off completely, or by diverting traffic.

The hardware and software of a switch can be analyzed for built-in vulnerabilities that might have been inserted. However, it needs to be possible to update the software in a switch from time to time, so each switch possesses a mechanism to “call home” and allow it to check and to get updates from remote locations. Policing this update mechanism is extremely difficult. The routing technique of the Internet uses tables that tell each switch which outgoing link to use to reach each eventual destination. These tables themselves are a vulnerability. There were several recent incidents where large amounts of traffic were misdirected through the territory of a particular state. Such consumer devices as cellphones have an inherent vulnerability, because they must see key process and display information, even if the data is encrypted for the rest of its existence. The manufacturers of such devices are in a position to see all of the input and output even if the storage of the device and all of its communications are encrypted. Such devices are routinely used for banking transactions and capture financial details. Transactions can, in principle, be captured.

Here are the recommendations. First, the government should ban such telecommunications providers as Huawei from participating in the development of 5G network infrastructure. In our view—I stress here that I wrote this brief with a colleague in computer science and a colleague in law—the government should ban Huawei from participating in the development of Canada's 5G mobile infrastructure. As a result of a recent change in a Chinese law, China can request any domestic company, including Huawei, to assist it to support national interests, including intelligence interests.

A related concern is that China and its industries are suspected to engage in industrial espionage on a large scale as an inexpensive means of R and D transfer. Moreover, Huawei and the ruling Communist Party appear interwoven in many important fashions, including via state subsidies of reportedly $10 billion in a single year. The systematic theft of IP, along with the massive state subsidies, made it impossible for such competitors as Nortel Networks to compete, and ultimately helped precipitate the demise of Canada's premier high-tech company. Since communications are a critical infrastructure, the government should be excluding wholesale any foreign entity with suspected ties to any country where strong evidence exists of significant prior IP theft or intelligence gathering.

● (1555)

For the sake of Canadian security, Canadian industry and Canadian research, Canada has a strategic interest in supporting our allies and banning foreign entities that they find undermine their national security interests. In doing so, the Canadian government would join not only its Five Eyes partners, including the United States, Australia and New Zealand, but a growing list of other allies that have already taken the step to ban—or are actively looking at ways of excluding—Huawei from their 5G and communication networks, including Japan, South Korea, Germany, France, the Czech Republic and Poland.

Furthermore, the evaluation board of the Huawei Cyber Security Evaluation Centre, set up jointly between the entity in question and GCHQ in the U.K., has become even less certain about this entity and its product security implications, with U.K. and French telcos actively replacing that equipment in their critical communications infrastructure.

In this matter, Canada appears increasingly out of step with key allies, and dithering carries reputational risks for Canada's perceived reliability as an ally, as well as for Canada's integration into the North American and allied communication infrastructure. Canada already opted to exclude this foreign manufacturer from critical infrastructure years ago. It should do likewise for the national grid.

● (1600)

The Chair: Thank you, Professor Leuprecht.

It was not a 10-minute presentation, but given your frustrations with security around here, I felt that you should be given some discretion.

Mr. Motz, you have seven minutes, please.

Mr. Glen Motz: Thank you, Chair. I'm going to go back to the question that I asked Mr. Kabilan.

Can you explain the vulnerabilities that exist in the IoT technology?

Dr. Satyamoorthy Kabilan: Going back to what I mentioned about the Internet of things, the way this has developed is that it's become cheaper and cheaper to literally build and place a tiny little computer into anything. That means you can have a smart fridge, which I don't want, because my wife will know how much beer I'm drinking.

Voices: Oh, oh!

Dr. Satyamoorthy Kabilan: However, what happens with this is that it is about low cost, and security comes at a cost. If you're trying to make something as cheaply as possible, that's the first thing that tends to drop off your list.

These things are pervasive. You can get them anywhere and everywhere. Now, if you think about it, when you aggregate a bunch of very small computers, they can't do much on their own, but they have no security. You can take them over very easily, and also, because they are doing things such as monitoring your home, they'll know when you're in and when you're out. If they're on a camera, they might know what you're typing in as your password. Add that to the fact that if you pool all of them together, these little computers suddenly become a gigantic supercomputer.

I believe that in the fall of 2016 there was an outage across the east coast that affected some of the major social media companies such as Twitter and some other major websites. It was essentially a large-scale denial of service attack. What one organization had done was to look at all of these poorly secured devices, pull them all together as a gigantic hammer, and literally hit what was essentially a major address provider in the Internet. That caused one of the largest outages ever, and to this day I think it's still the largest denial of service attack we've ever seen.

With cheap devices, therefore, security is compromised, but this is everywhere. It's in everything. When roped together, it can be pretty impressive and dangerous.

Mr. Glen Motz: Thank you for that analysis.

Dr. Leuprecht, thank you for your testimony. You are most likely aware of a joint study by the U.S. Naval War College and Tel Aviv University where they found that China was rerouting Internet traffic from Canada and the United States through their own servers in both Canada and the United States before it was sent out. To date, the only response from our current government is that, as best they can, they'll raise this issue with China. That's what they've told us.

How would you classify that sort of tactic by a foreign entity? Is that espionage? Is that a cyber-attack? In your own experience, what is that?

Dr. Christian Leuprecht: The challenge with these interventions is that they don't meet the threshold of force, so we don't have an international regime under which we could ultimately classify what this constitutes. It's clearly an exploitation of our network, and it hearkens back to the problem with the vulnerabilities of the network. This is rerouting of traffic by effectively recoding DNS servers. It shows the vulnerability within the network as a whole.

The network works on switches. There are only a certain number of top-level switches. Each of the telecom providers has a very small number of these top-level switches. The closer you can get to these top-level switches, the more you're able to capture traffic or to reroute traffic. Currently, what our adversaries have to do is to try to get as high as possible into these switches, including physically co-locating their own servers on the same premises as some of the large telecom companies.

We would hope that telecom companies would be watching out for that, but we don't actually know whether they're making sure that, for instance, adversaries aren't renting the floor space below or above to hook into those switches physically.

Currently, the problem is that you actually have to capture the traffic by having a server that captures traffic in and out, or you have to reroute using the DNS servers. You can do that only for a certain period of time, because eventually people will catch on, so you do this strategically when you're trying to capture particular communications.

The problem now is that if you have an adversary entity's technology in the system itself, they no longer have to get to the top-level switches, because everywhere in the system you now have a vulnerability. As opposed to rerouting traffic, they can now capture all the traffic they want.

● (1605)

Mr. Glen Motz: We've heard comparisons—and this is for you, Mr. Leuprecht—between the current state of cyberwarfare and what before was called the Cold War. We're facing millions of attacks, sometimes on a daily basis, against our critical infrastructure, which are below the level that would warrant a full-scale retaliation, as you mentioned previously, but they're damaging to individuals, to corporations and to government.

Can you explain the position that this puts Canada in and what we should be doing about it?

Dr. Christian Leuprecht: There are two vulnerabilities here, and I actually think we're much closer to cyberwar than people think, precisely because of these vulnerabilities. One is that our adversaries overestimate their capacities in this space. As a result of overestimating their ability, because they're being told by their signals intelligence agencies and whatnot that they can do this, they underestimate the response. So the uncertainties include, for instance, how the other side might respond and the targeting of these, if you want to call it that. These information weapons can easily get out of hand and get into other types of systems.

We, as a result, have difficulty gauging at which point a cyber-attack might either trigger a conventional response or have a cascading effect that would have conventional implications for us here in Canada, at which point we might, for instance, decide that this warrants a conventional response.

I have a whole separate paper on this, which I'm happy to share with the committee, but I actually think the uncertainty in this space is deeply troubling because it creates all sorts of potential for misperceptions and escalations, which we have no international framework to handle.

Mr. Glen Motz: I would certainly welcome having that paper submitted to the committee.

The Chair: If you wish to submit it to the committee, I'm sure the committee would be willing to entertain that.

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

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

I want to come back to the concept of—it feels like a big word but it's been brought up—warfare and the term “hybrid warfare”, which I believe you used as well. I want to come back to the supply chain a bit, because, without getting into specifics of individual companies and such, there is this question of...especially because I think that a lot of us, including those of us around this table, don't really understand the implications of 5G and it's been talked about a lot.

One of the issues is the ubiquity of things like smart homes and all kinds of things like that. You used the example of fridges. There's this issue that is coming up. You said you wouldn't attack the bank but you'd go after the individual. In that respect, is there a concern that because, for example, there are things being made in China, you might remove them from developing 5G by a company from there, but then the next thing you know, they're still involved in making the cellphone, for example, even if it's an iPhone or something like that?

What concern is there about the actual items themselves connecting to the network? The network might be secure, but for the individual items—household items that we'll now be using, the self-driving cars, and all of these things that are being talked about as the reasons that 5G would be helpful—we do not actually have any security protocols in place. I'll put the question to both of you, if I may.

Dr. Satyamoorthy Kabilan: This is classically what we call “end point security”. Literally, it's the end point of the Internet.

Let's just step away from the question of who provides this, just for a moment. Whatever is on that end point, if it isn't secure, no matter how good your network is, you've just created a major vulnerability. If you go back to the analogy I gave earlier about transfer of money—armoured cars and armed guards between two cardboard boxes—that's what you get. You might have secured the chain where the information sits, but the problem is the vulnerability at either end.

Regardless of who provides it—and there are providers from all over the world who fall into this category—when we look at the Internet of things more broadly, because security is an afterthought and it's expensive, it doesn't get incorporated. What you've described is exactly correct. No matter how secure the network is, that immediately creates a vulnerability, and that can allow someone to penetrate the system and get into your home network, for example.

The classic story that a friend of mine who used to work for the U. S. government used to tell me was that he always waited for someone to buy that wireless printer, because it was great. You didn't have to connect to it—this was 20 years ago, when these things first came out—but it immediately broadcast a signal that allowed you to penetrate the system and get in. His job was protecting the U.S. government from these threats, but that was his description.

● (1610)

Mr. Matthew Dubé: It has since been revealed that those printers are problematic—

Dr. Satyamoorthy Kabilan: Exactly.

Mr. Matthew Dubé: —if you think of a law firm printing off documents for court proceedings that are confidential and such.

I want to hear the other piece of that, but I want to focus quickly on what you said about the affordability piece as well. In other words, a lot of this technology is expensive, but as the only option.... Let's say you want a doorbell in your home. You won't be able to find a traditional doorbell, only one that has a camera and leads to a phone application. There will be a race to the bottom, price-wise, and that will inevitably, as I understand from your perspective, lead to security concerns. Is that a fair assessment?

Dr. Satyamoorthy Kabilan: It's a fair assessment, particularly if price becomes the only discriminator, but we've seen industries or marketplaces where we've actually managed to address some of these problems.

Think about car theft. As you can tell from the accent, I'm British. In the U.K., one of the ways in which we dealt with this was that the government put up a table of the cars that are stolen most often. That changed things immediately. It didn't matter if the car was cheap or not; that meant your insurance would go up and you were more likely to lose the vehicle. It was able to provide that ranking.

Even if we're in a race to the bottom—and it isn't about providing the expense—sometimes just the information can change behaviour and change consumer choice. Yes, there's a price component in this, but it needn't be the only determinant of whether or not you get good security.

Mr. Matthew Dubé: Okay.

Professor, go ahead.

Dr. Christian Leuprecht: We know how to make devices and phones more secure. It's a matter of actually stepping up and making that a requirement. I can walk you through all the technical premises behind this.

It continues to amaze me that in this industry, in the applications it uses, when you download an app and you read the long description that nobody ever reads, you essentially say that you're willing to use a faulty device and will put no liability and no responsibility on the manufacturer of that device. In what other industry has government decided that the manufacturer basically can completely absolve himself or herself of any responsibility for any faults in the product, even when those are known faults, or for the inability or unwillingness to patch those because the security concerns are more...and also because the app might no longer run on all sorts of different devices or whatnot?

I think this is simply irresponsible. I think that's where government needs to say, no, you can't manufacture technology that is knowingly insecure and knowingly faulty and then make the consumer responsible for using that technology.

Mr. Matthew Dubé: I wanted to quickly touch on the cyberwarfare piece with Bill C-59, for example, and CSE having the active cyber capabilities. My understanding is that there is not really any clarity in international law. Some would argue that when you attack a country's sovereignty.... Is data a part of sovereignty? I think that's the uncertainty we're at now.

There's a risk of escalation, but does it go both ways? Even with the announcement today, for example, on fighting foreign interference, if there's any kind of disruption that's being done proactively or pre-emptively, is there a risk there that we might antagonize while trying to protect ourselves if there's no action from a foreign state actor prior to whatever action our agencies are taking?

Dr. Christian Leuprecht: I think there are four categories that we need to think of. It hearkens back to your earlier question. I think the lowest level is the propaganda level, which is equivalent to graffiti on the wall, taking down a website, or something like that. Then you have subversion, sabotage, and attack. Attack is really the only time when it might need a threshold of force.

I think these four different levels, the three below attack.... As a government and as a state, we haven't really thought about the implications with regard to how we might retaliate, who gets to retaliate, and who gets to decide when, where, and under what conditions. Who's involved in that retaliation? Do we allow a private sector to retaliate? Is it solely a state responsibility? And we can clearly define, or fairly clearly define, the boundaries between the propaganda, the subversion, and the sabotage piece.

● (1615)

The Chair: We will have to leave it there, Mr. Dubé. Thank you for that.

Ms. Sahota, you have seven minutes, please.

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

My first question is for you, Mr. Leuprecht. You advocate for a sovereign data location strategy. That would require critical data to all be located and stored in Canada. Can you define what "critical data" is and how that would work?

Dr. Christian Leuprecht: There are four different strategies that countries can take with regard to data.

Maybe I will make a separate submission to explain, because it might take up too much time.

Ms. Ruby Sahota: Okay.

Dr. Christian Leuprecht: There are only four strategies that countries can pursue. I think that, given the disproportionate advantage Canada has with the number of data farms that Canada already houses—we're in a cold climate and we have lots of relatively cheap electricity, so lots of private players are already putting their data farms here in Canada—we actually have the ability to do this in a way that other countries might have much greater difficulty doing. It means that not only are those data then subject to Canadian law, but we are also able to impose requirements on industry that industry can then verify by virtue of those data continuing to be located in Canada rather than being farmed out throughout the world.

Ms. Ruby Sahota: So you're saying we definitely have the capacity to do that.

Dr. Christian Leuprecht: We have the capacity to do that; it's just a question of.... That's why I say that some regulation and tax incentives and whatnot can help in that regard.

Ms. Ruby Sahota: I've read some comments about our investment in AI and Canada becoming an AI superpower. This government has definitely taken a few measures in terms of investing more money. Minister Bains has made several announcements in the last several months when it comes to supporting AI technology and different companies. Can you elaborate a little bit on the previous comments you made?

Dr. Christian Leuprecht: AI is not this sort of fantastic, magical hat we pull a rabbit out of and whatnot. I mean, AI is just math. It's just fancy, sophisticated math and its applications. While the government has invested significantly in various applications of that, the irony is that the government has not made an investment in the cybersecurity side of those applications.

We're generating lots of highly qualified personnel—"HQP", as we call them in academia—but we have a massive disconnect between the cybersecurity side of generating the people who are in demand and our ability to have programs that will generate those in universities. We're doing lots of great, fun research, but it's not directed at generating cybersecurity talent.

I would bring up Australia again. They have nine different centres now that deal with cybersecurity. In Canada we really have none. We run our Smart Cybersecurity Network, SERENE-RISC, which we stood up with a colleague at the University of Montreal, but that's about it. I think we need to do a lot more. We can buy all the technology we want and we can make all the investments we want, but if our adversaries are simply going to steal all of our R and D investments, at billions of dollars a year, what's the point of putting money into R and D? And why, as a foreign company, would you invest in R and D in Canada, or in our AI investments, if you knew that we couldn't keep secure the intellectual property generated?

● (1620)

Ms. Ruby Sahota: Okay.

We had a witness just at the last meeting. Public Safety is working on creating a cybersecurity centre and also, within Defence, Minister Sajjan launched, last October I believe, the Canadian Centre for Cyber Security. I was wondering if I could get some of your views on that, Mr. Kabilan. I believe that's something you said you have also taken much interest in.

Dr. Satyamoorthy Kabilan: Certainly. The cybersecurity centre I believe you're alluding to is what's going to be spun out of CSE eventually, and I think you have Scott Jones coming in after this to talk about it. When I've discussed this with the government, I've talked about the analogy with what the U.K. has done with the National Cyber Security Centre. I see, certainly from the submissions and from the various discussions that have been had around this new centre in Canada, that it's trying to mirror a lot of what the National Cyber Security Centre does in the U.K.

Just to give you some context, I mentioned earlier that education and information are two big key elements when it comes to cybersecurity. That's what the NCSC in the U.K. does very, very well. It helps to bridge that disconnect between the public and the private sector in terms of getting information across, but it also does it in a way that's accessible to anyone. It gives advice to you personally; it gives advice to small and medium enterprises, and it goes all the way to the high end. My understanding is that this new centre in Canada is going to mirror some of that functionality. If it can, particularly in that education and information sharing piece, then it will be an incredibly valuable tool in terms of helping us build our capacity and our resilience to cybersecurity threats.

However, the challenge is with what Dr. Leuprecht brought up just now, which is the idea of skills. In the U.K., the NCSC actually runs competitions as well. It gets, for example, young women to come and code, and that actually helps to bridge the gender gap. What I haven't seen clearly is some of these elements to address the questions that Dr. Leuprecht brought up about not only sharing information but also using that as a platform to build the required skills to continue to support the development of cybersecurity in Canada. It will be interesting to see how that develops.

Ms. Ruby Sahota: Do I have any more time?

The Chair: You have one minute.

Ms. Ruby Sahota: In terms of skills development, we heard this in the last meeting as well, and for some of these jobs, government prefers to hire trained Canadians because of the security that's required. How do we go about doing this with our academic partners in order to create more centres, like those Australia has, and follow in the footsteps of the U.K., which you speak highly of as well? How do we establish that without government doing it all?

The Chair: Be very brief, please.

Dr. Satyamoorthy Kabilan: There are a couple of different challenges there, but I think the first issue is—and I think Dr. Leuprecht would be able to answer this more fully as well—making sure there's a chain that works all the way from education to the job at the end. We actually have some very good examples here in Canada, in fact one here in Ottawa, which is Algonquin College. They actually produce some great cybersecurity graduates. They have a program, and a big chunk of them get hired by CGI directly.

The Chair: Thank you.

Dr. Satyamoorthy Kabilan: We're actually producing the skills and getting them hired. It's about getting that pipeline aligned.

The Chair: Thank you, Ms. Sahota.

Mr. Paul-Hus, you have the final five minutes.

[*Translation*]

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

Mr. Leuprecht, you spoke at length about Huawei and the risks that it presents to the security of Canada, due to several factors. The document you tabled contains several recommendations that are important for the committee. It mentions the Huawei Cyber Security Evaluation Centre.

Is this a group of enterprises? What exactly is that evaluation centre? Who is a part of it?

Dr. Christian Leuprecht: The centre is a collaborative effort between the United Kingdom Government Communications Headquarters, or GCHQ, and Huawei. Its purpose is to strengthen links with Huawei and give the GCHQ the opportunity to verify the security of that enterprise's equipment. Despite that collaboration effort, a public report, which I can send to the committee, still came to the conclusion that Huawei products are suspect.

Mr. Pierre Paul-Hus: So after having worked with that company, that was the final conclusion.

There is a debate in Canada at this time as to whether we should continue to do business with Huawei. According to certain interest groups, it is very important for Canada to adopt 5G technology because it is superior technology, but in your opening statement you said that that technology presents a risk to national security.

We are not experts, but we hear a lot about this. You are a professor at the Royal Military College of Canada, and other experts throughout the world agree with you. Could you explain to us in simple terms why we need to get rid of Huawei technology?

● (1625)

Dr. Christian Leuprecht: In the interest of clarity, I will answer in English.

[*English*]

I think there are a couple of key risks. One is the pyramidal structures of the switches within the Internet. The higher up you are in that pyramid, the more traffic you can extract from the Internet. Currently, our adversaries have to try to get very high up in the Internet to extract as much traffic as they can. In the absence of that, they will reroute traffic. If the technology is embedded throughout the entire Internet, you don't have to make an effort to get at those switches anymore. You can just extract the entire traffic from the infrastructure as is.

The other problem is that even though we might test the technology,

[*Translation*]

—and this technology seems entirely safe to us—but we have to be able to update it. That is the problem.

[*English*]

There's always the ability for the manufacturer or an adversarial government to reach into that technology and, in the update process, install vulnerabilities in the technology. As for anything in life, it's an insurance policy that we take out.

Look at the November release by the joint congressional commission for the common defence, co-chaired by Ambassador Edelman. In its report, which you can download from the United States Institute of Peace, the commission concludes that if the U.S. today got into a war with Russia, China, or both, the U.S. would likely lose. Why? Because the war would start with a massive attack on the vulnerabilities within the critical infrastructure of, let's say broadly, the national grid; I don't mean just electricity. As a result, it would create such vulnerability, chaos and instabilities within the country that the U.S. would not have an opportunity to respond. It sure was a wake-up call in the United States. Countries such as China reserve the privilege of a first strike when it comes to cyberspace. This is part of the Chinese doctrine.

How much vulnerability and risk are we willing to expose ourselves to as a country? If we find ourselves in that situation, then it's a little late to go back.

Mr. Pierre Paul-Hus: Thank you.

The Chair: Thank you.

I hate to bring this to an end. This has been absolutely fascinating. I'm sure we could go on for a while.

On that last question, let me ask one brief question. Is it beyond the realm of possibility that a cyber-attack could trigger an article 5 NATO response?

Dr. Satyamoorthy Kabilan: It has been hotly debated whether or not it could. The EU had a session on this in 2017. The answer was, “We don't know.”

The Chair: That's comforting.

With that, I think I'm going to have to bring it to an end. I regret having to bring it to an end.

We're going to suspend and then re-empanel.

Again, on behalf of the committee, thank you both.

● (1625)

(Pause)

● (1630)

The Chair: We're welcoming Scott Jones and Eric Belzile back to the committee.

Mr. Jones, your last appearance was quite popular. I'm anticipating that this one might be equally popular. With that, we'll look for your presentation, between the two of you, for 10 minutes.

Thank you.

Mr. Scott Jones (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Good afternoon, Mr. Chair and members of the committee.

It's a pleasure to be here again, I think. I guess I was just scrummed, so I got a little taste of what your lives are like.

As you know, my name is Scott Jones and I'm the head of the Canadian Centre for Cyber Security, which is a change from the last time I was here. The launch of the cyber centre was imminent. I am joined today by Eric Belzile, the director general of our incident management and threat mitigation team.

Launched on October 1, 2018, the Canadian Centre for Cyber Security is a new organization but one with a rich history. The cyber centre brings together operational cybersecurity experts from across the Government of Canada under one roof.

[*Translation*]

In line with the National Cyber Security Strategy, the launch of the Canadian Centre for Cyber Security represents a shift to a more unified approach to cyber security in Canada. The Canadian Centre for Cyber Security continues the work of the Communications Security Establishment's (CSE) IT security mandate. It provides advice, guidance, and services to federal departments and agencies and other systems of importance to the Government of Canada.

The Canadian Centre for Cyber Security also keeps Canadians safe in cyberspace by providing easily accessible information on cyber security matters, as a single, clear, and trusted source of information. With the amalgamation of parts of Public Safety Canada and Shared Services Canada, the Canadian Centre for Cyber Security continues the work of these departments to encourage collaboration with other levels of government, the private sector, and academia.

[*English*]

Our partnerships with industry are vital. Governments everywhere are simply not able to keep pace with the rapid innovation that the private sector is able to bring to bear. The Government of Canada cannot improve cybersecurity for Canadians without collaborating with the private sector.

This brings me to the specific topic of today's discussion: cybersecurity in the financial sector as a national economic security issue.

A significant disruption to the financial sector could have effects that reverberate across Canada's entire economy. The effects of a cyber-disruption could be immediate, such as financial loss, or they could occur over the medium to long term in the form of decreased consumer confidence. The risk of a cyber-compromise increases as the financial sector continues its transition to digital services and connects more devices to the Internet.

Nevertheless, this digital transformation has the potential to create tremendous opportunities for growth. To not leverage innovations in digital technology would mean being left out of the global economy. Retrenchment is not an option.

● (1635)

[*Translation*]

To this end, Canada needs to remain vigilant and take action to prevent, detect and respond to cyber threats to the financial sector, and all sectors of Canada's industry.

In this effort, the Canadian Centre for Cyber Security was proud to release Canada's first National Cyber Threat Assessment in December 2018. This assessment describes our view of the current cyber threat landscape in Canada. The intent is to ensure that as cyber threat actors pursue new ways to use the Internet and connected devices for malicious purposes, Canadians are well informed of the cyber threats facing our country. The assessment includes several key judgments on the current cyber threat environment, including that facing Canada's financial sector.

[*English*]

First, we assess that cybercrime is the cyber-threat most likely to affect Canadians and Canadian businesses in 2019. While all businesses are at risk, the financial sector is a frequent target of cybercriminals.

In a survey on the impact of cybercrime on Canadian businesses, researchers at Statistics Canada found that nearly half of Canadian organizations in the banking sector were impacted by cybersecurity incidents in 2017. Cybercriminals can target the financial sector, such as banking institutions, for immediate financial gain, but they can also target this industry for data about its customers and partners or for proprietary information. Stolen information is often held for ransom, sold or used to gain a competitive advantage.

These incidents can result in major financial losses and can also result in reputational damage, productivity loss, intellectual property theft, operational disruptions and recovery expenses.

[*Translation*]

More sophisticated threat actors, including nation states, could also target the financial sector for its value as one of Canada's critical infrastructure sectors. However, we assess that at this time it is very unlikely that state-sponsored cyber threat actors would intentionally seek to disrupt Canadian critical infrastructure. While the financial sector is an attractive target for cyber threat actors, it is also a relatively hard target.

[*English*]

Indeed, in its 2017 survey, Statistics Canada found that two-thirds of banking institutions had a policy in place to manage or report cybersecurity incidents. The Canadian Centre for Cyber Security also plays an important role in helping to protect systems of importance to the Government of Canada.

We currently have ongoing and tailored initiatives with partners in Canada's financial sector. For example, the cyber centre regularly shares reports on indicators of compromise with critical infrastructure providers, including partners in the financial sector, with the goal of promoting the integration of cyber-defence technology.

When looking at what Canadians and businesses can do to protect themselves from cyber-threats, it is important to remember that adopting even basic cybersecurity practices can help thwart cyber-threat actors. Cybersecurity is everyone's business.

Thank you. I look forward to your questions.

The Chair: Thank you, Mr. Jones.

Ms. Damoff, please, go ahead for seven minutes.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you, Chair.

Thank you for your presentation.

I want to start with a comment you made that two-thirds of financial institutions have a policy to report cybersecurity breaches. Is that what you said? What about the other one third?

Mr. Scott Jones: The Statistics Canada survey found that two-thirds of organizations had a policy in place on how to report, and I would imagine that has been filled in as boards are starting to ask more questions around cybersecurity and cyber risks that organizations face.

Ms. Pam Damoff: Should financial institutions in particular have a requirement to report incidents?

Mr. Scott Jones: We're concentrating on building the relationship so they feel comfortable approaching us quickly at the start when they're not even sure they have an incident yet, so we can start to work together to react. We're trying to encourage them to report while it's in its early stages so we can engage quickly and hopefully provide assistance before it becomes a compromise.

Furthermore, the earlier they report and the better information we get, the more we can share with the entire sector, and that's really important to us from an incident management and threat mitigation perspective.

Ms. Pam Damoff: In my capacity as a member of the committee, I've met with a number of cybersecurity firms that advise businesses, governments and financial institutions, and one of the things they talk about is a number of different kinds of accounts. Some are left open when people leave a firm. Some are rogue accounts when somebody comes into an organization and creates an account that just sits there for years. Companies don't even take stock of what's there. There are accounts that have higher authority than they probably should have. People leave or they change jobs.

How can we educate organizations to be mindful of that, because it seems like a very easy fix to deal with a lot of these vulnerabilities that they're leaving themselves open to?

● (1640)

Mr. Scott Jones: Just so I'm clear, are you talking about computer accounts that people use to log into systems, not bank accounts that are abandoned?

Ms. Pam Damoff: That's right, actual employees who may have access to very high-level secure information and then they take another job or they move to another department but their log-in remains the same.

Mr. Scott Jones: That's absolutely critical. One of our top 10 actions is managing credentials: revoking those credentials when somebody leaves an organization, and making sure that your authorities meet the requirements of your position when you log into a system.

For example, when I log into a system at CSE, I don't have any administrative privileges whatsoever. I can't even change the time on the clock because I don't need that for my job. Our systems administrators take care of that. I can't install software. Our systems administrators take care of that after proper testing. Managing those credentials and making sure they're the most limited set possible is really important, and then for those employees who have elevated privileges, there are other steps that you should take to protect.

For example, if you are a systems administrator, controlling access —what employees can do and how they can do it, what they can do on that account.... One of the easy examples we give is, don't read your email from your administrative account and don't browse the web from your administrative account, because you're operating with elevated privileges. Some simple things can have a remarkably large effect on cybersecurity.

Ms. Pam Damoff: Whom are you saying that to?

Mr. Scott Jones: That's part of our public advice. We say it as part of our top 10. We certainly have been singing this song to government in managing administrative privileges. It's also a standard cybersecurity practice that you would hear from the SANS Institute or other organizations that promote good cybersecurity hygiene.

We certainly talk about it. Doing the basic top 10, even the top four of the top 10, has a remarkable effect on improving your cybersecurity.

Ms. Pam Damoff: Are organizations listening to you?

Mr. Scott Jones: In a lot of cases, they absolutely are. Certainly we've seen a significant change in the Government of Canada over the last five to six years, probably, as we've tried to show the consequence of not following the top 10, and I think businesses, boards of directors, etc., are very much looking for something they can measure their cybersecurity efforts against, so they do use the top 10 to evaluate how they're doing, and they go through them one by one.

Ms. Pam Damoff: Okay. Thank you for that.

Do you have any sense of the cost of cybercrime to the Canadian economy? Has anyone done any research on that?

Mr. Scott Jones: The Statistics Canada survey is probably the best survey we have right now. The issue we have is that cybercrime is one of the most under-reported crimes, so it's hard to tell. If you're duped into, say, clicking on a link or paying for something, etc., there's a large stigma attached to complaining or filing a complaint, and people don't know where to go.

I don't have a hard number. I think the Statistics Canada survey is probably the closest we have right now. One of the things we are trying to promote, in collaboration with the newly formed national cybercrime coordination unit at the RCMP, is, first of all, to encourage people to report crimes to the police so they can take action, and also to start tracking some of those statistics so we can see the impacts on the Canadian economy.

Ms. Pam Damoff: One of the witnesses we had here earlier was talking about consolidating data into one place in Canada. Do you see benefit in doing that? I don't know if you heard it or not.

Mr. Scott Jones: What type of data? I didn't hear.

Ms. Pam Damoff: I think he was talking about.... I don't know. I have only a minute left.

I had a constituent who contacted me, asking a question, and I asked this of the RCMP: If one of our Canadian banks contracts out to another country, and there's a data breach in that country, is it enforceable? The answer I got was pretty wishy-washy: maybe likely not, but it could be. Would having all that information held in Canada and not leaving the country help with something like that?

● (1645)

Mr. Scott Jones: I think the key thing is looking at the supply chain risks. That's one of the things we highlighted in the national cyber-threat assessment. Businesses need to be particularly conscious of the supply chain they're engaging in and the companies they're engaging with, and they need to put proper security provisions into their contracts, so that they can hold them accountable and make sure they get proper breach notification, etc.

Lowest cost is something we always say is not usually compatible with cybersecurity. Businesses need to find the best, most capable cybersecurity firm that can protect their data as well.

The Chair: Thank you, Ms. Damoff.

[*Translation*]

Mr. Paul-Hus, you have seven minutes.

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

Good afternoon, Mr. Jones. We saw each other last September. Everyone wants to know what we are going to ask you about your impressions of Huawei.

Before I continue, I'd like to say that over the past five or six months, I understood certain things and I would like to verify your mandate. For a certain time, I have understood from our conversations that your organization is more of an information centre and that it is not involved in tactics and strategy. I think that your role consists more in informing Canadians. Is that correct?

Mr. Scott Jones: Thank you for your question.

[*English*]

First, our mandate is to provide advice and guidance to Canadians, but it started off as the Government of Canada, so practical security advice. One of the mandates we've been given is also to ensure that Canadians have the information they need to take action on their own to protect themselves.

With the creation of the cyber centre, that mandate was expanded with the consolidation of the CCIRC, the Canadian Cyber Incident Response Centre, which had the role of the national CERT, the national Computer Emergency Response Team, the incident response team.

Our goal is to provide not only advice and guidance but also actionable things that people can take.

[*Translation*]

Mr. Pierre Paul-Hus: There is currently a whole debate going on about the Huawei company. Huawei proponents support 5G technology. Those who are opposed to the company, however, point to issues of national security. Our Group of Five allies tell us that we should not touch this company.

We would like to know if you will be providing the definitive advice to the Prime Minister. Who will decide what we should do regarding this company in Canada?

[*English*]

Mr. Scott Jones: Our role as part of the team and the government is to make sure we give the advice on the cybersecurity aspects. There are other aspects in a decision such as that. The timing has been.... Minister Goodale came out and talked about that yesterday. I think the key thing for us is to provide the advice we need to give, in terms of what the next government decision is. In terms of today, we're implementing the policy decision from 2013.

[*Translation*]

Mr. Pierre Paul-Hus: What is your answer to those who say that we lag behind other countries and that we are dragging our feet? You heard Mr. Leuprecht's presentation; he is a professor at the Royal Military College of Canada and he was very clear on this topic. He is not the only one, because experts from everywhere seem to be saying that this is quite obvious.

As I was saying, from a technical point of view, it is difficult for us to decide. We must depend on people like you to make a decision that is critical for Canada. Do you have enough information today? In September, you said that you were able to ensure the protection of Canadians. Is that still the case today, on January 30, 2019?

[*English*]

Mr. Scott Jones: Our role is to make sure we provide that information and counsel to the government, so the government can make an informed decision. From our perspective, we continue to work with industry on how to protect Canada's infrastructure today and tomorrow, to make sure we're addressing cyber-threats.

[*Translation*]

Mr. Pierre Paul-Hus: So, for the moment, we still don't know if Canada can trust Huawei.

Let's leave that company aside for now and move on to the financial sector, and the banks. Mr. Leuprecht also provided interesting information concerning financial transactions, which can now come from anywhere, since the Internet is global.

According to the CRTC, it's impossible to broadcast Canadian content abroad. When you go to the United States or elsewhere, you cannot listen to TVA, for instance, because that network is not accessible. So, there are certain barriers that exist regarding communications. Why do those barriers not also exist for the banks? Do you know? Do you know why from a technical point of view it is possible to have barriers for one activity but not for another? I don't know if it falls within your mandate to answer that.

● (1650)

[*English*]

Mr. Scott Jones: I'm not sure I quite understand the question. I think the key thing is that, when you're travelling, it depends on whether you can get to the services: for example, connect to your bank. Or is it that—

Mr. Pierre Paul-Hus: Professor Leuprecht just told us that the Internet is an open space, but when we travel, we can't watch Canadian TV, so why can't we block communication between banks or whatever?

Mr. Scott Jones: I think that really goes to it. It is a little bit outside of our mandate, but, fundamentally, we've chosen to have a very open Internet in Canada, where we block very little. Other than specific content providers stopping you from watching, for example, NBC, because Canadian stations have rights, we tend to have a very open Internet. Not all countries take the same approach and some have chosen to filter the Internet and their content. That's just the decision that Canada has made.

The Chair: You have a minute and a half.

[*Translation*]

Mr. Pierre Paul-Hus: In conclusion, I'd like to talk about China. Things are very sensitive at this time. We know that in diplomacy we have to be cautious, but from the point of view of national security, it is a fact that China often has malicious objectives involving various countries, including Canada.

Do you consider China to be a potential threat to Canada's security?

[*English*]

Mr. Scott Jones: From our perspective, one of the things we highlight in the national cyber-threat assessment is that we have to be vigilant against every nation-state, and certainly cyber-techniques are within the realm of every nation-state. Some are more aggressive.

Certainly in the past, CSE has been asked to attribute malicious cyber-activity to certain countries, and that's one of those things that we'll continue to do as per government's broader policy. It's something that we are always looking at, but, for me, we don't defend against only one; we have to defend against everybody. If we take a one-for-one approach, we would be focusing on—

[*Translation*]

Mr. Pierre Paul-Hus: Fine, but do you think that Canada should be frightened of China?

[*English*]

Mr. Scott Jones: I think we should be vigilant against anybody who doesn't hold our values.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

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

Mr. Dubé, you have seven minutes, please.

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

Mr. Jones and Mr. Belzile, thank you for being here.

Ms. Damoff asked you some questions on the banks' policy with regard to reporting breaches or problematic situations. For my part, I want to follow up on the questions I asked the representatives of the RCMP on Monday.

Things were not clear. An update of the law now requires that businesses report information leaks to the Privacy Commissioner. Those representatives told us that the new police centre—I too have forgotten the names and the acronyms—does not have the same obligation, and they are trying to work with those organizations. Is there a duplication of efforts? If a bank reports a suspicious or worrying incident to you, do you also report it to the police, so that they can do work of their own?

[*English*]

Mr. Scott Jones: I think there are a few things. Maybe I'll turn to Eric to talk about some of the specifics. First of all, in terms of our collaboration with the RCMP, we want to ensure that we are never in the way of the police doing their function of investigations and pursuing cybercriminals. That's where we make sure that we're coordinated.

Our role with the banks, with the financial institutions more broadly, is, how can we become proactive against cyber-activity? Our goal is to work to strengthen our defences and to strengthen our information sharing so that we can take action and protect. When there's a specific incident, though, we do protocols a little bit differently.

Maybe I'll let Eric....

[*Translation*]

Mr. Eric Belzile (Director General, Incident Management and Threat Mitigation, Canadian Centre for Cyber Security, Communications Security Establishment): This is what I would add on that topic.

When an incident is reported to us, we work in close co-operation with the other organizations. We do a triage, because there are other organizations that are concerned, like the RCMP and CSIS. Together we determine who will manage the incident. We co-operate so that each organization can fulfil its mandate and functions, and we make sure that we do not encroach on the mandate of the other organizations. This co-operation starts immediately.

This is how we have worked for several years. The consolidation of the Canadian Centre for Cyber Security and the creation of the new RCMP cybercrime centre will also help us improve this co-operation.

● (1655)

Mr. Matthew Dubé: Fine.

I know it can be difficult to make statements on hypothetical situations. Suppose an enterprise reports a suspicious situation to you, but does not report it to the police for some reason, be it public relations, financial consequences or other things. If there is enough evidence to have you suspect that a criminal act was committed, do you inform the police about the case so that can begin an official investigation?

Mr. Eric Belzile: Generally speaking, we consult the victim to determine the best approach. Often, if there are conclusive indications of cybercrime, we advise the victims to report the incident to the police so that they can be aware of it and can exercise their mandate.

Mr. Matthew Dubé: Fine.

You mentioned the report on cyber threats which was tabled. In your presentation, you said the following:

> However, we assess that at this time it is very unlikely that state-sponsored cyber threat actors would intentionally seek to disrupt Canadian critical infrastructure.

Is the threat unlikely only in the financial sector or is that also the case for all critical infrastructure sectors?

[*English*]

Mr. Scott Jones: I think the key thing we were referring to there in terms of nation-states is that they have specific objectives. Absent a major international conflict, etc., we said the threat of disruption was very low, in terms of the threat to Canadian infrastructure, but there is some nation-state interest in private information and in some of the other information that's out there. There are certainly nation-states that use cybercrime tools to generate revenue, especially to get around sanctions and so on.

We always have to be vigilant, and the key thing for us is how quickly we can get information and share information, so that we can take action against any of those types of malicious cyber-activities, but we think the threat of disruption at this time is very low, absent some major conflict. If there is disruption, it's more likely to be a secondary effect of a cybercrime tool—ransomware, for example.

Mr. Matthew Dubé: The other piece I just want to touch on is related to the announcement today on elections. I know that here we're studying the financial sector, but there's another issue I'm wondering about. In the announcement that was made, CSIS seems to be taking the lead with CSE, using its assistance mandate to provide support from that perspective. CSIS is engaged in threat reduction, which is certainly a debate that has been had and that we will continue to have, but not necessarily at this time. Given that we're studying the financial sector, I'm just wondering....

An election is a specific event in time. Time varies, certainly, as we all know. That being said, is there a trend there? Is there a precedent being set for CSIS taking the lead on engaging with actors that might pose a cybersecurity threat, or is this just a one-off for that specific event? For example, if there is a concerted effort in the financial sector—which our study is about—or in any other sector, is this something that's going to be recurring, or is this, again, related to elections specifically?

Mr. Scott Jones: I think the goal is to leverage the Team Canada approach and bring in the proper authorities. Obviously, it's Parliament's role to debate those authorities and assign them to organizations, so I won't comment on that.

For us, the key thing here is that we want to bring in the right authority. At CSE and the cyber centre, we don't direct our activities at Canadians, so if there is a threat emanating from Canada, the RCMP or the Canadian Security Intelligence Service is better positioned to respond.

Mr. Matthew Dubé: Just really quickly, with the 15 seconds I have left, would that structure and who's taking the lead look different if Bill C-59 receives royal assent today?

Mr. Scott Jones: If it's coming from within Canada, that doesn't change. The provision still says that CSE cannot direct its activities against Canadians.

Mr. Matthew Dubé: But in this case, CSIS is engaging foreign actors. That's the understanding I have from the announcement today. Is that accurate?

Mr. Scott Jones: We're using whatever tool is the appropriate one at the time. If Bill C-59 is passed by the Senate, gains royal assent and comes into force, then we would re-evaluate how we approach these problems, given those new—

The Chair: Thank you, Mr. Dubé. We're going to have to leave it there.

Mr. Picard, you have seven minutes.

[*Translation*]

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

Gentlemen, I imagine that when people report cyber fraud or cyber attacks, this confidential information is not made public. Is that correct?

● (1700)

[*English*]

Mr. Scott Jones: That is correct. As we've said repeatedly, we have a tendency to re-victimize the victims of cybercrime. We publish, and we punish them. We're looking for them to take ownership and respond. Our goal is to help them recover, to help them defend, and then to share the information widely.

[*Translation*]

Mr. Michel Picard: According to what I understand, the fact that companies report cybercrime does not necessarily mean that they increase their security or protection systems. They only report the incident.

[*English*]

Mr. Scott Jones: No. However, one of the trends I have certainly seen with larger companies and boards of directors is that cyber-risk is becoming the number one topic. I think we're starting to see that trend now. It is becoming a huge reputational risk, but also a huge business continuity risk to organizations, so they're taking it seriously.

Mr. Michel Picard: Let's see the risk from the business standpoint and the chair of the board's standpoint. When you look at the expenses required for security, there comes a point when you evaluate the expenses needed for the security of the system and the losses caused by the reputational risk compared to the amount you have to pay to reimburse the victims. When reimbursement is cheaper, you forget about security and go for the cheaper way.

Do you discuss this aspect with companies? Do they realize that it's not just a question of losing money, but that, along with the money, there's information attached to it?

Mr. Scott Jones: In our discussions, and the discussions I've had with numerous companies' C-suites or boards of directors, it's very much about the reputational damage. It's hard for them to calculate the cost of that. We certainly saw reputational damage in some of the larger U.S. breaches. I think the key thing for us is that—you're right—the equipment we're buying does not come secure by default. It's very poorly built, and that's getting worse with the Internet of things. That's a dynamic that we have to change, and we're encouraging industry to ask for security to be built in. They shouldn't have to pay extra. There are security features that should come in as part of any piece of equipment.

[*Translation*]

Mr. Michel Picard: Most of our discussions have been about technology to increase our security and protect our information. They have centred on the tools as such. One of the problems we can't get around—and correct me if I am mistaken—is the human factor. It is the only uncontrollable risk faced by any enterprise.

Does this mean that despite the important technology that may not even exist yet, but which may be developed, it will be impossible to protect ourselves because of the human factor?

[*English*]

Mr. Scott Jones: When you look at this, you're absolutely right. The human factor is part of cybersecurity. We tend not to put security on top of our products sometimes if it makes it harder for a user. It's all about usability.

I think part of it is also education, but you can't rely on that. For example, some of the cybercrime tools and some of the cybercrime spear-phishing types of things that we've seen are incredibly sophisticated. Even I—and this is my daily business—could make a mistake. You have to hope for education but rely on further measures that are kind of layered in a security approach, because relying on a person—and certainly, punishing a person—is the wrong approach for this. It is very easy to make a mistake, to click too quickly, etc., and some of them are incredibly well structured.

[*Translation*]

Mr. Michel Picard: What I had in mind was more in the way of a simple error due to distraction. We know the principle of indirect attacks, through software. Our problem is psychological piracy. The person is then deliberately in the system.

For instance, when I was a member of the Canadian Bankers Association, we were presented with an electronic payments terminal that was supposed to be unhackable. But it only took three weeks for that to happen. It was not due to human error, but really to malicious intent from the inside.

What solutions do we have to manage the human factor?

[*English*]

Mr. Scott Jones: I think there are a few. Typically, we would call that the "insider threat" side of things, where somebody who's going....

There are a few ways to do this. Number one is actually the credentials that we talked about earlier—making sure that people can do only the things that are absolutely necessary as part of their jobs, from the IT perspective.

The second one is having a program to look for these types of activities, things that start to spike. If we're a business, we tend to look at fraud detection as something that's being done to us from the outside. Sometimes fraud comes from the inside as well. There are internal losses and things like that, so it's about using some of those tools on the inside.

The third is one of the things with insider threat—and there are colleagues in the government who are probably better positioned to talk about this. It is the care of employees, so that if they get into situations where they turn to crime, there is a better outlet for them. Part of that is how to give them another outlet when something's going badly.

Certainly, from the intelligence side of things, from the CSE internal side, we've spent a lot of time on our internal security program to help our employees so that they don't ever get into situations like that, to manage the insider threat. It's always something you have to be vigilant against, and it is something that is typically overlooked. We don't like to treat our employees like they're criminals.

● (1705)

[*Translation*]

Mr. Michel Picard: We were concerned last Monday when we were told that the means of certain foreign states are far superior to any investment Canada may make to be up to date in high technology.

If we think we cannot invest what is needed to develop the necessary means, do we have to convince private enterprise to become part of the solution by becoming stewards or watchdogs of the market?

[*English*]

Mr. Scott Jones: Right now we're not finding difficulty with the private sector in terms of engagement. They are very willing to come to the table, partner with us, report incidents, work together collaboratively when they see something, or when we see something. I think Canadian industry very much wants to be part of the solution, but to your point earlier, it is expensive. You do have to spend money. If you're running closer to the margins, then cybersecurity is about how to work together to build it in.

We're not seeing an unwillingness for Canadian industry to invest. Sometimes there is a capacity, and certainly not all organizations have a cybersecurity organization that is capable of actually dealing with this, but then you turn to outside providers or places where it's already baked in.

The Chair: We're going to have to leave it there, Mr. Picard. Thank you.

Mr. Motz, you have five minutes, please.

Mr. Glen Motz: Thank you, Chair.

I thank both of you for being here.

We all hear of scams that happen, whether they happen to ourselves, or to our neighbours or family. They usually originate from overseas. Constituents have told me—and I've certainly investigated a number of these myself over the years—that when they threaten to call the police, the scammers become brazen enough to basically scoff at them and say, fine, we're over in whatever country you name, and your police can't do anything to us.

In your new mandate now as the Canadian Centre for Cyber Security, what role do you play in ensuring you get involved in helping the police? What tools do you offer to police to go after this or to try to mitigate the exposure of this, not only for helping the police and their tools, but also at the other end, hopefully rolling out more aggressive strategies for the consumer so they are not a victim?

Mr. Scott Jones: If you look from the policing perspective, certainly our goal is to try to get people to go to the police when they are victims of these types of scams, so the police can take action. I think that's one of the first things, to encourage people that the police aren't going to come and seize their computer, to get them to report so they can take action.

The second piece, though, is the education piece. That's the part we would be the lead on, to try to help Canadians understand what these threats could look like so they can be vigilant against them. The fact that the constituent actually challenged back and said, wait a minute, this is a scam and I'm going to call the police.... Then they went back, but they knew to challenge that it was a scam and not fall for it. That's an excellent thing.

My dad hangs up the phone. He made me promise not to reference him in this, but my dad just hangs up the phone because he knows it's a scam and doesn't believe anything anymore. I am worried about the day when somebody legitimate calls now, but the fact is that he knows to do this.

I think one of the key things is how we can make Canadians aware so that, number one, it's not such a stigma that you're a victim. It tends to be a more vulnerable part of the population that falls for these types of scams. Number two is that they report it. Number three, here are some simple things people can do. Number four, how can we work with industry to make us all a little more resilient and have some national level of defence? If you don't get that spam email because Canadian companies have blocked it, that means you can't click it.

How can we start to work on some of those types of outcomes about leveraging industry, and leveraging the fact that we have a commercial sector that actually wants to protect its customers as well?

● (1710)

Mr. Glen Motz: When you mention leverage, are you talking regs, yes or no?

Mr. Scott Jones: We're talking partnerships right now. We take a partnership approach.

Mr. Glen Motz: When we're looking at various threat levels to Canada, one expert has mentioned that you need to weigh the impacts of an attack and the probability of an attack. We heard just before you gentlemen came in, and we've heard it before, that the probability of a bank being hacked is low and the probability of an individual being scammed is significantly higher, but the impacts are both significant.

If the backbone of our communication systems were compromised —that is, the systems that carry all of our personal information, government information and banking information—is that one of the largest threats to Canada's security? Is our Internet itself maybe the most critical system we have?

Mr. Scott Jones: We tend to approach it from the point of view that we never trust the thing below what we're working on. For example, if Eric and I are communicating, sending emails back and forth, we always look and say that we can't trust the network, because the way the Internet works, that communication could be routed all the way around the world and go through every single country, so we use encryption. That's how we would protect the communication.

We always look at how to layer in protections, assuming that something else is not secure. The more you look at that and the more protections you layer in—more things like encryption, security, account management credentials—the more security you get.

At one point, though, you can only do so much before you make it so unusable that users either switch, or they go around your security. That's one of the things the industry has to balance, but I think one of the key things is that the entire industry needs to improve its security. You should not have to know how to secure the basic things that are going into your home. You shouldn't have to investigate how to enable security. It should come and help you do that from the very beginning. The second you turn that device on, it should help you use it in a secure way. “Secure by default” is the term we use.

The Chair: Thank you, Mr. Motz.

If the Prime Minister phones with your Senate appointment, it's probably a good idea to hang up.

Voices: Oh, oh!

The Chair: Ms. Sahota.

Ms. Ruby Sahota: We've been talking quite a bit about companies and individuals not wanting to report, for different reasons. Companies want to seem like trusted institutions or organizations, and individuals feel ashamed. Maybe that's similar in both cases.

Last November, the government created a mandatory requirement for federal organizations that are subject to PIPEDA. This requires them to notify the Privacy Commissioner, individuals who may be affected and third parties or government departments that may be able to help in the situation. I think a test is required to really assess whether the breach is harmful enough that they would be required to report it. There are fines of up to $100,000.

Do you think this step, this measure that was taken, would now help get the information out there to people in the right amount of time? How do you view this?

Mr. Scott Jones: Not to speak on behalf of the Information Commissioner, but I think from our perspective we're looking to get that information much earlier in the process than when you know the magnitude of a breach. We're hoping that it will be when the very first indication of a cyber-compromise happens, when you see that very first spear-phishing email, that very first attempt to compromise your system and that very first attempt to use credentials. It should never be used again.

We can work with the companies. We're hoping to get information —and we are getting it—earlier in the cycle, what they call the exploitation cycle, so that we can take action and help others take action before it hits them. If you put your emphasis on what we call exfiltration of data, well, you're too late. It has already happened.

We're trying to get proactive and take action earlier. I would rather have a company call us a hundred times with 99 false positives—I'm not sure Eric and his team would like me to do that—than not call that one time when it was true and we could have taken action and helped to warn the rest of the sector about a potential breach.

That's something we're trying to incent. We're trying to work with them on that.

● (1715)

Ms. Ruby Sahota: That's excellent. I commend it, but the reality is that we keep hearing.... For instance, on Equifax, I've read that the breach happened because of poor cyber-hygiene practices. We've heard from our previous witness that the regulations and standards that companies are applying are really outdated, and that there's really no motivation for them to be updating those standards regularly so that they're up to date on the current threats they might be facing.

How do we incentivize these companies to take those types of measures if we don't have penalties and regulations in place?

Mr. Scott Jones: I think the policy and regulatory approach is something that is probably best left in your hands. For us, the basics do matter, though, and organizations do need to do them. I think the issue now is working with them, and we're trying to get the technology companies to actually improve things.

The problem is that you have to get secure by configuration. It might not have been deliberate that the vulnerability was there and they weren't doing the basics. It might have been a simple mistake by a system administrator, but it shouldn't be that easy to undermine your security because a sysadmin typed in the wrong command. There's just something fundamentally wrong.

For computer scientists and engineers, it's the equivalent of designing a bridge: If we forgot to put in one rivet, the bridge would collapse. That's not how engineers design bridges. The industry needs to figure out how to make this so that the technology isn't in such a fragile state from a cybersecurity perspective.

Those are some key things we need to do, but whether regulation is the right approach is, I think, best left in your hands. As a public servant, I will faithfully implement the directions we're given.

Ms. Ruby Sahota: We're trying our best to learn in terms of what our recommendations are going to be coming out of this study. Some witnesses paint a very scary picture when they come before the committee, and others, like you, a more hopeful one.

What sectors do you see as the most vulnerable, as sectors that we should be looking at?

Mr. Scott Jones: The financial sector, for example, makes significant investments. They have excellent capabilities in terms of fraud detection, etc. In fact, it's one of the areas where we're hoping to learn from them in terms of how they use what I'll call artificial intelligence, machine learning to detect things like fraud, and to leverage their expertise as they leverage some of ours in cyber-defence.

When you look at it, you see it's sectors that don't see themselves as big IT users until you go one step in. So we're making sure that we're working with all 10 critical infrastructure sectors. There's a technology and cybersecurity element to all of those.

The Chair: We'll have to leave it there. We're a little past time.

Mr. Eglinski, you have five minutes, please.

Mr. Jim Eglinski (Yellowhead, CPC): Thank you.

I'd like to thank you both for coming today. You said that the only secure network is one with no users. Many, if not most, breaches of government networks begin with some type of phishing scam or other attempts for bad actors to gain access to legitimate credentials. The National Institute of Standards and Technology has recommended that it's no longer advisable for network passwords to be periodically reset, yet many government department IT shops still have standard 90-day reset functions in place.

Would a simple solution like this not be a good way for us to start protecting government cybersecurity?

Mr. Scott Jones: Thanks for the question. I think I actually said that, although I also said that being turned off makes it the most secure network.

I think there are a few elements to that.

The password is something that has changed quite a bit. We are relooking at our password advice for that exact reason. More than changing passwords, we also encourage people to look at a second factor of authentication, so a little token that generates a random number. For some people, sometimes it's a message that says “Type in this code” when they're logging into a new device, etc. Turning on a second factor is actually a key cybersecurity element. For those of you with Twitter or Facebook or any social media accounts, you should all be using your second factor of authentication to log in, and we should be applying that to all of the systems in government.

Periodic password advice is something that made a lot of sense when you had only two passwords and two systems to log into, or one. I lost count at 90 of the number of passwords I have in my personal, private and professional life. I stopped counting. We are looking at how to balance security and convenience. Also, people tend to use easy passwords when there are so many. It's something that has to be looked at.

● (1720)

Mr. Jim Eglinski: In your statement, when you were first talking about the cyber-threats most likely to affect Canadians and Canadian businesses, you mentioned education. Could you quickly tell me about some of the things you're doing to educate Canadians? I'm learning so much here in the last few days that I didn't know before, and I wonder how much Canadians actually know about their vulnerability with the Internet.

Mr. Scott Jones: The first was putting out the national cyber-threat assessment, trying to give something that gives the basics, and it came with a cyber-primer, explaining what these technical terms were and hopefully in plain language. We tried very hard.

Mr. Jim Eglinski: How did you get that to them?

Mr. Scott Jones: It's on the web. We tweeted it out and we published it. I did a lot of media. It's strange to be in a media role as a public servant. It's a little surreal. We're trying to get that information out in different ways. I would love to see every member of Parliament being able to communicate this back out. We're trying to get some simple tools that everybody can get.

Mr. Jim Eglinski: Thank you. I did that. I sent it out.

Why didn't you ever look at the newspapers versus the Internet to educate people?

Mr. Scott Jones: It's a matter of where we're allowed to advertise and how we do it, but we'll take that as part of our communication strategy. We're always looking for ways to improve our reach.

Mr. Jim Eglinski: You do most of it through the computer system, though.

Mr. Scott Jones: We do. We tend to go digital; it's our go-to.

Mr. Jim Eglinski: Am I running out of time?

The Chair: You have a minute and a bit.

Mr. Jim Eglinski: Are there any laws in place in Canada for Canadian companies providing security measures, whether it's alarm systems in your home or stuff like that, to be honest with the consumer?

I'm going to give you a prime example. I have a very major security company that has my place all wired up. They came to me last fall and said, “Mr. Eglinski, we can make your place much safer by installing three cameras. There would be no portion of your property where anybody could move around or get into your house without us.” It sounded pretty good. I said, how much? It was a fair amount of dollars, but I said okay. But then I checked with my service provider, and he said the system wasn't big enough for it yet. They were telling me that they were providing me with all these credentials and all this equipment, but my service wasn't there.

Is there a requirement and law in Canada to be honest with the consumer?

Mr. Scott Jones: I don't know the answer to that question.

The Chair: I think you're pretty well done.

Mr. Jim Eglinski: I had one more, but I'll let it go.

The Chair: Thank you.

Ms. Dabrusin, you have five minutes, please.

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

I was actually quite taken with the testimony given by Mr. Kabilan in the first one, particularly the 60% number. I know you've had some questions about that, but I think he talked about the secured armoured truck travelling between two cardboard boxes. A lot of what we're talking about can be focusing on that armoured car, and it's important, but if we don't secure the cardboard boxes, we have a real issue.

I appreciate that you used the example of your father hanging up on people, but the example was given about the U.K. cybersecurity centre and what they do for education. I was wondering how much you are planning on following that type of a model. What do you see that works from that model, and what would be different?

Mr. Scott Jones: We collaborate very closely with the National Cyber Security Centre in the U.K. We are trying to apply lessons learned. Part of it is that they're further along. We're about 121 days into the cyber centre stand-up and they're a couple of years in.

We are looking at how we can improve that. We've seen them do things like.... I think they have a few initiatives in the U.K., for example, on getting girls to code and reaching out to younger people. We've sponsored some events like Hackergal, and we sent out some of our professionals to mentor. This is something that doesn't necessarily scale easily, just because it's hard to send everybody across Canada—we're a giant country.

Whom can we partner with? How can we get more people interested in the digital side? We are looking at other ways of communicating. One of the campaigns we've seen around the world is to reach out to seniors, in terms of cybersecurity: “Go and talk to your grandkids and ask these questions.” It seems to be very effective. We're waiting to see how effective it is, and we're trying to see how we can reach out in different ways, but I think education is one of the key things.

Ms. Julie Dabrusin: Would you be able to send us some of the links that you referred to and what you are already putting out there? What I've always looked at is the Citizen Lab, which has a security plan and information as well, but it would be really helpful for us to have the best tools that we can be conveying.

● (1725)

Mr. Scott Jones: Yes.

Ms. Julie Dabrusin: I was reading an article from The Financial Post, and it was referring to OSFI's role in collecting information on different security breaches. We've talked about a few different information sharing models. How does OSFI fit into it?

I'm just trying to keep track of all the different organizations here.

Mr. Scott Jones: With OSFI's role in the regulatory space.... We certainly work with them, but one of the key things for us is that in the cyber centre, by not having a regulatory function, we can be turned to earlier. We obviously support a broader government, so we do work with OSFI. We try to work together when there's an incident.

Certainly, especially in the financial sector, one of the key things is that it's all about confidence. We want to make sure that whatever's happening we can maintain consumer confidence. We can do our part, but we don't speak on behalf of the government for monetary or financial policy.

How do we coordinate? We do have partners with them. They would be brought in as one of the major stakeholders if there was an incident in the financial sector, into some of the incident management things that Eric mentioned.

Ms. Julie Dabrusin: They deal with the federally regulated entities. Money lenders and those types of shops that you might find at the end of the street, do they have information sharing requirements? Who's watching what they're doing?

Mr. Scott Jones: We're hoping that they will call us. We've made our information available, but right now they don't have any mandatory reason to report to us.

Ms. Julie Dabrusin: All right.

Ultimately, our personal information, depending on the institution we're working with, might have different standards and regulations, at least for information sharing.

Mr. Scott Jones: As far as I know, there would be no mandatory reporting for anything that's outside of that regulated space. We do get a number of reports from businesses that are looking for help.

Ms. Julie Dabrusin: One last thing.... I know I have only about half a minute left, but the other part that was missing on OSFI's regulatory powers was that the federal banks might be actually outsourcing a whole lot of their security to companies that are outside of Canada. Who monitors that? Who monitors the relationship with these outside providers to make sure that they're keeping things up to snuff?

Mr. Scott Jones: One of the things we mentioned is the cyber-threat assessment, but we've also been working closely with businesses about the supply chain and how they're applying security constraints throughout their supply chain.

For a lot of the bigger incidents, it tends to be a breach as you've outsourced further things. Usually, it's not the first degree of outsourcing; it's when you get to the second. It's about making sure that you're building in security requirements and that they cascade, but also that companies are aware that outsourcing a function doesn't mean outsourcing the accountability for the information. That's something that I know a number of companies are concentrating on, but we also highlight it in the national cyber-threat assessment, for exactly that reason.

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you, Ms. Dabrusin.

The chair has one final question.

The last time you were here, Mr. Jones, you described the security approach as a kind of layering approach. You said that you had a certain openness with certain vendors where you could examine code and various things. When Professor Leuprecht was here, he talked about a system of switches and tables and the ever-evolving way in which that goes.

Are you still confident that the approach you are recommending, namely this layered approach, is as appropriate for a 5G network as it is for a 3G and possibly a 4G network?

Mr. Scott Jones: The approach for 5G is under review right now in terms of the approach for Canada. I'm very confident of the relationship we've built with Canada's telecommunications providers and the work we've done to increase the cybersecurity elements regardless of the network. The collaboration we have in terms of how we respond to incidents is something we'll need to continue, no matter what. We need to continue to build multiple layers of security, regardless of where the technology comes from.

In my job, I actually trust nothing. I assume that there are vulnerabilities in every single piece of product we have, so how can we layer more and more protections on? That includes when the data gets to the cardboard box. That shouldn't be a cardboard box; your data should be encrypted at its destination, and it should be protected. It's not about protecting the castle walls; it's about making sure you have the vaults of the really sensitive information properly protected.

Information security is evolving, as well, in terms of how we can protect that, how we can keep information protected and encrypted. Also, we have to start thinking about whether we need that information and for how long. Maybe it's not necessary to keep it that long.

It is the layered approach, and it still needs to continue.

On the 5G question, that's something that's being studied right now, and there will be specific recommendations coming out of that.

● (1730)

The Chair: With that, I want to thank both of you for coming and informing us, and we appreciate your appearance once again.

This meeting is adjourned.