ESRB
European Systemic Risk Board
European System of Financial Supervision

Press release

27 January 2022

ESRB recommends establishing a systemic cyber incident coordination framework

The European Systemic Risk Board (ESRB) has today published a Recommendation for the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF). The financial sector relies on resilient information and communications technology systems and is highly dependent on the confidentiality, integrity and availability of the data and systems it uses. Major cyber incidents have the potential to corrupt information and destroy confidence in the financial system, and they may therefore pose a systemic risk. This calls for a high level of preparedness and coordination among financial authorities in order to respond effectively to such major cyber incidents. The EU-SCICF would aim to strengthen this coordination among financial authorities in the European Union, as well as with other authorities in the Union and key actors at international level. It would complement the existing EU cyber incident response frameworks by addressing the risks to financial stability stemming from cyber incidents.

The ESRB report "Mitigating systemic cyber risk" explains in detail how the EU-SCICF would facilitate an effective response to a major cyber incident. Building on the ESRB report published in 2020, Systemic cyber risk, the report also assesses the ability of the current macroprudential framework to address the risks and vulnerabilities stemming from systemic cyber risk. It concludes that the macroprudential mandate and toolkits of financial authorities need to be expanded to include cyber resilience.

The report proposes a macroprudential strategy that should contribute to a better mitigation of the risks to financial stability stemming from cyber incidents. A monitoring and analytical framework for systemic cyber risk needs to be implemented to help design and calibrate this new set of macroprudential tools on cyber resilience. For example, testing the cyber resilience of the financial system through scenario analysis can show how systemic institutions in the financial system would respond to and recover from a severe but plausible cyber incident scenario. To draw conclusions from such cyber resilience stress tests on financial stability, macroprudential authorities need to set an acceptable level of disruption to operational systems that provide critical economic functions. It is also important to increase the understanding of systemic cyber risk-related vulnerabilities and contagion channels in the financial system. To this end, systemically important nodes at financial and operational levels should be identified – including third-party providers.

European Systemic Risk Board
Directorate General Communications, Global Media Relations Division
Sonnemannstrasse 20, 60314 Frankfurt am Main, Germany
Tel.: +49 69 1344 7455, email: media@esrb.europa.eu, website: www.esrb.europa.eu

ESRB recommends establishing a systemic cyber incident coordination framework

The ESRB and its dedicated European Systemic Cyber Group (ESCG) intend to explore a monitoring and analytical framework for systemic cyber risk and the required tools to address this risk in their future work. This work will focus on testing the cyber resilience of the financial system through scenario analysis and the definition of expectations for acceptable levels of disruption.

For media queries, please contact William Lelieveldt, tel.: +49 69 1344 7316.

European Systemic Risk Board
Directorate General Communications, Global Media Relations Division
Sonnemannstrasse 20, 60314 Frankfurt am Main, Germany
Tel.: +49 69 1344 7455, email: media@esrb.europa.eu, website: www.esrb.europa.eu