TC Webinar:

Resilience to Cyber Threats in the Financial Sector

Keynote Speaker:

Rob Stewart
Deputy Minister of Public Safety Canada

Panelists:

Danny Brando
Vice President of Cybersecurity Policy to Supervision Group, the Federal Reserve Bank of New York

Socorro Heysen
Superintendent of Banks, Insurance and Pension Fund Administrators of Peru; Board Member, Toronto Centre

Martin Moloney
Secretary General, International Organization of Securities Commissions (IOSCO)

Anna B. Puglisi
Director of Biotechnology Programs; Senior Fellow, Center for Security and Emerging Technology (CSET), Georgetown University

Host:

Babak Abbaszadeh
President and CEO, Toronto Centre

Date:

April 22, 2022

Transcript:

Babak Abbaszadeh: Hello, everyone. Happy earth day. Welcome to Toronto Centre's executive panel on cyber resilience in the financial sector. I am Babak Abbaszadeh, CEO of Toronto Centre, coming to you from Washington DC, where we are holding this event during the IMF World Bank Spring Meetings. I'm pleased to see that 700 people from 110 countries have registered for this event today. And we look forward to bringing you additional programming in the future.

Before we start, I would like to take a moment to acknowledge the devastating war in Ukraine. The world is awed by the resilience and heroism of the Ukrainian people. Toronto Centre has an ongoing training program with the National Bank of Ukraine. Please visit the website of the National Bank to learn from the governor how you can help Ukrainian armed resistance. Also, please stay tuned for an announcement about an upcoming Toronto Centre executive panel on war, sustainable development goals under fire, which will explore how can we mitigate the fallout on sustainability? This will happen sometime in mid-May or so, but no exact date has been said yet.

Since our establishment in 1998, Toronto Centre has trained more than 16,000 supervisors from 190 jurisdictions to become change agents for building more stable and inclusive financial systems. Cyber threats are a growing concern and fundamental risk to financial system and the broader economy. The changing nature of cyber risk is driven by evolving technology, which can lead to increased vulnerabilities for financial institutions and their clients. Since the start of the pandemic, we have also seen cyber risks heightened, as remote working and increased use of financial services over digital channels have opened more points of banking system access to malicious actors. These increasingly sophisticated attackers target large and small institutions, rich and poor countries, and operate without borders. If we want to harness the power of technology to lift people up, we need to effectively handle the technology threats that can harm livelihoods. This is essential for financial inclusion, an area where digital transformation creates many opportunities, and is also crucial for empowering women. Therefore, managing cyber threats to financial stability is a priority for financial authorities and governance.

Today, our guest speakers will discuss how financial institutions can improve their cyber resilience. They will also discuss the role policy makers, supervisors, and regulators can play. Now, it is my honor to welcome our distinguished speakers. Rob Stewart is deputy minister of public safety for government of Canada, and he will deliver a brief keynote. Danny Brando is vice president cybersecurity policy to supervision group at the Federal Reserve Bank of New York. Socorro Heysen, who's a member of the board of directors of Toronto Centre, is also on her spare time is superintendent the banks, insurance, and pension fund administrators of Peru. Martin Maloney is the secretary general of the International Organization of Securities Commissions, IOSCO. Anna Puglisi is director of biotechnology programs, senior fellow, Center for Security and Emerging Technology, CSET, Georgetown University.

You have seen their bios, and in interest of time, I won't read them. Please join me in welcoming them. Welcome, everyone. Our mission is sponsored by our key funders, Global Affairs Canada, Swedish International Development Cooperation Agency, the IMF, Jersey Oversees Aid, and the UNCDF. Now it is my honor to hand over the virtual platform to Rob Stewart, Canada's deputy minister of public safety, who brings a wealth of diverse perspective to this ongoing challenge. Prior to his current role, Rob was the associate deputy minister of finance, and was also Canada's finance deputy for G7, G20, and the Financial Stability Board. It is truly an honor to have Rob with us today. And without further ado, Rob, if I may ask you, we really are eager to hear your message. Thank you.

Rob Stewart: Thank you, Babak. A little bit of overstatement there, but happy to be here with you today, on fairly short notice, I have to admit. Let me just make a few remarks to frame the discussion. Obviously, this is a subject which is of interest to all public authorities in their various forms. From my point of view, cyber security, cyber security risk is the real pandemic of modern times. It's ever present, it's increasing like a virus, and we cannot inoculate ourselves against it. The fact is, increasing connectivity results in greater security risks, and hacks are becoming more frequent from a greater variety of actors. Let me share with you some statistics. The cost of cyber crime globally in 2021 was six trillion US dollars, more than the total global trade of illegal drugs. Cyber crime is projected to grow by 15% to reach 10.5 trillion US by 2025. During the pandemic, cyber crime increased by 600% globally, with the financial sector suffering the largest losses. And the total cost of all cyber crime damages in 2021 is expected to amount to six trillion dollars worldwide.

But this is not just about crime and the scourge of things like ransomware. We also need to contend with the activities of hostile state actors. And the most sophisticated and high-risk threats are from state sponsored programs of China, Russia, Iran, and North Korea. And these risks have come even more to the fore lately. I note that the Five Eyes security authorities, including CSA, FBI, the NSA in the United States and the Australian, New Zealand, UK and Canadian cybersecurity authorities have just published a report on the malicious cyber operations being prepared by various Russian state bodies and Russian aligned cyber crime groups. These risks are real. Canada's Communication Security Establishment is our security authority, cyber security authority, and it faces thousands of attacks every day on government networks. And this is true of any major financial institution you care to name. We all know that this is an ever present and real risk, and it's because financial institutions are vertically

connected to suppliers and to their clients, and horizontally connected amongst themselves. So, there is huge interconnectivity in the financial sector, and the reach of the financial sector in society is so deep and pervasive.

So, adapting systems and dealing with these risks requires holistic collaboration between public and private actors, and international collaboration on like-minded states. We need to tackle all these issues, including evolving threats, interconnectedness, and the robustness of the smallest players in the system and their resilience. We need to work across borders with international institutions like the G20, the FSB, and the Toronto Centre. The FSB's chair's letter this week to G20 ministers and governors notes that the FSB is continuing its work on promoting greater convergence in cyber incident reporting, which is a major issue. And we'll deliver a consultative report in October.

Here in Canada, we are very focused on cybersecurity across a great number of actors in the government space. While the Canadian Communication Security Establishment is the lead, there are many other organizations that are involved. And we have put in place a national cyber strategy, launched a Canadian Center for Cybersecurity to be the interface between the public sector, and to provide technical support for Canadian institutions and individuals. We've announced significant investments over the last three years in the capabilities of our cyber authority and our ability to do outreach and protect and defend government systems. We are continuously engaging with our domestic and international partners, associations, academia, and industry.

So, as I say, there are many challenges. Reporting is the first among them. And as you may know, the United States has passed a law recently involving reporting. And that's something we're considering in Canada as well. Awareness is of the first order in terms of protecting ourselves from threats. And at the same time, we are publishing and pro-sharing proactively, threats as we perceive them, typologies and various other forms of information that can be declassified and shared. Overall, our national objectives, as I believe are those of other countries, are to reduce cyber threats, and including the hostile and disruptive activities of states and criminals, to raise the bar and address vulnerabilities in the government of candidate systems and our critical infrastructure, to build our capacity to investigate, respond to, and recover from incidents, and to develop, and this is the leading edge, adaptation strategies for new technologies. This is not an area in which we can stand still. This is an area in which we are all

involved. It's a team game and we must play it together. Thank you very much.

Babak Abbaszadeh: Thank you very much, Rob. I heard almost everything you said, and your comments were very cogent and to the point, very short. Our apologies to invite you rather late, but we're really grateful that you did accept it, because we didn't know if we were going to have a panel. And I think we should all sleep better knowing that you're at the helm. And thanks again. And I know you're very busy. If you like to stay, please do. And otherwise, thanks again for your time. And you set a really good context for the conversation, so very grateful. Take care. Bye. All right. So, let's start the discussion without further delay. So, the very first question is going to go to Danny. You are leading cybersecurity supervision within the Federal Reserve Bank of New York. We are seeing more examples of crippling cyber crime across the financial sector. How big a threat is cyber crime to financial stability? And what are the substantive operational risks that keep you up at night? Thank you.

Danny Brando: Thank you, Babak. And thank you for having me today. And first I have to say that the views I express here today are my own and don't necessarily represent those of the Federal Reserve Bank of New York or the federal reserve system. With that said, I absolutely believe that cybersecurity risk is a threat to financial stability. Just recently, the Federal Reserve Board had published, in November of 21, our financial stability report that included a view on how we can consider cybersecurity risk in the context of our traditional financial stability monitoring framework. And in that, Rob mentioned the just countless and endless number of attacks our supervised institutions and organizations all over the world are experiencing every day. Those cyber attacks are the shocks to the system.

But those shocks alone don't necessarily cause any kind of financial stability implications. They first have to exploit a firm level weakness. And a firm level weakness can be anything from an employee clicking on a phishing email and that potentially wreaking havoc with ransomware throughout an organization, or a vulnerability in a public facing application. Those are firm level weaknesses. And again, that doesn't necessarily cause financial stability implications alone. It would then have to exploit a system level weakness. And Rob also mentioned the interconnectedness and dependencies that we have in the financial system today. If it were to exploit those kinds of weaknesses or the dependencies we have on data, lack of substitute ability on critical functions, financial relationships, and that trust relationship there, those are the types of system level vulnerabilities that if a shock were to exploit the firm level and system level vulnerability could have financial stability implications.

So, what keeps me up at night, Babak, is really two things. First, supply chain attacks. Supply chains are vast and complex and extremely difficult for organizations to identify, let alone protect and detect against risks to them. The very recent public example of SolarWinds, I think, tells this story very well. You have a relatively small company who provides software for network monitoring and management that was targeted by cyber threat actors, and code was embedded in their updates that would open up a back door to the organization. Customers did what security professionals like myself tell them to do, update your software, patch your systems. And unfortunately, that's what got them compromised.

The second thing that worries me and keeps me up at night are data destruction events. On the contrary, these are very easy to detect, because they're loud and disruptive, but they're much harder to respond and recover from. And if we put these two things together where we have a supply chain attack with intentional data destruction, we could see a financial stability impacting event. This type of event can encrypt or destroy data for transaction accounts, deposits, collateral management, custody systems. We could see payment system processing disrupted, trading systems halted, or even just customers unable to access their accounts and perform basic transactions. All of this can have considerable downstream impact to other firms and other sectors even. So, I think that's enough to keep me up at night.

Babak Abbaszadeh: That is plenty. Well, thank you. And also, your comment is very relevant to us, because there's always a debate about what exactly is a threat to financial stability. And some hardcore supervisors always try to link it to credit risk, but that's like trying to fight a war that happened already. And what you're talking about is very similar to what Rob said, which is this is pretty much our new pandemic, and there's no vaccination. So, thank you for making that point very clearly. I'd like to move on to Socorro. You bring many perspectives having worked at IMF and Peru and emerging markets. So really interested in your views on the fact that the pandemic expedited the adoption of digitization, which resulted in many benefits, including being able to empower women who were previously unbanked. And we know about a billion women around the world are not part of the financial system. But this has also heightened cyber risk concerns in the financial sector. As a leading supervisor in Latin America, what do you believe are the cyber risk challenges for emerging markets, especially in relation to financial inclusion? And what is being done to improve cyber resilience? Thank you.

Socorro Heysen: And thank you, Babak. Thank you for the invitation and thank you for the question. Indeed, the pandemic has accelerated two processes that were previously underway, the digital transformation of the financial industry and its service providers, and also the digital inclusion of millions of people who were previously unbanked. All these transformations and digital inclusion are creating added risk for the financial industry, as well as for customers. Of course, as Rob Stewart pointed out, Rob and Danny actually, cyber risk is a global risk. So, in emerging markets, we face the same risks and the same challenges that have been pointed out by the two previous speakers, cyber threats and incidents like ransomware attacks, hacking incidents, stolen data, destroyed data are all sources of concerns for us, for financial industry and financial stability.

It is more points of access to banks only enhance the vulnerability to these risks, and fast innovation that is being taken place during the pandemic also creates added risk, because during periods of fast innovation, what you have is that not all the areas of a bank move at the same speed. And that probably creates gaps in controls and in security that are making a bank more vulnerable to an attack. So, these are common to all of us, I think. This is not special about developed or emerging markets or developing nations. We all face the same risks.

But perhaps in addition to what has been mentioned, in emerging countries with recently included unbanked people, we face more of the type of risk that consumers are facing, or digital fraud associated to consumers. Like withdrawals or unrecognized credit cards or loans that basically create a problem for the consumers, and that in many cases, the banks end up covering, and the risk is being transferred to an insurance company and creating higher premiums because of these heightened risks. So, the consumer element perhaps is something that should be taken into account. And we need to pay a lot of attention to that, because consumers are vulnerable to aggressive selling, to fraud, to phishing, to all sorts of different cyber types of crimes. And young people, new digital consumers are especially vulnerable to this, because they tend to be very familiar with digital applications. And they feel confident in using financial services in their applications in their phones, but sometimes they are not as careful as they should be with the risks that accompany the use of financial services on mobile applications.

So, what do we need to do? Oh, well, a few examples. I can give you a few examples about a survey that we did in Peru and some of the concerns that people have. 70% of bank users in Peru were extremely worried about fraud to their own accounts. And this is a concern for us because it also threatens the reputation of the banking industry. And it also could create some slowing down for inclusion, because if people are not comfortable and they're not confident, they don't trust the financial system because they are they're afraid of fraud, well, they will not get included. 25% of bank users lost their credit card in the survey period. 69% of users did not update their antiviral software. 78% of users did not change their email passwords. And only 35% of bank users regularly check their activities on online accounts.

So, this environment creates special vulnerabilities for consumers. So, what do we need? First, we need to ensure that financial institutions have an adequate framework to address properly cyber risk, and to have an adequate management of cyber risks. And for this, we need adequate regulation, adequate supervision, supervisory capabilities. But as was pointed out previously, we need also sharing information, cooperation, not only locally among financial institutions, with supervisors, with other government authorities, with other types of industries and internationally.

With other types of industries and internationally, and also what else do we need? We need to make people aware that cyber risk is not only a financial industry problem, but also a consumer problem. And therefore, we need to work on public awareness of this risk and on digital financial literacy. We need to work on education, and we have been working very hard on that in different types of channels, of education that we have. Facebook, YouTube, our own webpage, and also going locally to different places and having classes for students, for teachers, for older people, for young people, for different sectors, and working very hard with the ministry of education to try to create an educational framework that includes this as part of the children education to work on this in the future. So let me leave it at that. But I think financial literacy is a huge, huge issue moving forward, because we are not going to solve this only by the industry and the government and the private sector working on this. We need the citizens' collaboration.

Babak Abbaszadeh: Thank you Socorro. I guess what I take away from your comments is that it's one thing to try to defend ourselves against cyber threats, and another thing is to take the war to the hackers, right? That's just in a simple way of what you just said. In a sense that you need the literacy of all kinds, but also vigilance, and let's do that international coordination. It also very useful to know that cyber, like pandemic, does not discriminate between advanced

and emerging economies. We're all in the same boat on that. Thank you very much for that. And just a reminder to our audience, we do have Spanish and French translations available. You can access them at the bottom of your screen. And at the end of the first round, after I ask my question to Anna, we will open up for a round of questions.

Then we go to the second round. So please put in your questions early. I already see at least one question that is posted so that we get a chance to read your questions. Martin, I'm very excited to ask this question up to you, because you are really an international standard setter, representative, and one of the senior ones and you have your finger on the pulse of the financial sector. Over the past five years, national authorities and standard setting bodies and private sector organizations have launched initiatives to address cyber risk and increase cyber resilience on financial markets in the industry. So essentially what Socorro was talking about, you guys have been involved at pretty much the forefront in that. Can you please briefly talk about IOSCO's efforts and steps taken related to improving cyber security? Thank you.

Martin Moloney: Sure. Sure, Babak. And, I think actually your way of asking the question is really good because we can learn a lot by looking at the history of how this has developed, because there may be many people in your audience who are feeling a little bit behind the curve that they're not really up to scratch with latest developments, but I think we've all spent the whole of the last 10 years actually constantly trying to keep up with developments in this area. It's hugely challenging. And if you look back, I think it was really only after about 2010, that many of us sort of became aware of the scale and importance of this issue. So, the first thing IOSCO ever did in this area was in 2013, when we did a report with the World Federation of Exchanges, because the natural thought at that point was exchanges are the weak point.

We've got to help the exchanges and we've got to look at the issues there. And you'll see there, some of the points that have continued to be major themes. So, we really emphasized the centrality of information sharing and we emphasized the changing sophistication of the attacks. That was a point we were emphasizing back even then. After that, what we did was also quite interesting. In 2016, we actually produced a framework for management of cyber risk by financial market infrastructures, that's by payment systems and CCPs and so on. And that covered everything you'd expect to see. Sort of governance, risk identification, sort of protection measures, how you detect attacks, but it also critically set targets for

financial market infrastructures saying they should be aiming to resume in two hours. That's a really tough target for anybody to meet, and it's become more difficult as attacks have become more sophisticated and changed their character.

Of course, it also emphasized testing and situational awareness, and learning and development, all those things that have continued to be important. And that you see in many of the other frameworks that have been produced since as well. Having dealt with the infrastructure, we then broadened our view, and you spoke over the last five years, and this is really the point at which this comes in. We said, okay, so we've dealt with the core infrastructure, but now we have to deal with everything else because this is not just a core infrastructure issue. So, we did a report in 2018, which looked across the whole of the financial sector that we produced standards for, and looked at it on a sectoral basis, but also came out and admitted that regulators were having challenges in this area. It was not easy for regulators to develop policies to deal with this.

And we described the wide variety of different approaches you see in different countries, where in some countries you're seeing specific rules being developed, in other countries there's an emphasis on raising awareness, which you should never be underestimated. And in some cases, you're seeing actually regulators coordinating drills and so on to test for this. So, a lot of good practices emerging at that time, and a lot of those good practices have continued since, but there's also lot of fragmentation and approach. So, in 2019, we produced a report, the cyber task force report, which tried to argue, and which did argue, I think successfully, that look, there were three core standards emerging and it asked everybody to look at one of those three core standards as the ones they would apply. Either our own framework or some standard that I've just talked about in relation to FMIs. Look at the ISO 27,000 or look at the at national Institute of technology framework.

And we've pushed since to everyone to try to conform to one of those three standards to reduce the amount of fragmentation in the way these things are approached. And then in the wake of March, April 2020, we then looked at what were the implications for operational resilience and particular in relation to cyber. In January 2022, we produced our report on operation resilience lessons from that period. We emphasized the issue of governance and making decisions under conditions of uncertainty. You don't know exactly what's going on, but you have to plan now in order to protect your data, and how critical it is of the proper governance frameworks in place to achieve that.

So, if you look at that history, it's a history of sort of trying to get good practices developed and then trying to zone in on the key issues where you're seeing continuing weaknesses. And we continue now to look at that. We are looking back again at our 2016 standards now, because you're now facing multi-vector attacks, increasingly complicated attacks, and we have to make sure those standards are still working well for the financial markets infrastructure that are so important for us.

Babak Abbaszadeh: Martin, this strikes me as I'm listening to you that, it's a benefit of a full call press, and it's been much similar to trench warfare, right? Using a war analogy because you can do all kinds of planning. But what good is that when technology's changing so fast, attacks are getting so sophisticated? So, thank you for that. And also, just a little plug for Toronto Centre. We actually have crisis simulations that are focused on cyber threats. It's a very interesting area that's evolving and we constantly learn ourselves through these simulations and exercises as well. So, every time you go into a battle, you learn something more. So, thank you for that. Now let's come to Anna. Anna, you are the non-financial authority in this group, and we're not going to hold it against you. We're open, we're friendly people, but we are very interested to hear from you. At Georgetown University, you are dealing with the latest developments in national security and emerging technology.

As an academic and also a practitioner out there in various counterintelligence, you can look both at the longer-term horizon and a historical perspective. You've been listening to the perspectives of leading financial authorities today. How are their concerns and approaches related to your cyber security work at Georgetown's center for security and emerging technology? Thank you.

Anna Puglisi: So, thank you. I was laughing at being an academic. It's a blessing and a curse as we're, looking at being able to pontificate a little bit, but all kidding aside, I think everyone is really laid out, just highlights the growing threat, but even really more importantly, the need to really bake in solutions and thinking about solutions from the very beginning and that it really touches us all. I know we're very focused on financial today, but it really comes across all of the different areas. Will that be infrastructure? Academia? We see that, especially from the intellectual property right perspective, and it's a really different way of thinking about things. And I think that's what makes it so challenging. And I think in some ways too, we haven't mentioned this yet, but we also need to think about whether we're dealing with financially motivated bad guys or girls, or nation states, because that really makes a difference as well.

And what the motivations and the drivers of some of these activities. Is it to gain information? Is it disruption? To undermine institutions. Or is it financial? In some cases, those actors it'll be all of them, but it's really important because how we message and how we talk about that, especially with the different constituencies is really important. A lot of what we do too, is also thinking about, it's pretty grim right now, but looking forward, what will technology developments, especially AI, have on actor's ability to use these tools? And that gets at really, especially as more things are linked, the tools are getting better and, in some cases, and I think all the speakers mentioned this, is that awareness piece.

And really highlighting that this is an issue for everyone, and not just the CTO, or the security folks that basically kind of get brought out for a board meeting and then sent back into their office down the hall. But as open level democracies, we really have to find principled solutions because we don't want to break the system. Right? The system has worked really well. So, we have to find ways of dealing with that. And it kind of highlights that academia and commerce is really the new geopolitical battle space. And we're just, again, not really thinking that way. And we have to have a holistic approach in bringing together public, private, government, especially as data becomes more important to the different functions of government, of academia, of the private sector. I love the analogy of vaccines, of course having a bio background. But I think it really hits that it's that prevention piece and getting out ahead of the threat and dealing with education. Thanks.

Babak Abbaszadeh: Well, thank you. That was a good way of wrapping the first round, and a couple of things that I'm taking from you, actually you're connecting, is the state actors versus the loan actors. I remember there was a famous former US president that thought some of the hacking was done by a 400-pound person on a bed, when in fact we found out it was like an army of expert Russians and doing that. And also, the young people, and I'm a father of a couple of them. They're essentially cyborgs, right? For them, technology is really an organ of their body as opposed to us trying to figure out how to do something. Level of sophistication is just going to increase.

Let's go to some of the questions that we received. Thank you for your questions. We'll try to answer these questions in CNN style, right? I ask a

question, I appoint it to someone, and please break it down for us in 20 seconds. So, the first one is from the courageous anonymous, how do you strike the proper balance between innovation and risk? Digital presents a huge opportunity to reach the un-banked, but at the same time, there has to be education and training to increase financial literacy. Who should address this training? Socorro, I'm going to pass it on to you and you literally have about 20, 30 seconds to answer. Thank you.

Socorro Heysen: Well, it is an impossible task really because not only the 20 seconds but answering the question. Basically what you have to do as a regulator or as a firm that wants to do innovation, is to try to keep all the areas of the organization going at the same speed, and the regulator will need to not be too intrusive to hamper innovation, but it will have to ensure that the banks are prudent when they're developing new products, or new applications, or accessing unknown areas of business. It is impossible to know what the proper balance is, but you just have to keep doing it and keep on trying.

Babak Abbaszadeh: Yeah. So, Socorro, if concision was an Olympic sport, you'd get the gold, silver, and bronze medals. Thank you. That was actually really good. And what's very interesting, what you're talking about is using a tired term, is maybe cyber mindfulness, right? The idea is that just be aware that this threat is there and do what you can to orient your work towards that defense and trying to combat it and incorporate it across the various issues you're working on. Thank you very much for that. I have a question from Colleen. She was brave enough to put her name, full name, could the speakers please discuss the best way to engage and educate consumers and who should take the lead on this? So, Danny, I'm wondering if you could just, this may or may not be in the purview of exactly what you do, but I'm sure you've reflected on this. Would you mind tackling this? Thank you.

Danny Brando: I'll do my best in a few seconds. I similar to what Socorro and Babak said, this is incumbent upon everyone. There's no single authority that's going to educate all consumers on cyber risk. I think as financial service providers are introducing new services and capabilities for consumers, it's incumbent upon them to make sure that they're also educating their consumers on the risks of using such services. So, I think it is for everyone, but individually, as we provide services, we need to provide education as a part of that service offering.

Babak Abbaszadeh: Good. Thank you. And Anna, I'm going to go with you on the next question. It's a fairly broad, big question. At first glance, the answer is obvious, but I think we need to reflect on it because it's important. Have recent world

events, I guess it's Ukraine, increased concern with cyber threats? Because the reason I'm saying it's an interesting question to look at is, one of the major arsenals, we're all afraid of about Russia and China, was the cyber attack and that has not seemed to have happened. Thank God, but are we all on edge right now because of this stuff?

Anna Puglisi: I think, the issue we were talking about it, like bringing it to the fore and awareness. And really kind of thinking through, there's been a lot of discussions about what would be the implications of that, and that is really far reaching. Whether that's infrastructure, whether that is the financial institutions, whether that is outside of areas of conflict, but I think it, in some ways, redefines what is warfare and what different aspects, that will become challenges in the future. Especially when you have incredibly robust state programs.

Babak Abbaszadeh: Great. Thank you. Martin, next question I'm going to pass on to you is from our good friend and former board member, Andrea Corcoran. I had the pleasure of seeing her at a Toronto Center’s dinner just a couple of nights ago. Andrea is asking, there has been increasing interest in mapping risks in financial intermediaries, including among systems where multiple systems interfaces, and some are legacy systems. Is this part of preparedness in your work? Thank you.

Martin Moloney: The answer, I think is, it absolutely has to be because a lot of, Danny probably knows more about this than I do, but I would say the way in which we're in the financial sector, that IT systems develop, and particularly the use of robotics to connect systems of different ages and therefore the existence of legacy systems, which are often not well understood by some of the people active in the IT departments in large organizations.

Meaning that you can actually have risks that you don't fully or easily understand within the organization, even though you think you understand your own systems, therefore you need deliberate processes to map those risks and understand the flows of information and the possible access points, which can be highly complex in a modern financial organization, in order to be able to get a grasp on what the risks could be. And I would link that very closely to the question of who is setting the risk appetite within the organization, because if they can't understand the complexity of the systems you've got, then their setting of the risk appetite will be a notional exercise. And that's part of the difficulty, I think, for regulators in interacting with organizations because of the difference you come at this as a regulator, it's very difficult to understand the complexities of these historically evolved and multilayered systems.

Babak Abbaszadeh: Thank you. So, in sense, you were talking about risk-based approach, risk-based supervision, trying to understand how the risk interact and don't spend all your time trying to assess every single risk, but try to do a bit of a triage of what's most important and go through there. Thank you for that. Just a point of order, as you can see, there's a lot of enthusiasm here on the boards, on the questions. Some people are putting questions in Q&A, some in chats. Pretty soon, I think someone's going to bring a question to me through a pigeon. If everybody who has their questions in chat, put them in the Q&A, and my team keep them, I'll come back to them again. Thank you. The most important thing is thanked you for your enthusiasm. It's a great problem to have for us. Keep the questions coming.

So, let's go with the next set of questions here. And Socorro, I think I'm wondering if I can just go to you right now and say that as the senior superintendent in Peru, what type of information do you require to improve your macro surveillance of cybersecurity and financial institutions to ensure early detection and resolution of infractions and infringements? Thank you.

Socorro Heysen: Thanks for the question. But first of all, let me say that we have done more progress on micro surveillance than on macro surveillance as a country. We do have a huge challenge ahead of us on issues regarding macro surveillance, because most of the progress that we've made so far regards micro prudential supervision of this risks, the cyber risks. Our supervision includes of course the assessment of the organization policies, allocation of resources and practices, and also an assessment of the banks' internal tools for the prevention and detection and the response for cyber risk, and their internal systems for the timely reporting of cyber security incidents.

And they're also the reports of cyber incidents to supervisors and to other specialized centers for the detection and response of this incidents. So, in general, most of what we have done is regarding micro surveillance. We have two types of reports that we get. First, the periodic regular reporting that includes reports on the important changes on the business, on operations, and on technology environment of each bank. Then we have reports of interruptions of operation, reports of cyber incidents. And also, we have a different type of reports, which is almost real time information. Special reports of significant cyber events of fraud or things that can affect reputation of institution, theft or damage, data.

Reputation of institution theft or damage data or service disruption. So special reports are key. They are important because they come early, but usually they are not very accurate. They are not very comprehensive. They cannot be comprehensive because the focus of the attention of the company while dealing with a threat or with an incident is resolving the incident, not informing the supervisor. So, in this context, the first reports on an actual incident can be imprecise, and they tend to be light because we want the industry to resolve, the company to resolve the problem.

In addition to these reports that we get, the periodical and the special reports, we get access to platforms. That's a very important source of information. International platforms of cyber risks, threats, and incidents across different countries in the world, that's an important tool also for understanding what the vulnerabilities are. And basically, we use this to assess what the situation is. One important piece of information is that for any quality response, you need institutions to interact with each other. You need to talk to other market participants to share information. And for that, we need good coordination, and we need to build trust. And it's very easy to say, but it's difficult to achieve. To get financial institutions to actually share information in a timely manner to prevent the expansion of an incident. Because basically if we share information at the right time, we may prevent the risk from getting bigger and the impact of the threat to getting bigger.

So, I think those are the key things. We need better, more standardized information to be shared among different supervisors, different government authorities, but also different financial institutions to solve these problems. And it's a continual task. We're always going to be running to catch up, basically. Running to understand the new threats, the new problems. And one of the things that you mentioned before, and I think that are very useful to build the trust that we need. And the capabilities for information sharing is building crisis simulation exercises. The crisis simulation exercises are not only to understand what our risks are, but also to know each other and to appoint specific counterparties, to know your counterparties, to have task forces in each crisis, task forces in each of the institutions that are essential to resolving this crisis so that they can know each other and talk to each other and have the contact information in the right time to be able to basically address this incident in the right moment.

Because basically for a significant event, for a systemic type of event, basically quick information sharing, and quick response is key. So basically, that's what I want to say.

Babak Abbaszadeh: Oh, that's great. Well, Socorro, thank you so much. I mean, the word crisis is very important. And Toronto Centre, we were born out of the Asian Financial Crisis in 1998, and I think we've done something like 130 crisis simulations, many of them bespoke since the global financial crisis. Some of your very senior officials have been trained by Toronto Centre as well. So, this is top of mind for us.

I went a little bit out of sequence. So, I'm going to come back to Danny. You thought you were off the hook, but now your question is here. So, Danny, collaboration on cyber security, our invisible enemy, is always a challenge. How can supervisors do a better job globally? And what are the success factors to make us more resilient, as the pace of digitization increases? It's interesting, these questions keep coming back over and over because sometimes the answer needs to be told more than once. Please go ahead.

Danny Brando: Yeah, absolutely. And it's an important question. And so, with collaboration and information sharing, the good news is I see progress happening year over year. Progress between firms sharing information about threats and incidents that occur. Between firms and regulators, government agencies, intelligence agencies, international partners. It's growing more and more year over year, and that's on the positive side. These kinds of sharing of best practices, unique approaches, insights, and ideas in forum like these are just going to make us better and better. And I want to thank the Toronto Centre for investing the time and energy on an important topic like this. Because cybersecurity information sharing is something that I'm extremely passionate about. I believe it's critical in the collective defense against this threat, but it does take a lot of time and energy in order to break down the natural barriers that come up with information sharing within an organization, let alone across borders and jurisdictions. Right? But I believe that effort is well worth it.

We can benefit from more well-designed scenarios and exercises to stress our ability to collectively respond and recover. And I promise you, when the event occurs, a financial stability, large scale cyber impacting event occurs, we're going to wish we did more exercises to practice and have that muscle memory. So, the more we do and the more difficult we design these exercises, I think the better off we're going to be.

And that leads me to every organization needing a playbook, and not just the technical one. I think Anna said this, right? Cybersecurity is not a technology problem alone. This is a problem that crosses technology and business. And so, the playbooks, I believe, need to be written not only with the technology pen, but also with a business pen. Business strategy and cybersecurity and continuity all need to be aligned, and need to be thought about from the beginning, not tacked on afterward.

So, partnering your cyber experts with your business experts is going to forge trust relationships that are going to pay dividends, if and when they're responding to cyber incidents, because these types of relationships will be stressed in times of crisis. So, the playbook should not only cover attacks against your organization. I think that's the normal inclination of most organizations, is, "All right. How do we think about cyber attacks against our organization?" But I'd also encourage people to think more broadly about, "How do you respond? What's your playbook for attacks that impact your counterparties or your trusted partner relationships, right? How does that change the way that your business might operate?"

So as supervisors, we play a critical role in ensuring the safety and soundness of supervised institutions, monitoring trends, coordinating, and assessing impact, and informing if there's any needed policy changes. We need to continue to collaborate across industry, across government, academia on improving our cyber risk data collection and modeling. Today we have lots of data and models around credit risk and liquidity risk. Not so much around cyber, right? And so, this is an area that I think we need to collectively improve and mature. So, if we do all of this, I can't promise we're going to all be okay, but I can promise we'll be a lot better off than if we hadn't. So back to you.

Babak Abbaszadeh: That's great. Thank you. I found your suggestions highly practical, and that's very useful, that we will end up using them in many of our courses as well, because you're always trying to find out what's the latest and the best here. Thank you.

Martin, before I go to your next question, one of the participants asked where can they see the documents that you have been referencing as part of your opening and other comments? So, people can go to IOSCO's website, I suppose. But also, Martin, someone on your team can send it to us, and we'll try to send it to the team here as well, distribute it. So, if you could be kind enough to do that, we'd be very happy.

Martin Moloney: Not a problem.

Babak Abbaszadeh: Yeah. Thank you. So, the question is, "At IOSCO, you monitor the consistency with the core standards, as well as consistency across national cybersecurity frameworks of member jurisdictions. But also, we know one size doesn't fit all. So, what are the main challenges they have been facing so far? And what needs to be done to address those challenges going forward?" Thank you.

Martin Moloney: I think I mentioned governance earlier. You can't get away from governance as a key issue, and jurisdictions struggle with that. And I think one of the reasons why you get a problem around governance with this is that there's actually a bigger challenge for organizations around proper governance of risk management in general. So, the key issue is often to get boards to make the risk management decisions and set the risk management appetite. But that is, for reasons that you've probably gone into in many seminars in the Toronto Centre, and I won't go into all the detail here. That's a really tough challenge for organizations, which trickles down into cyber just as it trickles down into many other types of risk.

And the one thing I would say is there's an obligation on chairs to conduct cyber risk skills assessment of their board members so as to make sure that you have the right combination of skills at board level to be able to do that. There's lots of other critical factors for being able to achieve that, but that's one.

I think another thing we come across a lot is patching and the risk in a lot of large organizations of the false economy of not keeping your patching up to date. And one of the things I would recommend to any new chief executive in an organization is ask what's the patching backlog in your organization and find out and do something about it, because that's what gets you the... What are these called? The zero-day vulnerabilities, which are so tough for many organizations. A problem that could have been fixed but wasn't. And as a CEO, you often don't know about that.

And the other thing we've definitely come across is testing is still not as good as it really needs to be. And regulators have a challenge, I would say, in setting standards for organizations in that. And some of the things that they have to challenge are, why are service providers not being included in the testing when we all know they're critical access points for many vulnerabilities? Why hasn't another test been run after you've done your remediation to check to see if the system works? And why haven't you gone up from just the ordinary standard tests to real threat hunting, which is something that some organizations don't do? It's possible to get very cozy with your IT provider, and they tell you everything you've got is okay. And that's often not good enough in terms of testing.

I think a lot of the points have been made about learning, are also really important. And those are around reporting to regulators. We're still not seeing that consistently happening everywhere. Sharing of information, there are a couple of really good initiatives. I see very good ones, particularly in the banking sector, but we also see ones that asset managers are involved in as well for sharing information. They don't all have to go through the national cyber center to be effectively shared. And there's a lot of varied practice there. I do myself wonder if this whole structure of national cyber centers is actually the best way to do this, but that's an interesting point to discuss.

And I think we're also seeing some cutting-edge developments where some jurisdictions are actually moving into effectively organizing testing themselves in cooperation with regulated entities. Some of those really interesting developments are showing us the next level that I think regulators are likely to go through in trying to press organizations to get better and better at this.

Babak Abbaszadeh: Thank you, Martin. You also get a gold medal. I mean, starting with governance is always a very, very important topic to talk about. But then you went further beyond that, and you actually talked about very specific questions that needed to be asked. Thanks again. And hope you don't mind if we just take some of your ideas in some of our courses as well, because I'm always looking for latest thoughts.

I'm going to go to Anna. And then right after that, we're going to go to questions. I'm very excited because there are a ton of questions out there. And I'll promise you we're going to get to as many of them as we can. And in the meantime, Jill's word has put in... From IOSCO, I believe. Has put a number of links here. So, a note to my team, please, let's copy these links. And for those who wanted IOSCO information, please copy the links as well. So, thank you very much for that.

And let's go to Anna. Anna, your challenge is to bring this section to an end, which is so exciting so far. So, you played a prominent role in drafting the recent US national counterintelligence strategy. Sounds exciting. And in designing mitigation strategies for both the public and private sectors to protect technology. As you reflect on that strategy, what do you think countries can do to achieve a more secure and resilient digital world?

Anna Puglisi: Great, thank you. First off, it's really kind of bringing it out of the shadows, right? And having events like this, both at this larger level, but also regional

levels, and really start talking about it because I think too often, it's blame the victim, right? The victim company, the victim institution, or an individual who gets their information stolen. And having that reporting. That's really, really important, right? To put that information back into the system so we really understand that evolving threat. And it's twofold. We have to think the unthinkable, right? I mean, many of our institutions and our systems are built on trust. And we are seeing over the course of the last several decades, especially as things become more interconnected, there's benefits to that, but there's also threats.

And I have to say, after hearing some of the comments from my co-panelists, I think I have more things that are going to keep me up at night tonight. But the flip side of that is that while we need to think the unthinkable, we really need to do the basics, right? And I mean, we were just talking about the patching or training the workforce on phishing, things like that. And again, I come back to really need to stop thinking of this as a nice to have, and it really kind of gets at, what is the value? We need to focus on the value of doing it versus the immediate cost. Because I think what really gets focused on is that immediate cost, as opposed to, "Okay, what's the cost going to be if my water plant goes down?" Or people begin to lack confidence in the institutions.

The sharing of information is really important. And I also debate whether a government is the right place to have that, or a central location, but it really is going to be that holistic full court press, right? Because each has different information, different skill sets, and also different risk and threat levels. So, government, civil society, universities really kind of working together. And collectively, we really deal with those state sponsored programs because they really do undermine global norms. They undermine the system that we all rely on, and we need to collectively, diplomatically make it clear that that's just not okay. Because really at the end of the day, when we think about those state programs, our companies, our people, our institutions are up against the nation-state, and it's not a fair fight.

And then finally, a number of the panelists have mentioned this, is it comes down to education. So, in what I click on personally or collectively of how we work together, but also thinking to the future, and what is that technically proficient workforce or digital savvy folks going to be? And so really trying to think ahead, and work on that, and having those training programs. And it really comes down to, I think, the education resilience and workforce.

Babak Abbaszadeh: I know that was a really excellent way of summing it all. And I will sum up your summation by saying that the work is never done, right? So, we have to be vigilant, we have to be mindful, we have to be proactive. But thank you for that. You give us a lot of different thoughts.

I'm going to go a little bit in a different sequence for the questions that are there. I'm very excited because we have a ton of questions. And if you stay till the end, you'll be fully rewarded because we're going to go through as many of them as possible. So, a question from Bill Coen, a member of our board of directors, which I also had a pleasure of seeing a couple of nights ago in person. And Bill and I had passed a saltshaker to each other and didn't have to say, "Unmute" when we were seeing each other in person. Bill's question is, "Financial institutions, mainly systemic important institutions, in some jurisdictions meet virtually on a daily basis to share notes on cyber attacks, defense measures, recent developments, et cetera. Should the Central Bank or supervisory authority be involved in this dialogue, or at a minimum encourage this type of private sector engagement?" Danny, I'm wondering if you may want to take this one up. Thank you.

Danny Brando: Sure, I'd be glad to. I could say in the US, I think this does happen to a degree. So first I absolutely think we should be encouraging, and we do encourage financial institutions to share information among themselves, getting that information out there quick so that they can defend themselves properly against the latest threats, absolutely something that we can and do encourage. But there are a lot of partnerships that we have between the federal financial and state financial regulators with industry. We meet in person on a regular basis. We share perspectives, thoughts, threats, have collaborative work group to tackle some of the bigger issues. So that kinds of cooperation and collaboration is occurring. And I would recommend all jurisdictions consider that kind of cooperation if they're not doing it today.

Babak Abbaszadeh: Thank you. And how could I resist this opening for a question from Cyber Mindy? "Good morning from Nepal. So, climbing a summit, my question is, how are attacks being tracked? Kindly provide an insistence if possible." Anna, I'm wondering if you might want to take a stab at that one.

Anna Puglisi: Actually, that's an amazing question. I think it's not as comprehensive as... And it should be more comprehensive, right? And I think it just really depends. And it gets back to that reporting issue because we know some organizations or institutions have issues and don't report it, some do. So that's something that I think we collectively really need to work on.

Babak Abbaszadeh: Yeah, I guess, I mean, if I can make a follow up from that question, the community of financial supervisors and regulators were all shocked by the... And I'm sure you've heard about it. The attack on the Central Bank of Bangladesh where millions of dollars were stolen. Is there any kind of a registry somewhere globally as you're aware of that keeps track of everything? And at least figures out, "Okay, in 2010, this happened. In 2012..." Is there such a thing that's centrally available for people to go and look at, maybe learn from? Or is that a good idea to have something like that?

Anna Puglisi: Yeah. I'm not aware of ones that cut across multiple sectors. I think there are more individual.

Babak Abbaszadeh: Okay. No problem. Thank you. Martin, Allison is looking for investment advice. So, she's asking, "What do you think about cryptocurrency in this context?"

Martin Moloney: You know, the interesting thing about cryptocurrency here is in a sense, it doesn't make any difference, because the plumbing is the same, whatever's going through it. And the potential to attack the plumbing is the same irrespective of what's going through it. In another sense, however, we have been very concerned about the potential link to the growth of interest to cryptocurrencies, obviously for payment systems, stable coin systems, which have a potential financial stability implication to grow to a point where they would actually have financial stability implications. And in that context, you have to worry about the growth of this space. I think one of the things that maybe I would say from a position of some ignorance, I would ask the question of the experts, "If somebody really starts to have a go at blockchain. And particularly with the development of quantum computing in the near future, could we not have a really vulnerable part of the financial system in this area? That's a question I have in the back of my mind. I don't know the answer to it. But if contrary to the conventional wisdom, these blockchains were not as secure as they appeared to be, we could end up with an extremely vulnerable part of the system.

Babak Abbaszadeh: Very good. Thank you very much. Socorro, we have a couple of questions here, I think they relate to credit unions. So let me see if we can figure out a way to ask them. They're a little bit worded in a long way, but the first question is credit unions are becoming increasingly important role players in the financial inclusion in most of developing countries. However, the rate of usage of digital financing is limited. How can they be affected by cyber risks and become resilient? It's actually a pretty good question when you think about it, in terms of you want to increase access, you talk about credit unions, and then how do you deal with that as a regulator when it comes to cyber?

Socorro Heysen: Okay. Well, in a way they are less exposed to cyber risks, at least in Peru, than other institutions of the financial system. Why? Because they tend to be less connected and less digital in their operations. They are... But of course, that is going to change. It's going to be changed quickly. And I think that they are a big tool for financial inclusion, and they are going to be a big tool in the future.

How do you deal with that? Well, pretty much in the same way as you deal with that in the financial system, the problem is that it's a problem of scale. You may have to do... Cyber risk, dealing with cyber risk is really expensive, and it is more expensive than dealing with other risks. And the investment that you need to deal with that may not be something that a cooperative, for instance, may have at hand. So perhaps they can use cooperation as a way of dealing with this risk. Getting together all cooperatives through a cooperative federation, for instance, to try to collectively get enough resources to fight this risk as a group of... As a sub sector of the industry. I think that would be a way of doing it. You need to use positive externalities to fight negative externalities.

Babak Abbaszadeh: Interesting. Very interesting. I'm going to come back to question two of Marwa a little bit later to give a time for other questions, but while we're with you, Socorro there's a question. Jonathan says, "Can Socorro share cyber risk platform resource links with us?" I think you'd mentioned that. So, I'm wondering if someone in your office can either put it on the chat, or you can send it to us. We can distribute it to the group. That would be great.

Yeah. I'm sorry. Okay. Sure. Sorry. Now the next question really is interesting. It's very brief, to the point. Priority of cyber versus climate risk. It reminds me of the questions we ask our kids. Do you rather sleep on a bed of nails or on a bed of spiders? We had Governor Mark Carney come and talk to us about a year ago, and he talked about how climate risk, climate change is like a slow-moving pandemic. You cannot self-isolate, and you cannot vaccinate. Rob Stewart said the same thing.

And Martin, maybe we could go to you. Supervisors seem to be doing so much more. Don't you miss those subprime mortgages and Lehman Brother issues? Now you have to deal with so many things. So, as you look at the risks ahead, how do you prioritize between climate risk to the financial

system, which has now been incorporated in FSAPs and cyber? Or can you chew gum and walk at the same time?

Martin Moloney: I think in this case.

Babak Abbaszadeh: And do anything else.

Martin Moloney: I think in this case, we can. I shouldn't be so ambitious as to claim we can, but actually I don't see any significant trade off between the two. There are some risks which definitely you do have to trade off. And for example, we talked a minute ago about crypto. You definitely, there is a trade off between facilitating crypto and innovation and controlling the risk for the investor. But in this area, I don't see that much of a trade off between sustainable finance and dealing with cyber. In fact, the integrity of the systems is critical to the development of sustainable finance solutions.

So, I would see them as very complementary. They are both challenges of our times. Yeah. We are clearly trying to create internet protocol enabled communication systems that really drive forward the financial sector. And we're trying to use that in order to create a new sustainable finance sector that works, in which you can trade carbon credit securely, in which you can get information analyzed and spread around the world, and you can gather information on level three emissions and so on.

So, there's a lot of complementary between in the technology that cyber attacks and a lot of the sustainable finance solutions that we are working towards. And there's a need for a very high level of trust in the information that is going to be at the heart of the sustainable finance system. And for that, the systems for developing that information and for communicating that information need very high levels of integrity. So, I don't see any trade off. These are two that we are going to have to push forward hand in glove together, in order to get where we're trying to get to over the next five years.

Babak Abbaszadeh: You win. Correct answer. Thank you very much. That's great. That's fantastic. It's always good to be on top of what's going on.

So, Anna, this question's going to go to you. It's an interesting one, and I think can cut across supervisory issues or really any sector. Will cyber police be a good solution? Since cyber attack is an organized crime, a private company might not have sufficient resources to deal with. Moreover, cyber crime does not affect only the financial sector, but also other aspects, example national defense, weather services, education... Sorry, elections.

Elections, yeah. They are also often cross border crime. So, between cyber police in different countries share information with each other.

So, what is the thinking on that, since you've been dealing with some of the counterintelligence issues, and going back to your... We talked about academia that you've had time to think about these things. What's your general sense? Should there be a central Interpol for cyber?

Anna Puglisi: I have to say when I hear cyber police, it hits me... It makes me take a step back. And then maybe because it's much broader than a law enforcement issue in some ways, because it cuts across so many different sectors. I think I'd have to think a little bit more about how you would actually implement that. And then it still creates an “us and them”, as opposed to more of a collective, how are we going to work together across public, private, academia to really find workable solutions, and across governments as well, to find workable solutions.

And I think it comes back to some other points I made earlier, about it's the information sharing, and its awareness of how far reaching some of these are. And pushing back against... These are really norm breaking activities that undermined... We're talking about financial systems here, but really it undermines the global norms of science, when you're attacking universities. It undermines our stability issues if it gets a critical infrastructure. And so, I think it will incorporate all of those things.

Babak Abbaszadeh: Yeah. It's interesting. As you are speaking, it makes me think that you got a point there, in the sense that you don't want to duplicate, triplicate in other agencies' work. I guess a high-profile example is in the United States, you have the Southern District of New York that essentially deals with a lot of... District attorneys deals with a lot of financial crime. And so anyways, yeah. The answer is not as apparent as it appears.

Anna Puglisi: Right. Because I think gut reaction, you can say simply, "Yes, let's do that." But then thinking about, okay, how do we... We're not resource infinity also. So how do you leverage the strengths of the organizations we already have.

Babak Abbaszadeh: Yeah. And you want to avoid a cure... Sorry, a solution that is worse than the cure, right?

So, Danny, let's go to you on this one question from Humphrey. What sort of risks should supervisors be concerned about for financial institutions, which are implementing innovative, authentic products, like digital cash?

Danny Brando: It's a good question. And I think just to answer it more broadly, I think as our services, financial services are digitized and interconnected in a digital way, those risks are the same. I think we need to be looking at resiliency. How are we... The whole spectrum of the... I use the NIST Framework, but any cybersecurity framework that you want to use really to cut across, how are you looking at risk management for those services? So as things get digitized, as we move much, much more into these digital innovations, I think we just need to have strong risk management approaches to it and making sure that we're building a resilient architecture for those services.

Babak Abbaszadeh: Thank you. Socorro, for you, I'm going to try to do a hybrid of Anthony's question, and Marco’s second question. I'll do the best I can. They're not exactly the same, but they're close enough. So as emerging financial institutions like credit unions, but you can think of any other, are migrating from manual systems to digital financing, smaller jurisdictions, what major attention should they put to avoid cyber risk and become resilient? And also dealing with cyber crime? What's your general take on that? And Anthony, I'm sorry if I didn't do justice your question, but I tried to find a similarity. Go ahead.

Socorro Heysen: Well, as Danny said earlier, the innovation has to come together with risk management. If you go ahead with innovation without proper risk management, basically that's a recipe for failure. So, credit unions have to be aware that it... Or credit unions or smaller emerging market institutions, they have to be aware that as they move forward with innovation, which is something that is desirable, they have to spend the resources also to do a proper risk management of the vulnerabilities that may be created by this innovation, by this new product, by these applications.

There's no... They can not afford to do it at the same time, because it would be more costly to basically have a threat, a damaging threat that will destroy the whole company or the whole industry.

So even though it is very costly to face this risk to manage this risk properly, we cannot afford not to do it. So, there is room for collaboration, for pooling resources, and maybe even in some countries... Or since this is a global problem, for using even government resources to try to address some of these issues. Because since public, since financial inclusion is a public good, maybe there is some room to address some of these issues with public resources too. But that has to be thought and decide and all incentives have to be there to control moral hazards and all sorts of problems that come with it.

Babak Abbaszadeh: Thank you. That's great. Martin, I'm going to pose the question from Cindy Russell to you. You did bring up the question of trying to look at it from a risk-based approach. And also, in addition to securities, you have been a supervisor regulating in other sectors as well. So, I think it's a good question for you. Cindy asked, "I think presently cyber risk is seen as a subset of operational risk. What are your thoughts on cyber risk being treated as a separate, distinct risk outside of being housed under operational risk?"

Martin Moloney: Generally speaking, and this is a bit of an off the cuff answer, I would tend to be a bit skeptical about that, and I'll tell you why, because it has an awful lot to do with how organizations behave. And if you silo cyber risk as a specialist activity, it ends up with a smaller voice within the organization until the day after the successful cyber attack, and then suddenly everybody's listening. But before that, nobody's listening. If you take it as part of a broader operational resilience program within an organization, then I think that's a better envelope within which to get it to the senior decision makers within the organization and to attach yourself to budgets.

But that's me, trying to predict how organizations behave. But my instinct as a supervisor would be to be nervous about that because... and as we've increasingly looked at it, we see that the touch points... I'll give one key touchpoint, for example, is this touchpoint between cyber risk and outsourcing, and the wider group of risks relating to outsourcing. We've got a lot of financial firms which have a huge number of complex outsourcing contracts, and very often second- and third-party outsourcing contracts, and not necessarily but clear visibility as to all the terms of those arrangements. Now, those arrangements are inherently... They've got cyber risk in them, because you connect all those suppliers up to your systems, or you usually do. And what do you do, and how do you manage that in a holistic way, if you have put cyber risk over in a corner? I think it'll turn out badly.

Babak Abbaszadeh: Okay. Well, thank you for that. I'm going to, Danny, give you the last question, make it hybrid, anonymous and Humphrey's first question. So essentially, should regulators supervisors' scope be expanded to include non-financial institutions, providing financial services? For example, many telecoms, FinTech firms provide digital financial services. And carrying on with Humphrey, what risk should supervisors be concerned about for financial institutions, which are implementing innovative FinTech products? So, the way I'm looking at this is you're talking about the entity that might be regulated as a financial institution, and the activity of, let's say, a telco that is a financial, but the entity itself regulated, that activity is not. What's

your general sense in that, in terms of dealing with that in the world of cyber?

Danny Brando: So, I'm going to cheat a little bit and first answer a little bit... I'm going to tack onto Martin's question and answer a bit, because I agree completely with Martin that I do think cyber belongs under the operational risk umbrella, but maybe to highlight something that I think was behind the question, is how to make sure that cyber risk isn't buried into an operational risk. Let's just solve the broader operational risk problem, and then we don't have to worry about cyber so much. I think there's middle ground. I think there's a way of highlighting and saying that there's a large gap in cyber risk management that needs to be focused on, while keeping it under the operational risk umbrella.

As far as the FinTech and digital, as I mentioned earlier, I think solid risk management as we're introducing new digital products like this is critical. As far as whether they should be regulated or... Regulators and supervisors should expand their scope to include them, that's probably beyond my area of expertise on how to design that properly, but I am a supervisor. So, I would say that maybe I'm biased, but I do believe that supervision and regulation is important, and they should be supervised in some way and regulated in some way. Where or how that happens, again, it's probably outside of my expertise.

Babak Abbaszadeh: Okay. Thank you. So, I think we're coming to the close. One of the things you always want to do in Toronto Centre is end the sessions on time so that you guys come back, both the speakers and the audience. And you certainly exceeded our expectation in terms of making a session very lively.

And for those of you who ask questions, and we didn't answer your questions, please don't feel bad. We are saving your questions. We will deal with them one way or another, to our courses, this will be your contributions to our work. And in some cases, we may actually try to get back to the audience on this or cover it in other forums.

It's a very difficult time, as supervisors have a lot on their plates, and they never get a positive press release for whatever they do, but they always get a finger of blame pointed at them. And every time there's a crisis, ministers of finance seem to be okay, but they either in some countries go to jail or whatever. And they have to continuously look at how to deal with emerging risks as they're appearing.

Babak Abbaszadeh: And thank you very much for very coherently and clearly explaining your points in a simple way that all of us can understand, plain speaking. And don't be surprised if we come back to our speakers and involve you in some other things. So, thank you again. You have our gratitude.