Staff memo

Cyber risks and financial stability

Joacim Häggmark, Kristian Jönsson, Ulrika Nilsson and Johanna Stenkula von Rosen

June 2023

SVERIGES RIKSBANK

Contents

Summary

The Riksbank's work on financial stability aims to safeguard the fundamental functions of the financial system. It does so by mapping and analysing the vulnerabilities and risks that threaten these functions. The Riksbank also works to ensure that the financial system can withstand shocks. The increasing digitalisation of society, and not least the technological development in the financial sector, means that cyber risks can become systemic risks and thus threaten financial stability. In this staff memo, we illustrate how cyber-related vulnerabilities and risks can be linked to the Riksbank's work on financial stability. We also provide general examples of how cyber risks can be incorporated into a central bank's financial stability work to make the financial system more resilient to cyber-related shocks. The way that cooperation between actors in the financial sector and between different vital societal sectors can increase resilience against cyber incidents is also addressed.

Authors: Joacim Häggmark, Kristian Jönsson, Ulrika Nilsson and Johanna Stenkula von Rosen, work in the Department for Financial Stability at the Riksbank.[1]

[1] We would like to thank Karl Blom, Mattias Hector, Olof Sandstedt, Marianne Sterner and Annika Svensson for valuable comments.

1 Cyber risks have a natural place in the Riksbank's work on financial stability.

A well-functioning and stable financial system is required for the economy to function well and for the economy to have scope to grow in the long term. Several authorities, including the Riksbank, have the task of promoting financial stability. In this work, the Riksbank maps and analyses vulnerabilities and risks that may threaten stability. The Riksbank also works to ensure that the financial system is resilient to shocks. In addition, through its stability task, the Riksbank also has a specific task of overseeing financial infrastructure companies to ensure that they comply with internationally agreed standards.

The stability of the financial system means that its basic functions are maintained, enabling payments, savings, investment and risk management. Risks that threaten these functions therefore also threaten financial stability.

In the financial system, there are a variety of actors, each of which can influence the extent to which the basic functions are maintained. For example, infrastructure companies provide basic services such as enabling payments, other financial transfers and the registration of securities. Further examples are banks and other financial companies that, among other things, provide various types of payment, savings and financing services to their customers, i.e. to households and companies that are thus also important players in the financial system.

Participants in the financial system are active both in various financial markets, where trade in various financial instruments takes place, and in the real economy, where trade in goods and services takes place.[2]

There are certain types of risk that can threaten financial sector participants or markets to such an extent that the fundamental functions of the entire financial system are also threatened. Such risks are usually referred to as systemic risks.

The general digitalisation of society has been going on for a long time and the financial sector is experiencing rapid technological development. The digitalisation of society brings great benefits and advantages, such as new goods and services and more efficient and secure processes. However, digitalisation also entails exposure to risks that threaten the IT components and systems on which digitalisation is based. Digitalisation automatically entails exposure to cyber risks.

As financial system participants are directly dependent on IT components and systems for their operations, cyber risks become an important factor to consider when it comes to the basic functions of the financial system.[3] In other words, cyber risks can

[2] Elestedt et al (2021) describe in more detail the role of different actors in the financial system.

[3] See also Kashyap and Wetherilt (2019) who link cyber risks and financial stability from a macroprudential perspective, with the critical economic functions of the financial system in mind.

be systemic risks.[4] This also gives them a natural place in the Riksbank's work on financial stability.[5]

2 Cyber risks can pose a direct threat to financial stability

2.1 Availability, integrity and confidentiality essential to maintain stability

When it comes to cyber risks in general, three aspects are often highlighted in the analysis. These are the availability, integrity and confidentiality of IT systems and of data contained in the systems. The three aspects are also relevant when it comes to cyber risks and financial stability.

Availability is an important aspect when it comes to IT systems. If an important IT component were to stop working or an important IT system were no longer available, fundamental functions of the financial system could be lost. Lack of availability can therefore have a direct impact on financial stability.

But even if all components and systems are working properly, there are cyber risks that can threaten stability. This is because much of the activity in the financial system is directly dependent on accurate information on, for instance, prices and balances, i.e. on the integrity of the data. If the information were no longer accurate, it could have a direct impact on various participants and markets. This would also affect the financial system and its ability to supply basic functions.

The third aspect of cyber risk, confidentiality, relates to whether information in a system is accessible to unauthorised persons. In this case, the direct link to financial stability is less obvious. However, confidentiality can still have a bearing on financial stability, but then instead through the indirect links discussed below.

2.2 A high concentration of economic functionality or of IT systems can increase vulnerability.

An IT incident, or disruption as it could be called in financial stability work, that has a direct impact on the basic functions of the financial system can take several different forms. For example, a particular central IT system may be affected by a disruption at the same time as there are no alternatives in the financial system that can deliver the same economic function. But a disruption can also have an effect by simultaneously

[4] Adelmann et al (2020), ESRB (2020), ESRB (2022), Fell et al (2022), Koo et al (2022) and Elestedt et al (2021), for example, focus on cyber attacks and emphasise that they can pose a systemic risk. In addition, Maurer and Nelson (2021) express the view that it is only a matter of time before a cyber attack will have repercussions on financial stability.

[5] For example, based on the analytical framework presented by the ESRB (2020), Elestedt et al (2021) discuss in detail how a cyber attack can directly and indirectly affect financial stability.

affecting several different systems that, in a normal situation, could constitute alternatives to each other to achieve a certain economic function. It is also possible to imagine a disturbance in an IT system where the function can initially be achieved in another system, but where the disturbance gradually spreads to the other systems and thus gradually undermines financial stability.

The different aspects of cyber risk and types of disruption illustrate how different arrangements and measures may be needed to strengthen financial stability. If there is no interchangeability in the financial system with regard to a particular IT component or system, and if the same economic function cannot be achieved elsewhere in the economic system, it becomes crucial that the component or system has a high level of IT security. This means a very good ability to protect against incidents. But this is not sufficient. It is also important that any IT incidents can be detected and mitigated at an early stage. Moreover, it is important to be able to quickly restore or replace the components or systems affected by an incident that has affected or risks affecting the stability of the financial system.

When it is difficult to replace a component or a system to achieve a certain function, efforts need to be made to develop alternatives that can take over the basic economic functions that risk being lost in the event of an IT incident. Seen from a system perspective, such work need not only focus on developing alternatives to an individual IT component or an individual IT system for a specific actor; a central starting point could instead be how best to find alternatives that promote the stability of the entire financial system.

In cases where different IT systems and actors are interchangeable, a different set of arrangements and measures may be needed to safeguard financial stability. While it is of course still important to maintain IT protection for the various IT systems that contribute to the basic economic functions, it may also be important to recognise which factors mean that several computer systems suffer problems at the same time. For example, if several systems operate in the same location, with the same software or hardware, or are dependent on the same service providers, they could be more likely to suffer a disruption at the same time. By knowing the factors that contribute to several systems being affected by a disruption at the same time, there are better conditions for reducing the financial system's vulnerability to cyber risks.

Sometimes there may be a risk that an initial disturbance in an IT component or system may spread to other components and systems. In such cases, in addition to the two aforementioned aspects, it is important to be aware of the possible propagation paths between components and systems that are important in the financial sector, and to have plans to be able to shut down such propagation paths if necessary.

On the whole it is important in the work on financial stability to pay attention to vulnerabilities arising from different types of concentration of economic functions IT resources in the financial system, and how disruptions can spread between different IT systems and participants.

3 Cyber risks can also pose an indirect threat to financial stability

Financial sector actors are not only highly dependent on their own IT resources, they are also dependent on basic societal functions that in turn rely on other IT resources. These include, for example, the supply of electricity or data and telecommunications. Disruptions to such functions can therefore, without directly affecting IT resources in the financial sector, have consequences that lead to negative effects on the basic functions of the financial system and thus affect financial stability.

However, the indirect effects of cyber risks do not necessarily operate only through technological channels. There may also be an interaction with other well-known economic contagion channels. For example, an IT incident at an apparently non-systemically important actor, or an actor outside the financial sector, could have stability implications if the minor incident simultaneously affects general confidence in the financial system. Since trust is a pillar of financial systems, any disruption that negatively affects trust can also threaten financial stability. Accessibility, integrity and confidentiality, which were described above in terms of direct effects on financial stability, are also highly relevant when it comes to indirect channels and aspects of trust in the financial system.

In this context, it can be noted that confidence in the financial system is not only linked to confidence in private actors. Authorities can also play an important role in maintaining overall confidence in the financial system. It is therefore important that authorities with responsibility for financial stability also maintain a high level of protection against cyber risks, so that stability disturbances cannot spread into the financial system through a trust channel via the authorities.

In addition to the trust aspects, there are at least two other types of transmission channels where technical and economic aspects interact. First, an IT incident in a small actor can lead to cascading effects throughout the financial system. This means that if a participant that initially appears less important is unable to fulfil its commitments, consequences may arise among other participants, which in turn leads to a further spread of the problems so that the entire system ultimately risks being affected. Such cascading effects could arise, for example, in the case of payments[6] or securities settlement[7]. What can happen in such a situation is that the financial system's inherent vulnerabilities, linked to, for example, liquidity or leverage of securities, are hit by a cyber disruption that triggers problems.

Second, through the exposure of the financial system to credit and liquidity risks, a cyber incident in the real economy could have an impact on financial stability.[8] This could happen if IT resources somewhere in the real economy are affected, raising doubts about the ability of the actors involved to fulfil their financial obligations. For

[6] For example, Brando et al (2022) and Eisenbach et al (2022) discuss cyber risks and cascading effects related to payments.

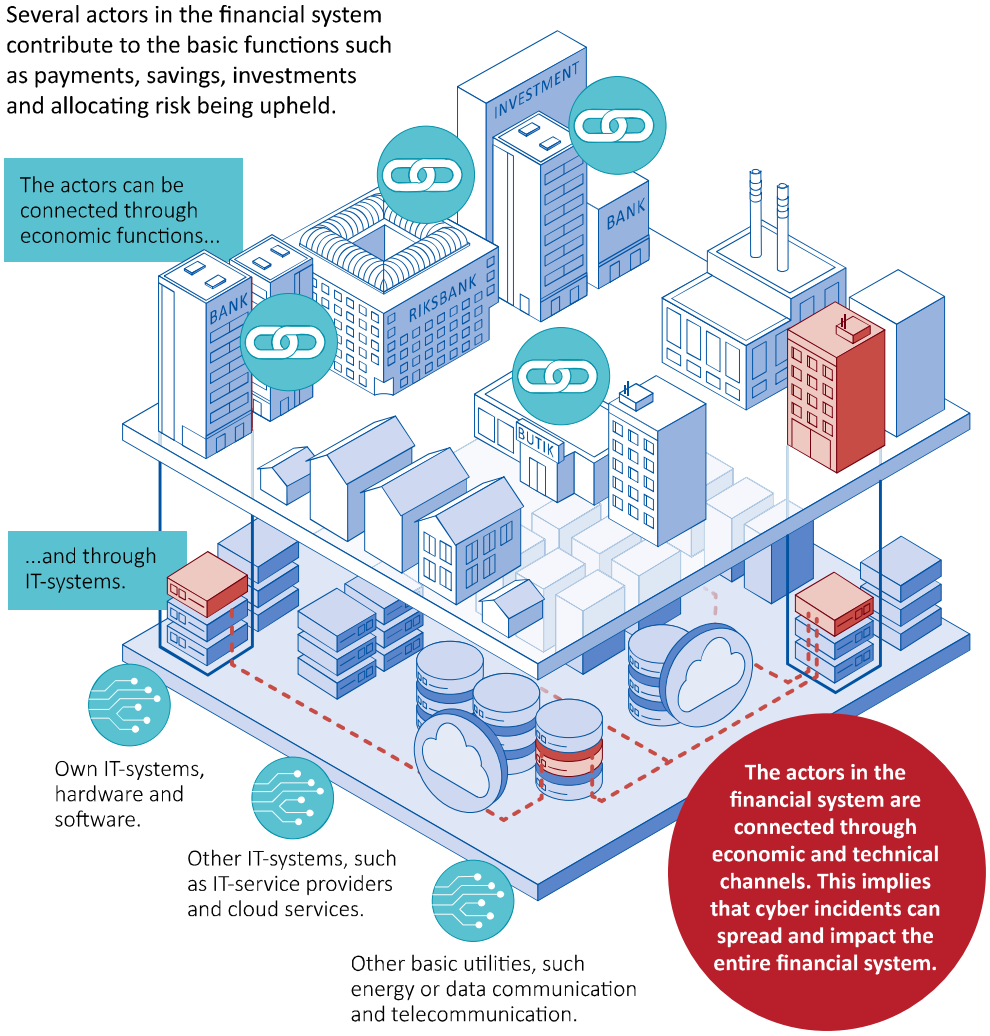
[7] Kopp et al (2017) mention cascading effects related to the settlement of securities.

[8] See, for instance, Fell et al. (2022).

example, a disruption could affect the financial situation of many or particularly important companies, which in turn could affect actors in the financial system and thus financial stability.

Thus, cyber risks can also affect financial stability indirectly through both technical and economic transmission channels. Moreover, the different channels may in some situations interact with each other (see Figure 1). As a result, the overall picture of cyber risks is complex, and there are a number of interactions that are important to recognise when assessing potential impacts on financial stability.

Figure 1. Cyber incidents can spread through interconnectedness.



4 The complexity requires a broadly-based approach in the work with cyber-related systemic risks

4.1 Cybersecurity of individual actors important for the resilience of the financial system[9]

Strong participant protection is important

For the resilience of the financial system to be sufficiently strong, the individual actors in the financial sector need to have strong protection against IT incidents in their IT systems. Thus, it should not be possible for events to occur easily that have extensive or far-reaching consequences. Strong protection means that it becomes very difficult and disproportionately resource-intensive for unauthorised parties to influence or gain access to the IT systems in question.

Strong protection means buying secure products and services and then using them properly to achieve a high level of cyber security. However, IT systems are inherently difficult to monitor and in many systems different types of weaknesses and vulnerabilities are discovered later. So a strong protection of IT systems also means that the actors need to have a complete overview of which systems are in operation, which versions of the systems are used and to ensure that the systems are continuously updated as weaknesses and vulnerabilities are discovered. It is also important to regularly review permissions in the systems and not to grant higher permissions than necessary in the systems.

The resilience of the system can also be strengthened if actors can share information about the vulnerabilities they discover in the systems and the ways in which the vulnerabilities may lead to cyber incidents. Such information sharing is needed both between actors in a given sector and between different sectors (more on this in sections 4.2 and 4.3 below).

An important share of the cyber risks to which the financial system is exposed originate from actors who have the intention and ability to cause damage, known as antagonistic actors. An important part of the work on high IT security in the financial sector is thus to map the antagonistic threats that exist against both systems and actors in the financial sector. To obtain a nuanced threat picture, both authorities and private actors need to cooperate and share information, knowledge and experience. Being aware of the threat landscape, and thus having the conditions to counteract the threats, strengthens the entire system's resilience to cyber risks.[10]

[9] For a general discussion on measures for a high cyber resilience see also NCSC (2022).

[10] One example of how such collaboration can take place is the pilot activity that the National Cyber Security Centre has started with the financial sector.

To get an idea of how to improve protection, the actors can continuously carry out different types of tests on their systems. In this way, they can get indications of how strongly protected their IT systems are, while at the same time it is possible to discover what can improve the protection without an IT incident first occurring. This type of testing can take many different forms. One type is the so-called TIBER tests. These first produce a picture of threats to and possible vulnerabilities in an actor's IT system, and then try to utilise these to gain access to the systems. In this way, one learns which measures can increase the actor's resilience.[11]

Good ability to detect and respond to IT incidents is important

Regardless of the level of protection achieved in IT systems, it is virtually impossible to completely avoid IT incidents. It is therefore important that actors who could play a systemically important role in the financial system are also able to detect and respond to incidents. This means, for example, that a malicious actor who has bypassed the protection of the IT systems should not be able to move freely in the systems for any length of time without being detected and ejected.

A good prerequisite for a high ability to detect IT incidents is that the actors have access to an operational function that monitors what is happening in the IT systems around the clock, every day of the year, and gives clear and early signals if an incident is detected or if there are signs that an incident is imminent. Such a function needs access to information from the IT systems, such as security logs, and also needs tools that analyse the information and immediately signal if signs of incident are detected. Participants providing IT systems that have a direct impact on the basic functions of the financial system may also consider the possibility of also using existing advanced detection and warning systems.

Should an IT incident be detected, it is important that it can be resolved. Actors who contribute to the maintenance of systemically important financial functions therefore need to have the capacity to respond quickly to IT incidents. It is also an advantage if they can investigate how the incidents occurred and what the consequences have been.

Important to have rapid restart if critical functions are affected by serious incidents

If it goes so far that the IT system functions are interrupted, it is important to be prepared to restart the systems. The same applies if data in the systems can no longer be trusted, or if data in ordinary systems is destroyed and disappears. It is then important to be able to read back data that is correct with reasonable certainty.

This may mean, for example, that several updated backup copies of data and sometimes entire IT systems are needed, 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

[11] The ECB's framework for threat-based penetration testing, TIBER-EU, and the Riksbank's work on a Swedish adaptation of this framework, TIBER-SE, are examples of how central banks can contribute to increasing the resilience of the financial system to certain types of cyber risk.

copies. It can also mean that there are routine descriptions of how IT systems should be restarted after a serious IT incident, and that routine descriptions of how data should be restored are needed, 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 various tests and exercises when it comes to restarting systems and restoring data from backup copies. If the participants regularly carry out such tests and exercises, the conditions for IT incidents to be as short as possible will increase, thereby reducing stability risks in the financial system.

It is of course difficult to say how long important IT systems can be unusable without becoming a problem for stability, and this also depends to a very large extent on the situation. But it is important that all systemically important operations in the financial sector can rapidly and securely restart their systems and recover data. In this context, it may also be important that, as soon as an incident occurs, there is an approximate idea of how long it may take to restart systems or re-read data under different scenarios.

Financial sector authorities also need to maintain a high level of cyber security

It is important to note that it is not only the private actors in the financial sector that need to have a high level of cyber security with strong protection, a good ability to detect and remedy IT incidents and readiness to quickly restart important systems. The authorities responsible for maintaining stability, i.e. Finansinspektionen, the Riksbank and the Swedish National Debt Office, all play a central role in the financial system, and need to ensure that their operations are highly resilient to cyber risks.

There are at least two reasons why it is important that financial stability authorities also maintain a good resilience to cyber incidents. First, cyber incidents at the authorities could have a direct impact on their ability to fulfil their tasks within financial stability. Second, incidents could also affect confidence in the financial system, which in itself could have implications for stability.

4.2 A systemic perspective is also needed to safeguard financial stability

Action by individual actors is not enough to make the financial system resilient

Although it is very important that all actors in the financial sector have good resilience to cyber incidents, this is probably not enough to ensure that the resilience of the financial system as a whole is sufficiently high. As a complement, there needs to be a system-wide perspective that is reflected in the work to counteract cyber risks.

There are at least two concrete situations where it is important to take the system perspective into account. The first situation is when an individual actor deploys all the measures that are well-balanced from the perspective of its own operations, but where the actor's weight in the system means that the measures are not sufficient from a system perspective. This situation can arise in an environment where the cost of an IT incident from the system's perspective exceeds the cost that is relevant when an individual actor considers protecting itself against the IT incident. Similar mechanisms, i.e. where individual actors do not fully internalise the risks that may arise at system level, also exist in the financial system when it comes to other types of risk than cyber risks. One way to manage these types of risk is to use different types of system-wide tools, such as macroprudential tools. These tools could also be used in the cyber area to increase the overall resilience of the financial system.

It is also possible to imagine a second situation where it is not enough for individual actors to act separately, but where a systemic perspective is required to make the system resilient. This could be in a situation where the actors involved make sufficient efforts in themselves, but where coordination between them is required for the efforts to bear fruit and strengthen the system's resilience.

One example of such a situation could be if several actors simultaneously realise that external assistance is needed to ensure a rapid recovery from a cyber incident. Individually, the actors can have managed to secure sufficient external assistance before the incident occurs. However, if it were to turn out that several actors were simultaneously affected by a cyber incident, without coordination there is a risk that the actors have tied themselves to the same external help and that this then becomes a scarce resource. In such a situation, coordination between the actors could contribute to increasing the total resilience of the system.

Analysing dependencies within the financial system can be a first step towards increasing resilience

One of the first steps in strengthening the financial system's resilience to cyber incidents is to map out how the system's various central economic functions are interrelated and what types of IT systems they in turn depend on. But it is not enough to map which systems are used by a particular actor. One also needs to know how different financial and technical functions of different actors in the sector are interdependent.

This type of system-wide mapping can be done in several different ways, but one way is to use so-called cyber stress tests.[12] This involves developing a scenario with a hypothetical cyber incident. A selected group of actors in the financial sector then examines the impact of the hypothetical cyber incident on their own systems and on links

[12] See more about the tool known as Cyber Resilience Scenario Testing (CyRST) in ESRB (2023).

with other actors. In this way, it is possible to get an indication of how large the system-wide effects of a particular IT incident could be.[13]

Financial stability can benefit from knowing when a cyber incident risks affecting the system.

Cyber incidents occur continuously and it is reasonable to expect that the vast majority of incidents will be dealt with by the actor(s) affected without any consequences for the financial system as a whole. However, if there is a risk of an incident approaching such a scale that the entire financial system's stability can be affected, it is important that the stability authorities step in and as far as possible counteract such a development. If this is to be done adequately, it is important to be able to determine when an incident goes from being a matter for an individual actor to becoming an event that needs to involve the authorities responsible for financial stability. As a tool to obtain such an overview, and to be able to take measures to prevent the incident from having system-wide effects, it may be helpful to define concrete levels that trigger different types of measures by the stability authorities.[14] These actions could include, for example, increasing information gathering, sharing information between authorities, preparing for different types of mitigation or counteracting measures or general crisis preparation measures. The overall purpose of defining the levels is to have a clear picture in advance of which incidents risk having system-wide effects and of what may need to be done to prevent such effects.

Collaboration and cross-sectoral guidelines can further contribute to resilience[15]

Collaboration within the financial sector makes it easier to safeguard the systems perspective and strengthen resilience to cyber incidents. For the financial stability authorities, Finansinspektionen, the Riksbank and the Swedish National Debt Office, there are several different forms of cooperation that can ensure the systemic perspective, such as the work on cyber issues within the framework of the Financial Stability Council and exercises of various kinds. A cooperation of particular importance could also be to establish a strategy for the more long-term work on strengthening resilience to cyber incidents in the financial sector. Such a strategy could, for example, specify how the authorities consider that individual actors can contribute to the stability of the financial system by increasing their resilience. It could also describe what system-wide considerations are needed in the sector. A direction for the sector's work on contingency planning could also be included in such a strategy.

[13] Cyber stress tests for actors in the financial sector are being used or considered by institutions such as the Bank of England, the European Central Bank and the Danish financial supervisory authority Finanstilsynet.

[14] See more about the tool called Systemic Impact Tolerance Objective (SITO) in the ESRB (2023).

[15] Legislation, such as the Protective Security Act, can also reflect society's need to take systemic consideration. Some risks may have such a small probability of occurring that it may be reasonable for an individual business to accept it. However, if the risk were to be realised, it could have major consequences for society, which means that the risk still needs to be addressed. The Swedish Protective Security Act regulates the management of security-sensitive activities and financial sector actors may need to conduct security-sensitive analyses to determine whether they have activities that may be of importance to Sweden's security.

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) and a collaboration forum for the National Cyber Security Centre (NCSC)[16]. Both of these deal with issues related to cyber security. It is essential that such work continues in the future to increase the resilience of the financial system to cyber risks and cyber incidents.

4.3 Financial system stability closely linked to other fundamental societal functions

It is not only the financial sector and the financial system that are increasingly exposed to cyber risks as a result of increased digitalisation. The same applies to many different sectors of society, several of which may also have an indirect impact on the stability of the financial system.[17] For example, the functionality of the financial system depends on the maintenance of basic societal functions, such as electricity supply and data and telecommunications. If such functions were to be affected by large-scale cyber incidents, it is very likely that financial stability could also be affected. Thus, cyber security is not an aspect that only needs to be addressed when it comes to the financial system; it should be a national concern that affects both the financial sector and other vital sectors.

The fact that cybersecurity is a national concern suggests that coordination and action at national level is also needed to address cyber risks in society. The arguments in favour of taking into account multiple sectors at national level are the same as the arguments for taking into account multiple actors in the financial sector. That is, there are problems that are so comprehensive at the national level that individual actors or individual sectors are unlikely to be able to implement sufficient measures to address them. Thus, coordination at national level will be as necessary for the overall resilience of society to cyber incidents as coordination within the financial sector will be for the resilience of the financial system.

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. 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. Within the framework of their respective assignments, they will deepen their cooperation in the field of cyber security and thus be able to coordinate the work of preventing and responding to cyber incidents. The

[16] 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.

[17] See, for instance, Forscey et al. (2022) for a discussion.

NCSC's authorities will also provide advice and support regarding cyber risks and constitute a national platform for collaboration and information exchange with other actors, both private and public, in the field of cyber security.

A financial sector cooperation forum has been created as a pilot project in the NCSC. Both private actors and authorities participate here. The authorities include those with close links to the NCSC and the authorities responsible for financial stability, i.e. Finansinspektionen, the Riksbank and the Swedish National Debt Office. The private actors include trade organisations and companies in the financial sector.

It was recently announced that the Swedish Defence Radio Agency will take over responsibility for the national cyber security centre.[18] The fact that an authority will be responsible for the cyber security centre may mean that there are greater opportunities to give the centre assignments that go further than the current one. Among other things, the centre could actively contribute to the systematic cyber security work of government agencies, for example by clearly highlighting the requirements that need to be placed on IT systems in certain types of procurement. The centre could also be tasked with systematically sharing information that emerges from different authorities' security reviews of IT systems. There is currently no coordination in this area, which can lead to inefficiency and increased risk exposure, because each authority needs to conduct its own security reviews and cannot easily communicate the results to other authorities. A single centralised cybersecurity authority could also be helpful in communicating information on vulnerabilities in IT systems to both private and public actors. As a further example, it could be easier to allocate resources to the cybersecurity center, so that it can actively assist different actors and sectors with cyber skills in the event of serious cyber incidents that are of such a nature that they risk having a significant impact on important societal functions or on Sweden’s security.

5 Summary

The digitalisation of the financial sector means that both individual actors and the entire financial system are exposed to cyber risks. To increase the resilience of the system, efforts are required from both individual actors and at the general system level.

For a high level of resilience in the system, it is important that actors have strong protection, a good capacity to detect and respond to cyber incidents and a high level of preparedness to restart systems and recover data.

At the systemic level, it is important to identify key functions of the financial system and their dependence on different IT systems. It is also important to assess the level of resilience of the system as a whole and how different measures can help to strengthen the system.

Taking a systemic perspective is important both in the financial sector and at national level, for example by taking into account the interdependence between the financial

[18] See Kristersson et al. (2023).

sector and other important sectors of society. In this way, there can be conditions for increasing the resilience of society as a whole to cyber incidents.

References

Adelmann, Frank, Elliott, Jennifer, Ergen, Ibrahim, Gaidosch, Tamas, Jenkinson, Nigel, Khiaonarong, Tanai, Morozova, Anastasiia, Schwarz, Nadine and Wilson, Christopher (2020) Cyber Risk and Financial Stability: It's a Small World After All, IMF Staff Discussion Note, SDN/20/07, 7 December 2020, International Monetary Fund.

Brando, Danny, Kotidis, Antonis, Kovner, Anna, Lee, Michael and Schreft, Stacey L. (2022) Implications of Cyber Risk for Financial Stability, FEDS Notes, 12 May 2022, Board of Governors of the Federal Reserve System.

Eisenbach, Thomas M, Kovner, Anna and Lee, Michael Junho (2022) Cyber Risk and the U.S. Financial System: A pre-mortem Analysis, Journal of Financial Economics, 145, pp. 802-826.

Elestedt, Lukas, Nilsson, Ulrika and Rosenvinge, Carl-Johan (2021) A cyberattack can affect financial stability, Economic Commentary No. 8, 19 May, Sveriges Riksbank.

ESRB (2020) Systemic Cyber Risk, February 2020, European Systemic Risk Board.

ESRB (2022) Mitigating Systemic Cyber Risk, January 2022, European Systemic Risk Board.

ESRB (2023) Advancing macroprudential tools for cyber resilience, February 2023, European Systemic Risk Board.

Fell, John, de Vette, Nander, Gardó, Sándor, Klaus, Benjamin and Wendelborn, Jonas (2022) Towards a Framework for Assessing Systemic Cyber Risk, Financial Stability Review, November 2022, European Central Bank.

Forscey, David, Bateman, Jon, Beecroft, Nick and Woods, Beau (2022) Systemic Cyber Risk: A Primer, 7 March 2022, Carnegie Endowment for International Peace and Aspen Institute.

IVA (2022) Cyber security for increased competitiveness, Royal Swedish Academy of Engineering Sciences.

Kashyap, Anil K. and Wetherilt, Anne (2019) Some Principles for Regulating Cyber Risk, AEA Papers and Proceedings 2019, Vol 109, pp. 482-487.

Koo, Helga, van der Molen, Remco, Vermeulen, Robert, Verhoeks, Ralph and Pollastri, Alessandro (2022) A Macroprudential Perspective on Cyber Risk, Occasional Studies, Volume 20-1, 8 June 2022, De Nederlandsche Bank.

Kopp, Emanuel, Kaffenberger, Lincoln and Wilson, Christopher (2017) Cyber Risk, Market Failures, and Financial Stability, IMF Working Paper WP/17/185, 7 August 2017, International Monetary Fund.

Kristersson, Ulf, Bohlin, Carl-Oskar, Jonson, Pål, Persson, Mats, Slottner, Erik and Strömmer, Gunnar (2023) FRA får ta över ansvaret för Sveriges cybersäkerhet (National Defence Radio Establishment may take over responsibility for Sweden's cyber security), DN Debatt, 27 April 2023, in Swedish.

Maurer, Tim and Nelson, Arthur (2021) The Global Cyber Threat, Finance & Development, March 2021, International Monetary Fund

NCSC (2022) Cybersäkerhet i Sverige 2022 – Del 2: Rekommenderade säkerhetsåtgärder, Nationellt cybersäkerhetscenter, in Swedish.

SVERIGES RIKSBANK
Tel +46 8 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUCTION SVERIGES RIKSBANK