Rannveig Sigurdardottir
Deputy Governor, Central Bank of Iceland
Introductory remarks
Third Annual Nordic Cyber in Finance Conference
28 November 2019
Stockholm

Panel – Cyber-Risk Governance (morning session)

I welcome the opportunity to be here today and participate in this conference on Cyber in Finance, and I am especially delighted to have a chance to participate in this panel on *Cyber Risk Governance*. Unfortunately, figures show that cyberattacks are on the rise, and consequently, so is our awareness of how threatening cyber-risk is to institutions, markets, and society as a whole.

Cyberattacks are difficult to foresee; indeed, some say that we are always behind the curve when it comes to cyberattacks. But one thing we can do is have a proper framework in place when they do occur, so as to prevent them from escalating to a systemic level.

It is widely accepted that sound governance is a key factor in in countering cyberattacks. And this is consistent with other forms of risk management.

But what are the ingredients for good cyber-governance?

Good cyber-governance entails ensuring that a proper cyber-resilience framework is available and endorsed by an institution's board or equivalent body – a framework consisting of policies, procedures, and controls aiming to identify, protect, detect, respond to, and recover from a cyberattack. The framework should accord high priority to the safety and efficiency of the institution's operations while supporting broader financial stability objectives.

The framework should also be guided by a cyber-resilience strategy that defines how cyber-resilience objectives are determined and identifies the people, processes, and technology requirements for managing cyber-risks.

The fact that cybercrime is a relatively new category of operational risk – one that is driven by highly innovative criminals – means that an event like this one is of vital importance in raising awareness and sharing information and best practices. We still have much to learn when it comes to cyber-risks and how to manage them.

And in the spirit of information sharing, I would like to share with you some of what is happening on the small island of Iceland, a country with 350,000 inhabitants that operates one of the world's smallest central banks.

The Parliament of Iceland has just recently passed a law that implements the NIS Directive (Net- and Information Security Directive). That law will enter into force in September 2020. Until then, a constructive mapping of who may fall under the scope of the new law is to take place.

With respect to the banking sector and financial market infrastructure, the new law entrusts the Financial Supervisory Authority with deciding this. At the same time, the Central Bank of Iceland has both an oversight role to play and the duty to promote a sound and efficient financial system – a role it can only fulfil by promoting proper cyber-risk governance.

And to conclude, these are also interesting times for the aforementioned institutions: on 1 January 2020, the Central Bank of Iceland and the Financial Supervisory Authority will merge into a single institution under the name of the Central Bank of Iceland. For a nation of 350,000, the merger will give us the opportunity to perform more effectively in the field of cyber-resilience for the financial market and to promote the importance of proper cyber-risk governance. Furthermore, the Central Bank of Iceland plans to launch a Financial Sector Forum for Operational Robustness in 2020, with emphasis on enhancing the sector's resilience against cyberattacks. Having said this, I look forward to fruitful discussions and to this afternoon's session on how to increase cyber-resilience in finance.