Cyber risk in central banking

Author:Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros, David Whyte

Date:2022-09-14

Keyword:central banks, financial institutions, cyber risk, cloud services, cyber regulation

Attachment:[Link](https://www.bis.org/publ/work1039.pdf)

From:[BIS-working\_paper](https://www.bis.org/publ/work1039.htm)

Summary

Focus

Cyber attacks are becoming ever more frequent and sophisticated, and firms and policymakers list cyber risk as a major concern. Financial institutions and financial market infrastructures are especially at risk, and the financial industry ranks consistently as one of the most-attacked industries. While there have been several studies and surveys on cyber threats for the private sector – and firms in the financial sector in particular – little is known about central banks' assessment of cyber risk.

Contribution

We use a survey conducted in 2021 among the members of the Global Cyber Resilience Group to provide an overview on cyber risk in the central bank community. The survey contains responses from 21 central banks from all regions of the world. It examines the following questions: What are central banks' main cyber concerns, and how do they see the threat landscape? What measures do they take to pre-empt or counter cyber attacks? And how do they assess the risks to and the readiness of the financial sector at large?

Findings

We uncover four main insights. First, central banks from advanced economies and emerging market economies assess the frequency and costs of different cyber attacks differently. Second, central banks actively discuss and develop policy responses to cyber attacks and have significantly increased their cyber security-related investments. Third, central banks deem the potential losses from a systemically relevant cyber attack in the financial sector to be large, especially if it targets a big tech providing critical cloud infrastructures. Only a few central banks fully agree that the financial sector is adequately prepared for cyber attacks, and over half of the respondents think that the sector's investment in cyber security has been inadequate over the past year. And fourth, central banks already cooperate widely on a range of topics related to cyber risk, for example in developing sound principles for cyber resilience, creating a specific coordination centre for knowledge-sharing and developing common projects to limit cyber threats.

Abstract

The rising number of cyber attacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policy makers. This paper presents the results of a survey among members of the Global Cyber Resilience Group on cyber risk and its challenges for central banks. The survey reveals that central banks have notably increased their cyber security-related investments since 2020, giving technical security control and resiliency priority. Central banks see phishing and social engineering as the most common methods of attack, and the potential losses from a systemically relevant cyber attack are deemed to be large, especially if the target is a big tech providing critical cloud infrastructures. Generally, respondents judge the preparedness of the financial sector for cyber attacks to be inadequate. While central banks in most emerging market economies provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in advanced economies do. Cooperation among public authorities, especially in the international context, could improve central banks' ability to respond to cyber attacks.

JEL classification: E5, E58, G20, G28.

Keywords: cyber risk, central banks, financial institutions, cloud services, cyber regulation.