FSB FINANCIAL STABILITY BOARD

Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence

Available as: PDF

19 October 2021

> Cyber incidents remain a threat to the financial system and are rapidly growing in frequency and sophistication.

This report explores whether greater convergence in the reporting of cyber incidents could be achieved in light of increasing financial stability concerns, especially given the digitalisation of financial services and increased use of third-party service providers.

Following a stocktake of existing supervisory and regulatory practices, the FSB found that fragmentation exists across sectors and jurisdictions in the scope of what should be reported for a cyber incident; methodologies to measure severity and impact of an incident; timeframes for reporting cyber incidents; and how cyber incident information is used. This subjects financial institutions that operate across borders or sectors to multiple reporting requirements for one cyber incident. At the same time, financial authorities receive heterogeneous information for a given incident, which could undermine a financial institution's response and recovery actions. This underscores a need to address constraints in information-sharing among financial authorities and financial institutions.

Recognising that information on cyber incidents is crucial for effective actions and promoting financial stability, the FSB has identified three ways that it will take work forward to achieve greater convergence in cyber incident reporting:

- Develop best practices. Identify a minimum set of types of information authorities may require related to cyber incidents to fulfil a common objective (e.g. financial stability, risk assessment, risk monitoring) that authorities could consider when developing their cyber incident reporting regime.
- Identify common types of information to be shared, understand any legal and operational impediments to sharing such information, and continue efforts to reduce such barriers.
- Create common terminologies for cyber incident reporting, in particular a common definition for 'cyber incident'.

The report notes that greater harmonisation of regulatory reporting of cyber incidents would promote financial stability by:

i. building a common understanding, and the monitoring, of cyber incidents affecting financial institutions and the financial system;

ii. supporting effective supervision of cyber risks at financial institutions; and

iii. facilitating the coordination and sharing of information amongst authorities across sectors and jurisdictions.

By end-2021, the FSB will develop a detailed plan for taking this work forward.

Press Release

FSB calls for greater convergence in cyber incident reporting

19 October 2021

Greater harmonisation in cyber incident reporting would promote financial stability, especially given the digitalisation of financial services and increased use of third-party service providers.

Related Information

Effective Practices for Cyber Incident Response and Recovery: Final Report

19 October 2020

A toolkit of effective practices for cyber incident response and recovery.

Cyber Lexicon

12 November 2018

A lexicon to support work of the FSB and others to address financial sector cyber resilience.

Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices

13 October 2017

Conclusions from the FSB's cybersecurity stocktake delivered to the G20.