Steven Maijoor: Managing climate and environmental related risk - stepping up the pace

Speech (virtual) by Mr Steven Maijoor, Executive Director of Supervision of the Netherlands Bank, at Afore Consulting's 7th Annual FinTech and Regulation Conference, 8 February 2023.

* * *

Hello everyone.

Almost ten years ago, in 2014, an article on 'the secret life of passwords' was published in the New York Times.[1]

The author of the article, Ian Urbina, was fascinated by what people use as passwords. And after collecting stories about passwords for some time, he heard about scholarly research on a gigantic password hack. A few years earlier, in 2009, a database of 32 million passwords had been published on the internet. And this triggered a group of academic researchers from the University of Ontario Institute of Technology to start analysing the database. Not only with a security focus, but also with a linguistic, psychological and anthropological focus.

And they found that for every ten passwords, one turned out to be a name, or a name plus a year. For every 1000 passwords, two turned out to be the word- "password". And the most commonly used verb turned out to be to "love" – tellingly, more often in combination with a man's name than with a woman's.

None of these popular passwords are safe options, of course. So it is no wonder that the overall conclusion one of the researchers drew, was not overly optimistic. He was worried about the fate of our privacy. To him, "the database made clear that humans really are the weak link when it comes to data security."

This was almost ten years ago. A lot has happened since then. Today, when you log in on your device, you often still use a password, but probably in combination with facial recognition, fingerprints, or a piece of unique hardware.

Unfortunately, however, humans remain the weak link in data security.

Last year's Global Risks Report from the World Economic Forum[2] says that 95 percent of cybersecurity issues can be traced back to human errors.

The report also says that, in 2020, there was an increase of 435 percent in ransomware compared to 2019. Many of you are probably familiar with the ransomware attack on a big American insurer a few years ago. This insurer ultimately had to pay 40 million dollars to retrieve its data and regain control of its systems.

The report also says that, worldwide, we will need three million additional cyber professionals to adequately protect our data – professionals for cyber leadership, to test and secure systems, and to train people in digital hygiene.

From my perspective, as a supervisor with De Nederlandsche Bank, I can only underscore the urgency to act that speaks from this report.

My aim is to safeguard trust in the financial system. And cybercrime, be it a data leak or ransomware or any other form, poses a significant threat to that trust. What happened to the Central Bank of Bangladesh in 2016 was a loud and clear reminder.

But it is, of course, no wonder that cyber threats are on the rise.

Over the years, financial institutions have been morphing more and more into IT companies with a banking licence. More and more of what financial institutions do, happens digitally. As a consequence, the IT infrastructure has become more and more essential to the functioning of the financial institution as a whole. In the past, it was the vault with cash and coins that needed protection – today, it's the digital infrastructure.

Three other evolutions further complicate effective protection of data and operational continuity.

First, there is the increasing interconnectedness between financial institutions. They rely on each other for many services, including handling transactions, balances, clearing and settlement. A disruption at one financial institution could have consequences for another.

Second, the increasing digital dependency on specialised third parties – for instance for cloud solutions, payment systems, or security operation centres. Often, this makes sense – if only for the economies of scale that come with outsourcing. But by now, we have reached a point where a significant number of financial institutions are highly dependent on third party services for some of their vital processes. And this creates a potential security threat. If an external party were to fall victim to cybercrime, this could permeate through the entire financial system with severe results.

The third evolution is that only a few specialised and increasingly dominant providers handle the majority of outsourced services and processes. And some of them are definitely very well equipped to counter cyberattacks. Nevertheless, with this evolution comes a concentration risk. If one of those service providers were to encounter operational difficulties or get hacked, a lot of its financial clients might experience difficulties.

Across the board, it is safe to say that as the digitalisation of financial services increases, and the subsequent interconnectedness, dependency and concentration along with it, the more difficult it becomes for a financial institution to estimate if, how and when it runs the risk of a cyberattack.

Let me now turn to the Netherlands.

In its studies from 2021 and 2022, De Nederlandsche Bank found that, on average, five percent of financial institutions in the Netherlands had to deal with the repercussions of a successful cyberattack at some point. "Successful" in this case does not necessarily mean that corporate operations were in danger or that data was stolen, but it does mean that there was a security breach.

But overall, it remains hard to pinpoint exactly how many cyberattacks occur in the Netherlands, and what the success rate is.

So that begs the question: how well-prepared for cyberattacks is the Dutch financial sector?

The TIBER-NL program, developed and coordinated by De Nederlandsche Bank, gives us an idea.

TIBER is short for threat intelligence-based ethical red teaming. Financial institutions participate voluntarily in staged test attacks, using them to gauge their cyber resilience. The aim is to gain insight into strengths and weaknesses, and to identify areas for improvement. Afterwards, they share experiences and improvement plans with other institutions.

Over the past five years, De Nederlandsche Bank has coordinated over 40 TIBER tests on vital Dutch institutions. And in many of the cases, ethical hackers successfully accessed critical parts of the financial institutions' systems.

The results of the TIBER tests have led financial institutions to take measures to increase their cyber resilience. But the results also tell us that we need to remain vigilant at all times.

I am pleased that our TIBER program has inspired the European Central Bank to draw up the TIBER-EU Framework. This is important. Because increasing cyber resilience will, at least partly, need to happen on a European level. Simply because cyberattacks know no borders.

That is why I am also very pleased with the finalisation of the Digital Operational Resilience Act – DORA. From 2025 onwards, financial institutions will have to comply with this European regulation aimed at increasing cyber resilience. This means, among other things, that third parties will have to comply with certain cyber security criteria. Hence, they will become part of the supervisor's scope.

With TIBER, we already have an instrument that supervisors could use to broaden their scope from financial institutions to third parties. But even with such an instrument at hand, successful supervision will always require a degree of adaptability – it will always require the capacity to identify and understand new risks and threats, and adapt accordingly. To successfully do this, consistent and constructive collaboration between financial institutions, third parties, and supervisors, will remain at the heart of cyber resilience.

Another part of DORA is that a financial institution's leadership will need to be highly involved in cyber security. This is fully in line with what De Nederlandsche Bank has been working on for some time now – increasing the boardroom's cyber knowledge and expertise. Whenever corporate digital strategy is discussed, somebody who knows the ins and outs of cyber security should have a seat at the table.

So, I am very pleased with the regulatory advancements. But, compliance alone is not a financial institution's recipe for success. However important, it is a mere ingredient.

Financial institutions themselves are responsible for the entire recipe. And just as a professional kitchen can't operate without basic ingredients like salt and pepper, a financial institution must have its basic cyber security ingredients in place. Without the salt and pepper of cyber security, a financial institution is a sitting duck for cyberattacks.

You could think, for instance, about drafting and implementing a security policy – a policy that explicitly describes who gets access to your offices, how people should protect their hardware and software, and how new employees should be screened. Or how digital vulnerabilities, like necessary software updates, are managed. Or whether a cyber security crisis plan and team are set up.

And most importantly, the basic ingredients of cyber security should not just be put in writing. They should not just be items on people's to-do list. Everyone, from staff to top management, in-house or third party, everyone must understand why this is important.

The article on the 'secret life of passwords' I talked about a few minutes ago, reveals how important the why is for people.

The author of the article spoke to dozens of people about their passwords, and he found that a lot of passwords have rich background stories. A lot of passwords are a motivational mantra. A lot of them are a daily reminder of something important, someone important.

Of course, this is exactly what makes passwords potentially unsafe. This is exactly what hackers aim for. This is exactly why, more and more often, additional safety features are used – like facial recognition or fingerprints.

But the answer to diminishing the weak link in cyber security – which is us, humans – might not be to take away meaning, but, on the contrary, to build on it.

Today,

- the complexity people have to deal with is increasing sharply, just like the complexity of the financial landscape;
- the number of third parties is increasing, just like the interconnectedness and the dependency;
- the complexity of cyber threats is increasing, just like the measures to prevent them;
- and it is hard to predict when or where the next cyberattack will hit, but chances are that it will have to do with a human error.

And so, it is all the more important that people, in all layers of an organisation, know the why of it all. Why they need to follow certain processes and procedures. Why they should preferably use meaningless passwords. Why they need to protect themselves – and with that, their colleagues, their institutions, and the whole financial system.

Here lies a great responsibility for financial institutions – the responsibility of giving meaning. But one thing seems clear – cyber resilience should definitely not lead a secret life. It should very much lead a human life.

Thank you.

[1] Ian Urbina 2014, *The Secret Life of Passwords,* The New York Times, accessed on 24 January 2023, < The Secret Life of Passwords - The New York Times (nytimes.com) >.

[2] World Economic Forum 2022*, The Global Risks Report 2022* (p.45-56), World Economic, accessed 24 January 2023,