ARTICLE – Cyber risks and financial stability

The digitalisation of the financial sector has exposed its participants to cyber risks. In addition, the participants are closely interconnected both economically and technically. There is consequently a risk that a cyber incident happening to an individual participant could have consequences for the financial system's ability to maintain its basic functions. This means that cyber risks can also threaten financial stability. The individual participants in the financial sector must therefore have a high level of cybersecurity, but it is also important that the stability authorities contribute by ensuring that a systemic perspective is taken into account in the financial sector's work on cybersecurity. A systemic perspective is also required at the national level to increase society as a whole's resilience to cyber incidents.

Cyber risks can threaten the stability of the financial system

Digitalisation brings great benefits. But it also exposes the financial sector to cyber risks, i.e. risks that can have a negative impact on the IT systems used or on the data stored or transferred in the systems.[129]

International developments in recent years, not least the changed security situation in Sweden's neighbouring area, have also contributed to an increase in cyber threats for Sweden, as well as for participants in the financial sector.[130]

Concentration and interconnectedness can affect the stability of the entire financial system

The financial system consists of a multitude of participants and markets and a plethora of interconnections between them. Several factors in the structure of the system can contribute to its vulnerability to cyber risks. The concentration of economic functionality, IT systems and suppliers is one such factor. For example, the concentration of an important economic functionality among a small number of participants can increase vulnerability. This is because the entire functionality can then disappear from

[129] For a widely used definition of cyber risk and related concepts, see, for example, "FSB Cyber Lexicon", November 2018, Financial Stability Board.

[130] How a cyberattack could affect financial stability in Sweden is described by Elestedt, L. et al. "A cyberattack can affect financial stability", *Economic Commentaries* No. 8, 2020, Sveriges Riksbank.

the financial system even if only a few participants suffer an IT incident. Similarly, vulnerability can increase if different participants in the financial sector rely on the same or very similar IT systems, whether hardware or software. This is because if there is a weakness or vulnerability in a certain type of system, there is a risk that it will quickly affect considerable parts of the financial sector. Moreover, it may be the case that several different participants rely on the same provider of a certain type of IT service (such as a specific cloud service or a specific provider of IT operations) and that a cyber incident at this provider may have repercussions for several participants at the same time.

In addition to concentration, technical and economic interconnectedness among financial sector participants can also increase vulnerability. This is because IT incidents can spread from individual participants and IT systems to eventually affect financial stability.

In order to reduce systemic risks, financial sector participants must have a high level of cybersecurity.

A high level of cybersecurity is achieved by working in several different dimensions

To reduce the cyber risks to which the financial system is exposed, it is important that participants in the financial sector have a high level of cybersecurity. Achieving a high level of cyber security involves working in several different dimensions. For example, it is important that the IT systems have a high level of protection, that the participants in the financial sector have the ability to detect and respond to IT incidents and that they have the preparedness and ability to quickly and safely restart systems and restore data.

A high level of protection against cyber incidents in the IT systems reduces the risk that the systems, or data in the systems, will become inaccessible or that data will be inappropriately disseminated or modified. The IT systems that support the basic functionality of the financial system need to have protection that is designed to withstand cyberattacks on a par with those that can be carried out by state actors or state-sponsored actors. This high level of protection needs to be in place regardless of whether the financial company providing the basic functionality is responsible for the operation of the IT system or whether there is an external service provider.

In order to examine their systems and get a picture of how protection can be improved, it is important that participants continuously carry out different types of tests, such as penetration tests, both in individual systems and in the entire IT environment.

Regardless of the level of protection achieved in IT systems, it is virtually impossible to completely avoid IT incidents. However, it may be possible to limit the damage if one has the ability to detect and respond to IT incidents. For example, this may mean having a function that monitors IT systems 24 hours a day, every day of the year, and provides a clear and early warning if an incident is detected or if there are signs that

could indicate that an incident is imminent. Such a function needs both access to information from the IT systems, such as security logs, and access to systems that analyse the information and immediately signal if signs of an IT incident are detected. Participants providing IT systems that have a direct impact on the basic functionality of the financial system may also explore the possibility of accessing advanced technical detection and warning systems.[131]

Having the ability to respond to IT incidents can mean, for example, that participants have access to resources that can continuously counteract cyber incidents regardless of the time of day or day of the year and that they have access to human resources that can investigate, at short notice, how the incident has arisen and what consequences it has had or may have.

As with the testing of protection in IT systems, it is important to continuously test and practice the ability to detect and respond to cyber incidents. For example, as part of such tests to examine both protection and the ability to detect and remedy cyber incidents, participants that are systemically important to the Swedish financial system can conduct threat-based penetration tests, known as TIBER tests.[132]

In the event of a serious IT incident, there needs to be a high level of preparedness and ability to quickly and safely restart systems and restore data that is reasonably certain to be correct.[133] This may mean, for example, that one has several updated backup copies of data and sometimes entire IT systems where at least one of the copies has such protection that it cannot be affected by the same IT incident as regular systems and other copies. One can also have routine descriptions of how IT systems should be restarted after a serious IT incident, along with routine descriptions of how data should be restored, even in a serious scenario where the regular IT environment is not available.

Just as it is possible to carry out different types of test to assess both the security and the ability to detect and fix problems in IT systems, it can be useful to carry out tests and exercises when it comes to restarting systems and restoring data from backup copies.

Financial sector stakeholders need to ensure that cybersecurity efforts continuously address these dimensions and that resilience to cyber risks is continuously enhanced.

[131] Finansinspektionen has previously indicated that the technical detection and warning system (TDV) of the National Defence Radio Establishment (FRA) could increase the cyber resilience of systemically important participants in the financial sector (see Report "Förstärkt digital motståndskraft hos företag i den finansiella sektor" [Strengthening digital resilience of financial sector companies], Finansinspektionen, 6 May 2022).

[132] TIBER is a framework for conducting threat-based penetration tests and has been implemented both at EU level (see e.g. TIBER-EU Framework, May 2018, ECB) and in Sweden (see *TIBER-SE Implementation Guide*, December 2019, Sveriges Riksbank) and other countries. The Riksbank has developed the Swedish implementation of the TIBER framework and coordinates the TIBER tests in Sweden.

[133] There are different guidelines on how long outages can be tolerated (see, for example, the summary in *Advancing macroprudential tools for cyber resilience*, February 2023, Financial Stability Board).

A systemic perspective is also needed to safeguard financial stability.

Action by individual participants is not enough

It is of great importance that all participants in the financial sector work continuously and over the long term to reduce cyber risks and increase resilience. But this is not enough to ensure that the resilience of the financial system as a whole is sufficiently high. As a complement, there also needs to be a system-wide perspective in the work. One reason for this is that cybersecurity can be seen as a common benefit in the financial system. This means that an initiative aimed at benefiting an individual participant can also have positive effects on the entire financial system's resilience to cyber incidents. When no systemic perspective is taken on cybersecurity, participants become encouraged to act from their own perspectives, which can result in too low a level of resilience in the system as a whole.

Systemic perspective in the financial sector

A first measure to safeguard the systemic perspective in the financial sector is to map how the system's various central economic functions are interrelated and how they, in turn, are dependent on different types of participants and IT systems. A second measure that contributes to the management of an IT incident is for the stability authorities, on the basis of this mapping, to form an opinion as to when an incident may go from being a concern for an individual participant to becoming a concern for them as well. By identifying, in good time, when an event risks affecting the entire financial system, the authorities can intervene and counteract the system-wide consequences.[134]

Cooperation within the financial sector makes it easier to establish a systemic perspective on cyber resilience. For the stability authorities (Finansinspektionen, the Riksbank and the Swedish National Debt Office), there are several cooperation forums that can contribute to a systemic perspective. For example, they cooperate on cyber issues within the framework of the Financial Stability Council. But cooperation between authorities and private actors is also important to strengthen resilience to cyber incidents in the financial system. Some collaboration forums have already been established, for example within the framework of the group for private-public cooperation in the financial sector (FSPOS). This forum deals with issues related to cyber security. This type of cooperation needs to continue to increase the resilience of the financial system to cyber risks and incidents.

Cooperation between critical sectors

It is not only the financial sector that is highly exposed to cyber risks. This also applies to many other critical sectors, several of which can also indirectly affect the stability

[134] For more on the tools known as the Systemic Impact Tolerance Objective (SITO) the Cyber Resilience Scenario Testing (CyRST) see *Advancing macroprudential tools for cyber resilience*, February 2023, ESRB.

of the financial system. Cybersecurity is consequently a matter that also requires co-ordination at the national level.

One initiative that could strengthen resilience to cyber incidents in society at large, and thus also in the financial system, is the creation of the National Cyber Security Centre (NCSC).[135] Currently, the NCSC's work takes the form of a collaboration between four authorities within the framework of their respective mandates. Recently, it has been proposed that one of the authorities, the National Defence Radio Establishment, be given responsibility for the future operations of the NCSC.[136] One positive aspect of such a proposal is that it would create the conditions for clearer responsibility and a clearer mandate for the centre's activities. It is important to include the financial sector in the NCSC's future work to safeguard the resilience of the financial system and society as a whole against cyber incidents.

[135] The NCSC is a collaboration between four authorities: the National Defence Radio Establishment, the Swedish Armed Forces, the Swedish Civil Contingencies Agency and the Swedish Security Service. The work of these four authorities in the NCSC takes place in close collaboration with the Swedish Defence Materiel Administration, the Swedish Police and the Swedish Post and Telecom Authority.

[136] See opinion editorial by U. Kristersson et al. (2023), 27 April, DN Debatt. "FRA får ta över ansvaret för Sveriges cybersäkerhet" [National Defence Radio Establishment may take over responsibility for Sweden's cyber security].