FSB FINANCIAL STABILITY BOARD

As prepared for delivery

Cyber security: finding responses to global threats[1]

G7 2019 Conference: Cybersecurity: Coordinating efforts to protect the financial sector in the global economy

Banque de France, Paris, 10 May 2019

Remarks by Dietrich Domanski, Secretary General, Financial Stability Board

Firstly, many thanks to the French G7 Presidency for organising this conference. In my brief remarks this morning I would like to recall the case for international cooperation on cyber security, highlight important challenges for cooperation, and discuss the FSB's work to promote cyber security against this backdrop.

The case for international cooperation

The case for international cooperation on cyber security in the financial sector is strong, and perhaps even stronger than in other areas of regulation.

One reason is that cyber threats to the financial sector are global by the power of two. Cyber risks themselves are global. They can originate anywhere and affect anybody around the globe. And cyber attacks target a financial system that is highly interconnected globally – through financial infrastructures, but also through cross-border exposures and foreign operations of different financial institutions.

The 2016 attack on the Bangladesh Bank illustrates this: the incident affected institutions in Bangladesh, Belgium, the Philippines, Vietnam and the United States; it affected a central bank, commercial banks and a major global financial infrastructure.

Another reason why cooperation is so important is that the financial sector is a preferred target of cyber attacks – both for financial and symbolic reasons. IBM estimates that 19% of all cyber attacks and incidents in 2018 were focused on financial services, more than any other sector.[2] Threats are rapidly evolving and increasingly sophisticated and able to impact institutions of all sizes and targeting the weakest link in the network.

Challenges for international cooperation

There are also significant challenges for international cooperation. First and foremost, there are a whole host of issues around the sharing of information related to cyber risks and security. One aspect is confidentiality and commercial sensitivity of information, some of which, for

---

1 The views expressed are those of the speaker and not necessarily those of the FSB or individual FSB members.

2 IBM, *X-Fore Threat Intelligence Index*, 2019

instance on cyber defences or identified vulnerabilities may even touch on national security concerns. Another, closely related aspect is trust, which may take time to build.

More generally, the rapid evolution of cyber threats raises the question as to whether cooperation processes are sufficiently agile to be fully effective, both in terms of speed, and in terms of involvement of relevant stakeholders.

These are difficult challenges. But they are also not fundamentally different from those that international regulatory and supervisory cooperation had to deal with in the past.

The fact that cooperation on cyber security at early stages put a particular onus on three aspects of cooperation: enhancing mutual understanding of the issues; ensuring that there is a common language that facilitates effective communication between authorities and the private sector; and seeking to identify possible solutions and make progress in areas where confidentiality of information is less of an issue.

The FSB's work on cyber security

The FSB agenda on cyber security has evolved along these lines.

First, on enhancing mutual understanding. In 2017, the FSB took stock of financial sector cyber security regulations, guidance and supervisory practices.[3] This work catalysed discussions around cyber security within the FSB, and it also informed, in the form of a public report, the public debate.

Second, on helping to build a common language, the FSB in 2018 published a cyber lexicon to support the work of the FSB, standard-setting bodies, authorities and private sector participants to address financial sector cyber resilience.[4] The Lexicon comprises a set of approximately 50 core terms related to cyber security and cyber resilience in the financial sector. Since November, the Lexicon has been downloaded about 3,000 times. This is a large number for a technical document and shows the demand for this kind of product.

Third, on finding solutions, the FSB is currently developing effective practices for cyber incident response and recovery. The objective is to identify a set of tools that the private sector and authorities can use in designing incident response and recovery policies. We will publish a survey next month which will feed into this work and we will consult on the report early next year.

And, last but not least, the FSB will also continue to discuss issues related to cyber risks as part of its ongoing work to assess vulnerabilities in the financial system.

Concluding remarks

The prize for successful cooperation on cyber security is big, both in terms of greater resilience and in preventing fragmentation. But so are the challenges. What is called for is a combination

[3] FSB, *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*, October 2017
[4] FSB, *Cyber Lexicon*, November 2018

of ambition and a clear recognition of the importance of the specific challenges around confidentiality, trust, and speed. Bearing these in mind, successful cooperation is possible. The FSB has shown that.