

# MEMORANDUM



Date 2021-03-02  
Author Finansinspektionen

FI Ref. 20-3685

Finansinspektionen  
Box 7821  
SE-103 97 Stockholm  
[Brunnsgatan 3]  
Tel +46 8 408 980 00  
Fax +46 8 24 13 35  
finansinspektionen@fi.se  
www.fi.se

## Cyber threats and financial stability – FI’s role and assignments

### Summary

In recent years, a number of legislative proposals and other initiatives have been presented with the aim of strengthening the financial sector’s resilience to cyberattacks. Given this background, Finansinspektionen (FI) has prepared this memorandum to describe FI’s role in terms of contributing to strong cyber security and its work to prevent cyber threats to the Swedish financial sector.

The digital developments of the past few decades have introduced considerable opportunities, but they also place demands on managing the risks that accompany them. These risks are also enhanced by a security policy that is somewhat impaired. FI notes that cyber threats are an obvious risk that every financial firm must manage for their own interests. We also note that there are risks of negative externalities, in other words that individual firms do not face incentives to fully consider how a cyberattack on an individual firm can affect the economy. Thus, the same fundamental justifications exist for FI to take action in this area as for the risk of a traditional financial crisis.

Because the financial sector is highly digitalised, cyber security has become an important topic for financial firms in recent years. Given the central role the financial sector plays in society, cyber security in the financial sector is highly relevant for society as a whole. Given that financial firms and markets are closely linked to one another, and that potential problems could therefore spread quickly, the need for cooperation in this area is even larger. In light of this background, the authorities’ cooperation to combat cyber risks in the financial sector must be enhanced.

FI, through current legislation, already has several tools for managing cyber risks in the firms under its supervision. The authorisations vary, however, for each sector in the financial market. In late 2020, new rules were proposed within the EU that will have an impact on the supervision of financial firms’ cyber risks. The Swedish defence is also undergoing a reconstruction. This places demands on authorities, including FI, to take measures that will increase resilience to cyber risks.