Occasional Studies
Volume 20 - 1

A macroprudential perspective on cyber risk

DeNederlandscheBank
EUROSYSTEEM

Central bank and prudential supervisor of institutions

Authors
Helga Koo, Remco van der Molen, Alessandro Pollastri, Ralph Verhoeks and Robert Vermeulen

The Occasional Studies aim to disseminate thinking on policy and analytical issues in areas relevant to De Nederlandsche Bank. Views expressed are those of the individual authors and do not necessarily reflect official positions of De Nederlandsche Bank.

Subscription order for DNB Occasional Studies and requests for specimen copies should be sent to:

De Nederlandsche Bank N.V.
Communications
P.O. Box 98
1000 AB AMSTERDAM

Internet: www.dnb.nl

Content

1 Introduction

Cyber risk is an increasingly important source of risk, not just to individual financial institutions, but also to the financial system as whole. The number of cyber incidents has increased over the past years, and the incidents have become more costly. Several features of the financial system make it especially exposed to cyber risk. Even though many financial institutions have increased their cyber resilience, cyber incidents will keep occurring and have the potential to cause major damage to the financial sector. Therefore, it is important to also develop a macroprudential perspective on cyber risk.

The financial sector is increasingly targeted in cyberattacks. Financial institutions are leading targets of cyberattacks. First, attacking them offers multiple avenues for profit, given the presence of high-value assets. Second, nation states and hacktivists target the financial sector for political and ideological reasons because of its central role in funding the economy. As such, the cyberthreat has increased systematically in recent years and is also moving upstream in the financial chain. Cyber incidents have become more frequent, as well as increasingly costly and damaging. For example, the incidence of cyber-related operational losses reported by Dutch banks doubled between 2018 and 2020 (see Box 1), while 5% of pension funds and insurers were victims of a successful attack in 2021.[1] This is accompanied by a shift from attacks on customers to attacks on the financial institutions themselves as well as their service providers.[2]

1 DNB IB Monitor 2021
2 See for instance BIS (2020) and the Cyber Threat Intelligence Report (2021) by Accenture.

The global financial system has become more digitalised and interconnected, making it more exposed to cyber risk. For example, banks have reduced their number of branches and shifted to an expansion of online banking services. Within capital markets, the vast majority of securities are only traded electronically nowadays. Other components of the financial market infrastructure, such as central clearing and payment and settlement services have also become fully digitalised. Moreover, financial institutions, market and infrastructures have become more interconnected, partly due to the interdependencies of their IT systems. The strong reliance on IT systems and the high level of interconnectedness has significantly increased the potential impact of cyber incidents on the financial sector.[3]

The coronavirus crisis gave impetus to cyberthreats. The coronavirus outbreak led to changes in working conditions and the activation of pandemic protocols to guarantee the continuity of critical business processes. The pandemic measures also forced institutions to switch to large-scale homeworking for a protracted period. Dependence on the internet for homeworking makes the threat of DDoS attacks on vital infrastructure or hacking and extortion attempts even more relevant. In addition, homeworking generally requires more capacity in order to guarantee the availability of business networks. As a result, the network capacity required to detect and process malicious activities came under pressure too. The risk of digital intrusion is also increasing as a result of workarounds, as homeworking blurs the boundary between work and private life, increasing the likelihood that employees disregard basic digital hygiene (DNB, 2020). The behavior of attackers during the coronavirus crisis shows that cyber-attackers react rapidly to the latest events.

3 See Aldasoro et al. (2022) for an overview of the characteristics and drivers of cyber incidents.

Various criminal groups used the coronavirus as a theme for fraudulent emails and websites aimed at capturing personal information.

The Russian invasion of Ukraine and the resulting geopolitical tensions have led to a further increase in cyberthreats. Cybersecurity firms, governments and regulators have pointed to the risk of direct repercussions on Western financial institutions through cyberattacks. Even though this risk does not seem to have materialised so far, Russian hackers are able to execute sophisticated cyberoperations and have already done so in the past. Examples are the NotPetya attack in 2017 and an attempt to hack Dutch ministries in 2018. Dutch financial institutions themselves also consider that the threat in their sector has increased. Moreover, the financial sector can be hit indirectly or unintentionally if related third parties are attacked.

Box 1 The incidence of cyberattacks in the banking sector

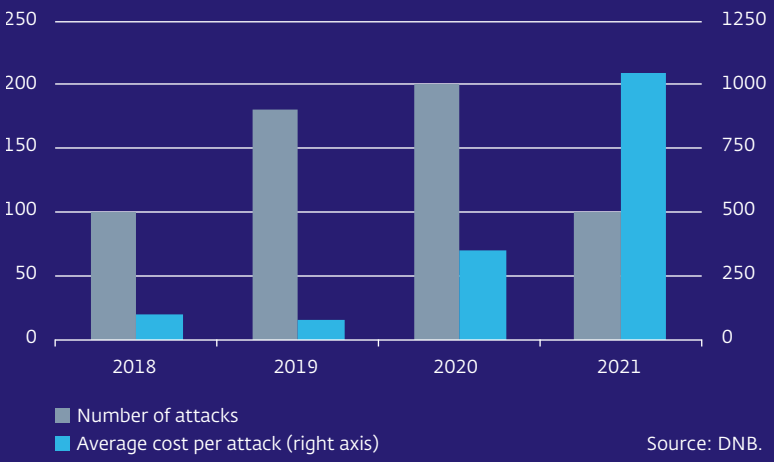
Estimating the incidence and costs of cyber incidents is difficult for at least two reasons. First, not all cyber incidents and associated losses are being reported in an integrated reporting framework. Information about cyber incidents is collected by various authorities, which often do so from a slightly different perspective or for a different population. For example, some reports focus on the number and type of cyber incidents, but do not contain information about the losses involved. In other cases, the report focuses on a specific type of cyber incidents, such as fraud. Second, when losses associated with cyber incidents are reported, it is likely that the loss estimate mainly includes direct losses (loss of revenue, funds stolen, repair costs, etc.). Indirect costs of cyber incidents (such as loss of reputation, damage to brand value, legal costs and fines, etc.) may not be included, but they make up a potentially important part of the costs of cyber incidents.

Banks report higher operational losses due to cyberattacks. If losses are above a certain level, banks are required to report their losses associated with operational risks, including cyber risks, in the Common Reporting (COREP) templates. Based on a subset using the most common keywords associated with cyberattacks[4], we find that the most common types of cyberattacks that led to operational losses during the years 2018-2021 were phishing and/or spoofing (81%). This occurs, for example, when a bank customer clicks on a link in a text message and thereby unintentionally discloses confidential data to cybercriminals. The COREP data also show an upward trend in the number of reported cyber incidents as well as in the average loss per cyber incident. Figure 1 shows that the number of reported cyber incidents increased in 2019 and 2020 and that the average loss resulting from a cyberattack was 10 times higher in 2021 than in 2018. When comparing the reported losses resulting from cyberattacks to the total losses from operational risks, we find that the share of losses due to cyberattacks in 2020 was four times higher compared to 2018.

4 The most common keywords associated with cyber risks are malware, ransomware, DDoS, rootkit, spyware, trojan, worm, virus, phishing and spoofing.

Figure 1 Increase in the number and severity of cyberattacks since 2018

Index 2018=100



Source: DNB.

Other sources confirm the increasing trend in the incidence of cyber-attacks on banks. The COREP data contains only a subset of the cyber incidents, as banks only have to report the incidents if they lead to substantial losses. However, the increasing trend is also found in other reports. For example, 40% of the large European banks suffered at least one successful cyberattack in 2019 (ECB, 2021). This is substantially higher than in 2018, when 28% of the banks were victim of at least one successful cyberattack. In addition, the damage due to fraud with banks' payment services increased from almost 50 mln euro in 2020 to more than 60 mln euro in 2021 (Dutch Payments Association, 2021).

The growing dependence on third-party providers makes financial institutions more vulnerable to disruptions in these providers' operations. The trend towards outsourcing of digital business processes, such as data storage, payment systems and software, causes a larger digital dependency on third parties, such as IT companies and cloud providers. On the one hand, these technology firms in most cases have more expertise and higher standards with respect to information security and cybersecurity. On the other hand, DNB has found that financial institutions tend to have insufficient risk management processes in place for their service providers.[5] For example, institutions do not sufficiently check to what extent third parties actually comply with their contractual agreements with respect to information security, cybersecurity and business continuity. The recent failure of Amsterdam Trade Bank (ATB) illustrates the consequences of the dependency on third party providers, albeit in a different context. After the Western sanctions against Russia, ATB was about to lose access to essential (information) systems that require a software license from in particular American and British service providers. As an alternative was not available on short notice, ATB could no longer operate and had to file for bankruptcy.

TIBER hacking tests show that cyberattacks can lead to financial stability risks. The cyber resilience of financial institutions is tested with the Threat Intelligence-Based Ethical Red Teaming (TIBER) programme (see Box 2). These tests show generally high levels of cyber resilience, but at the same time they show that sophisticated attackers could potentially cause a lot of damage to institutions that are essential for financial stability. If these controlled tests had been genuine attacks, they would in some cases likely have caused failures of key functions, losses of highly confidential information, financial losses or market manipulation. Despite the efforts of

5 See DNB IB Monitor 2021.

financial institutions to protect themselves against cyberattacks, TIBER tests show that cybersecurity always needs further improvement. By simulating real attackers and sharing the lessons learned in the TIBER community, every institution can learn and improve continuously. Because cyberattackers are constantly evolving and adapting, so should the financial sector.

Box 2 TIBER: how do hacking tests work?

Testing within the TIBER programme involves testing on live systems, based on the principle that no actual disruptions should occur under any circumstances. The participating institutions' learning experience is central. In order to strengthen this learning experience, the lessons learned from the tests are shared among a closed group of participating institutions.
The TIBER-NL programme ensures that the tests meet high quality standards, so that institutions can exchange sensitive information about the tests in a responsible and standardised way. The TIBER framework has been set up in such a way that other vital sectors can also use it.

After the Financial Stability Committee recommended in 2015 that the resilience of Dutch financial institutions be tested in practice, DNB set up the Threat Intelligence-Based Ethical Red Teaming (TIBER) programme in 2016 together with the institutions in the financial core infrastructure. The programme has now been extended to include the most critical insurers and pension providers and more than 40 TIBER tests have been carried out or are currently active in the Netherlands. In May 2018, the programme was replicated in the EU (TIBER-EU framework, published by the ECB) and TIBER tests are now being carried out in 14 jurisdictions. In the TIBER programme the participating institutions engage specialised companies to carry out controlled attacks on the critical systems of financial institutions based on the most up-to-date threat information. In order to have access to the best threat information, we collaborate with experts from the sector, the intelligence services, the police and the National Cybersecurity Centre.

In this Occasional Study, we develop a macroprudential perspective on cyber risk. Due to the increasing importance of cyber risk, it is necessary to approach this topic not only from the perspective of individual institutions, but also from the perspective of the financial system. Chapter 2 therefore presents a conceptual framework to better understand under which circumstances and through which transmission channels cyber risk can evolve into a systemic risk. In Chapter 3, two of these transmission channels are explored using scenario analyses, with the aim of gaining a better understanding of how cyber risks can be quantified. Chapter 4 examines how macroprudential policies could be extended to cyber risk to mitigate its potential systemic impact.

2 Cyber risk and financial stability

Even though cyber events have until now not led to major financial stability problems, it is widely acknowledged that a cyber incident could potentially turn into a systemic event. This chapter describes the relevant amplification channels that could give rise to systemic cyber risk. A crucial factor in this regard is whether a cyber incident escalates from a mere operational issue into a confidence issue.

Financial stability is threatened when a cyber event leads to the failure of essential parts of the financial system. In such a situation, the financial system is unable to absorb the consequences of a cyber event and continue to perform its key economic functions, such as cash and electronic (retail) payments, high-value interbank transfers and securities transactions. Given the pivotal role of the financial sector in the economy, a failure of the financial sector – or parts of it – could potentially have a significant financial and economic impact. Typically, a systemic event requires not just a large initial shock, but also amplification through, for example, bank runs, liquidity freezes or fire sales.

Financial instability as a result of cyber risk is to a large extent driven by factors that have historically played a role in the development of financial crises. The evidence from historical financial crises shows that financial instability could arise as a result of both the direct impact of a shock on financial institutions (e.g. the insolvency of a large bank) and of a broad increase in uncertainty and loss of confidence. If the impact of the initial shock is very large, or if information about the impact is lacking, financial market participants may become concerned about the ability of institutions to bear the losses. This could induce them to withdraw their funds, which may create market instability. Thus, when considering the

potential for a cyber event to become systemic, it is important to consider both direct and indirect transmission channels.

Cyber risk differs in important ways from more traditional sources of risk. Typically, financial stability assessments tend to focus on financial risks, such as credit, liquidity and market risk, which are related to the specific characteristics of the assets and liabilities of financial institutions. Cyber risk is different in the sense that it is part of operational risk, i.e. the risk of financial losses stemming from operational failures. Moreover, cyber risk differs in at least two important ways from more traditional sources of operational risk. First, cyber incidents can propagate very quickly and on a large scale, both within an institution as well as across sectors and countries. Second, whereas more traditional operational risk concepts are often related to accidental failures, cyberthreats often come from actors who aim to cause financial harm or a disruption to the financial system. This increases the likelihood of a cyber incident leading to prolonged problems, severe losses, and a disruption of confidence.

Cyber incidents can spread rapidly through the financial system, potentially amplifying an operational problem to a liquidity crisis. The ability of cyber incidents to spread quickly and widely is mainly caused by the interconnectedness of various information systems supporting the financial system. The outsourcing of digital business processes has led to increased concentration risk, for example if a specific digital service provider works for a large number of financial institutions. In this situation, these third parties become an attractive target for digital attacks, as a vulnerability in a single third party can be used as a springboard and be exploited to affect multiple financial institutions. As threat actors are becoming more sophisticated, their ability to exploit these interdependencies is also growing. This has not only enabled actors to penetrate the networks of individual institutions,

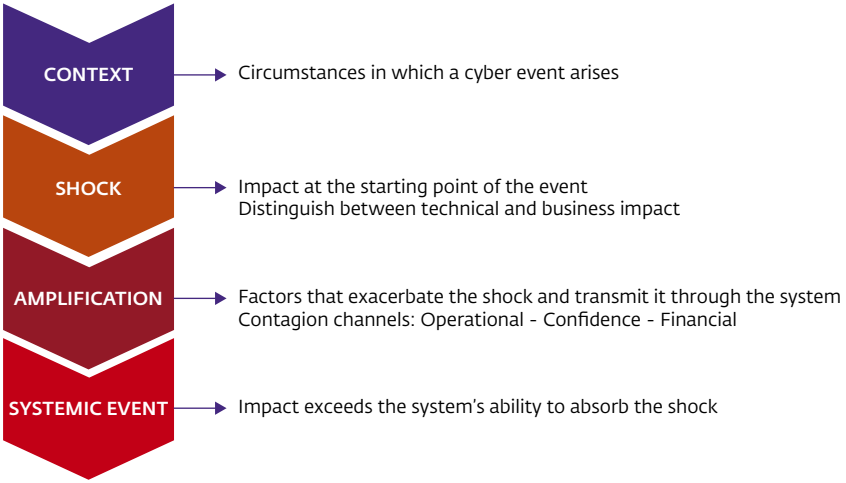
but has also allowed cyber incidents to spread easily to other entities, sectors and countries. As a result, a major cyber incident has the potential to spread faster and more widely than many other shocks. This could in turn lead to large financial losses and a significant weakening of trust in the financial system, as also seen in more traditional financial crises.

The European Systemic Risk Board (ESRB) has developed a conceptual model to analyse the conditions under which a cyber incident could become a systemic event. This conceptual model (ESRB, 2022) splits the analysis of a cyber incident into four distinct steps: (i) context; (ii) shock; (iii) amplification; and (iv) systemic event (see Figure 2). The first step is a description of the context in which a cyber incident is taking place. The second step is a description of the incident itself and its technical and business impacts. This step is limited to a description of the immediate technical impact and the organisational repercussions for the affected institution. The third step describes how the initial impact can spread to other financial institutions, by exploring the interactions between the affected institutions and how shocks can propagate through the systems they use. Examples of such amplifiers are a high degree of interdependence, a lack of transparency and a reliance on data.

If several amplifiers are in place at the same time, a cyber incident could turn into a systemic event. Note that a system-wide disruption caused by a cyber incident does not necessarily lead to a systemic event. For example, widespread disruptions in cash withdrawals or retail electronic payments typically do not have a systemic impact if they are solved quickly. A cyber event becomes systemic only if the system no longer has the capacity to absorb the shock and recover. This may happen if the cyber incident does not just remain an operational issue but raises serious financial and confidence concerns, for example through the disruption of critical functions or the

Figure 2 ESRB conceptual model of systemic cyber risk

Adapted from ESRB (2022)



financial losses from the incident. This would require several amplifiers to be at work at the same time and to reinforce each other. Although the ESRB assesses this to be 'a conceivable event', the conceptual model does not provide a quantification of this risk.

3 Quantifying cyber risk amplification channels

This chapter contains a first attempt to quantify systemic cyber risk. Based on the ESRB conceptual framework, we assess two amplification channels through which a cyber incident could potentially cause a severe disruption to the Dutch banking sector. The first channel assumes operational problems related to the TARGET2 payment system. In the second channel, a cyber-induced loss of confidence sparks a bank run. We find that these amplification channels can lead to a systemic event, but only in rather extreme scenarios. Follow-up work would have to involve a broader set of amplification channels, and the interaction between them.

How a cyber incident will play out depends on many factors and the narratives on how stress arises can differ. This study is one of the first in which an attempt is made to quantify the impact of cyber incidents on financial stability. The ESRB conceptual model describes operational, confidence and financial amplification channels through which a shock could be amplified through the system. Cyber incidents can lead to disruptions in payment systems and create loss in confidence. Therefore, we explore the first two amplification channels to better understand the potential financial stability impact of cyber incidents. Although many examples exist of cyber incidents affecting financial institutions[6], real life examples on how a cyber incident leads to a systemic risk event are lacking. Moreover, standard stress scenarios for cyber-related stress events are not yet available. This lack of historical cases poses challenges when it comes to calibrating severe but plausible stress scenarios. The scenarios in this chapter are therefore hypothetical and highly uncertain.

6 For a good overview of cyber incidents affecting the financial sector, see Timeline of Cyber Incidents Involving Financial Institutions - Carnegie Endowment for International Peace.

3.1 Operational problems in interbank payments

In this scenario, we assume that due to a cyber incident one or more banks are not able to settle payments with other banks. Therefore, the liquidity position of the banks that do not receive payments might be put under severe stress. In turn, these banks might decide to stop making payments to their counterparties, thereby stressing the liquidity position of the whole Dutch banking sector.

TARGET2

The scenario analysis is based on TARGET2 transactions. TARGET2 is the real-time gross settlement system owned and operated by the Eurosystem. The system enables EU banks to transfer money between each other in real time. It processes on average more than 350,000 transactions daily with a corresponding turnover of EUR 1,900 billion. The average transaction value is EUR 5.5 million. We limit the analysis to the transactions that involve institutions located in the Netherlands as the receiver and sender of the payment. This means that a foreign institution that sends a payment to a Dutch institution is not included in this analysis. Furthermore, TARGET2 distinguishes between several payment types. The payments are divided into four different groups: 1) main transactions, 2) payments with a central bank involved, 3) payments from and to ancillary systems and 4) liquidity transfers. In the analysis we focus on the transactions that belong to group 1: this group consists of transactions related to customer payments (identifier 1.1 in TARGET2) and interbank payments (identifier 1.2 in TARGET2).

Central banks require credit institutions to hold a certain amount of liquidity on their account in TARGET2. This is called the Minimum Reserve Requirement (MRR), which requires liquidity to be held for a predefined period of time ranging from four to five weeks. The MRR is calculated on the basis of the amount of liabilities held by the banks. The requirement does

not have to be strictly satisfied every day of the maintenance period. Instead, banks are required to have an average level of end-of-day (EoD) reserves during the maintenance period to be above the MRR. Based on the ratio of the level of EoD reserves to the MRR, we define four risk areas. A bank belongs to risk area 1 if its EoD reserves are below the MRR, i.e. the ratio is below 1. A bank is in risk area 2 if the ratio is between 1 and 1.5, in risk area 3 if the ratio is between 1.5 and 4, and in risk area 4 if the ratio is greater than 4.

Scenarios

We first analyse how a cyber incident affecting one large bank could spread to other banks. In this scenario, we assume that one large Dutch bank is affected by a cyber incident that takes five days to resolve.[7] The cyber incident is rooted in the software used by the bank to assess the incoming and outgoing payments in TARGET2. As a consequence, the bank is unable to remit payments to the rest of the system and therefore the outgoing payments to counterparties are halted. This means that other banks in the Dutch payment system will not receive the liquidity they were due for five consecutive days. We further assume that, although the affected bank is not able to make payments, it will still receive the due payments from its counterparties.

The second scenario analyses whether a cyber incident affecting many (smaller) banks could harm a large bank through the TARGET2 channel. In this scenario, we assume that all banks except the large bank use a cloud computing service from the same provider to run a number of daily operations, including the assessment of incoming and outgoing payments in TARGET2. The latest update of the software contains a bug that does not allow the

7 A series of cyber incidents related to TARGET2 has taken place between 2020 and 2021. In some cases, TARGET2 participants could not access their online account and on October 2020 TARGET2 payments were suspended for eleven hours. Source: Reuters.

user banks to make payments to the large bank. This happens because the software does not correctly log the payments due to the large banks. On the other hand, all banks using this service provider will be able to remit payments to each other. As in the first scenario, we assume that this malfunction is not resolved before five days. Therefore, the large bank will not receive liquidity from its counterparties for a period of five consecutive days.[8]

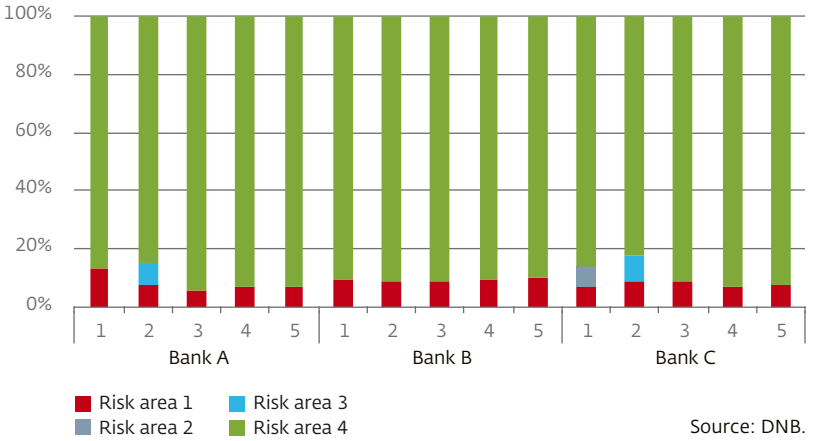
Results

We apply the first scenario to a small set of large Dutch banks for every day of 2019. We select the three banks with the highest daily average transaction amount sent to TARGET2 participants. To assess how disruptive the cyber incident is, we calculate, for each day, how not receiving the payments from the bank that suffered the cyber incident would affect the EoD reserves of the other banks. The 'fictitious' EoD reserve for these banks is obtained by depleting the actual EoD reserve that we observe in the data by the transaction amount due from the bank experiencing the cyber incident. For ease of exposition, we focus, for each bank, on the five days where the scenario has the largest impact, i.e. where the share of banks that end up in risk area 1 is the highest. Figure 3 shows the results.

8 In our analysis we have also tested scenarios where the duration of the cyber incident is longer than five days. For ease of exposition, and given that results do not significantly differ from the included scenarios, we only report the results for the five days scenarios.

Figure 3 Large bank scenario: share of banks in different risk areas

Percentages



Source: DNB.

In this scenario, the share of banks ending up with a reserve position below the MRR is contained.[9] Figure 3 shows that the majority of counterparties are in risk area 4 after five days – when the cyber incident is resolved. For bank A, on the day with the biggest impact, the share of banks reaching risk area 1 due to the cyber incident is 13%.[10] The other days show a share of counterparties in risk area 1 between 6% and 7%. For banks B, the share of counterparties in risk area 1 is around 10% for each of the five selected days. Finally, for bank C, the share of counterparties in risk area 1 is also around 8%.[11]

9 In our analysis, we consider banks with head-office in the Netherlands because our interest lies in the impact of Dutch banks on the Dutch banking sector.

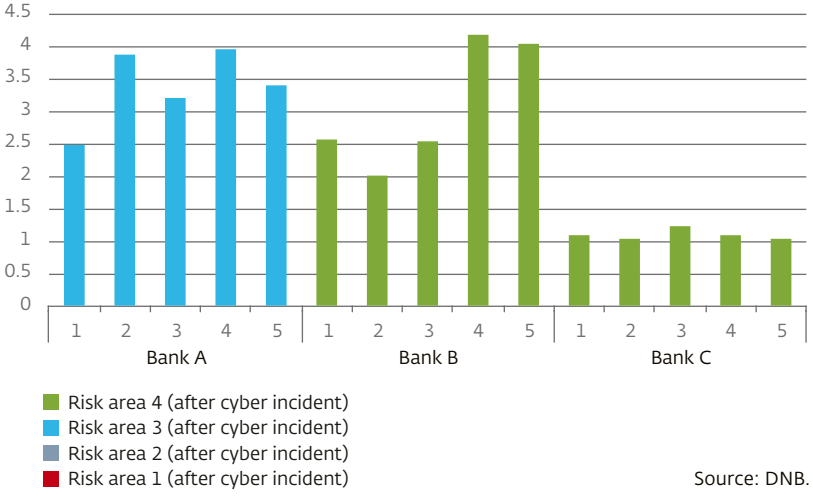
10 Banks A, B and C have, respectively, an average number of counterparties equal to 20, 18 and 15.

11 Banks that are below the MRR before the cyber incident are not counted as in risk area 1. This is done to isolate the effect of the cyber incident on the liquidity position of the banks irrespective of their reserves starting points.

For the same three large banks, we assess whether the second scenario could bring their reserves below the MRR. In this scenario, all banks that use the same cloud computing service provider will contribute to the EoD reserve depletion of the large banks. Analogous to the first scenario, we report results for the five days for which the scenario results in the lowest EoD reserve to MRR ratio. Figure 4 shows the decline in the reserve to MRR ratio for each of these days, as well as the risk area after the cyber incident. Before the cyber incident, all banks have a ratio level corresponding to risk area 4. At the end of the fifth day of the scenario, banks B and C are still in risk area 4, whereas bank A reaches risk area 3. We conclude that in this scenario none of the three large banks would end up in risk area 1.

Figure 4 Multiple bank scenario: reserves to requirement ratio depletion

Decline of reserves to MRR ratio



Source: DNB.

A different liquidity landscape

In the observed period, banks had a very high level of reserves compared to the MRR. The amount of reserves held by banks varies significantly over time, as shown in Figure 5. This shows the time series of the EoD reserve to MRR ratio between 2012 and 2019. The ratio decreases from mid-2012, reaching the lowest point in 2014, with an annual average of 2.3. Since then, the ratio has increased and reached an average value of 16 in 2019.

Figure 5 Time series of reserves to requirement ratio

Ratio of balance to MRR, average across Dutch banks

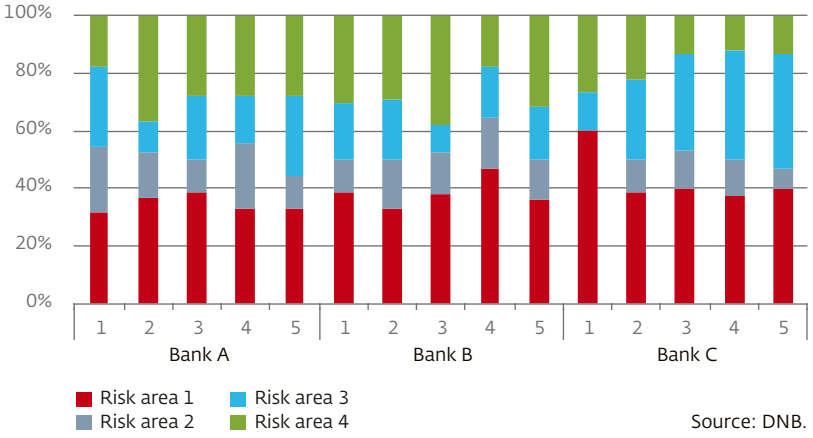
Source: DNB.

The impact of a TARGET2-related cyber incident on the Dutch banking sector could be more severe in a different liquidity landscape. To assess the impact in a situation with less liquidity, we apply the two scenarios with the assumption that all Dutch banks in TARGET2 hold a level of reserves equal to that in 2014 instead of 2019. Figure 6 shows the results from the first scenario, where a large bank is not able to remit payments to its counterparties for five days, for the same three large banks analysed

previously. The share of banks that end up in risk area 1 is now above 30% for each of the three banks and each of the five days. Bank C would have the biggest impact on its counterparties, with a peak of 60% of them being in risk area 1 after the cyber incident. Figure 7 shows the results of the second scenario, where three large banks do not receive payments from a large number of other banks due to a cyber incident affecting a cloud computing service provider. When a large number of counterparties stop making payments due to the cyber incident, all three banks end up in risk area 1, with EoD reserves below the MRR, on all of the five days. These results highlight that in a different liquidity landscape a cyber incident would have a more severe impact.

Figure 6 Large bank scenario: share of banks in different risk areas assuming 2014 level of reserves

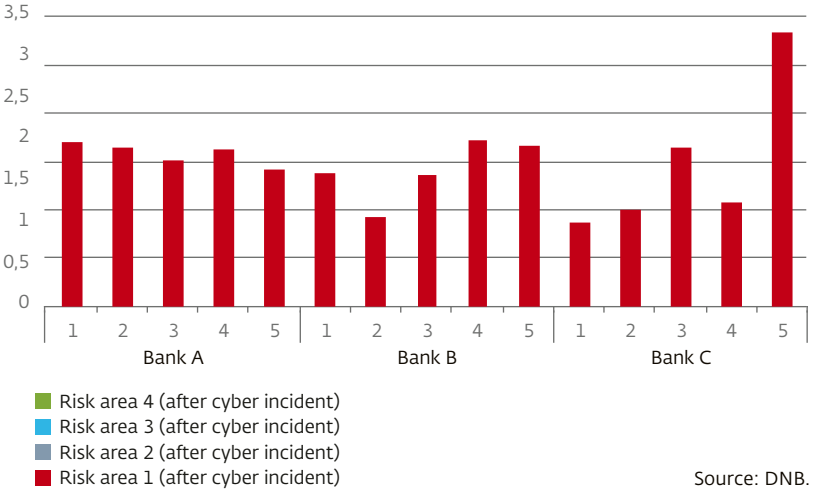
Percentages



Source: DNB.

Figure 7 Multiple bank scenario: reserve to requirement ratio depletion assuming 2014 level of reserves

Decline of reserves to MRR ratio



Source: DNB.

From this analysis it can be concluded that a cyber incident with TARGET2 as the operational channel is unlikely to directly cause financial stability concerns, in particular when liquidity is ample. Using two scenarios, we have analysed how a cyber incident might propagate to the financial system via TARGET2. The results suggest that a cyber incident is unlikely to cause financial stability concerns solely through the TARGET2 operational channel. When interpreting these results, the following considerations should be taken into account. First, our analysis shows that in a different liquidity landscape, the impact through this channel is significantly higher. This suggests that the results are to a large extent due to the exceptionally high reserves that banks currently hold. Second, we consider the impact on a bank in isolation. Clearly, the impact would

increase in the case where more large banks are affected at the same time (scenario 1) or do not receive payments from the other banks (scenario 2). Further refinements to these scenarios could also be added by explicitly taking interactions between the institutions into account, for example, assuming a strategic behavior of the banks in TARGET2 as in Eisenbach et al. (2022) or by assuming that multiple large banks are subject to a cyber incident as in Kosse and Lu (2022). Third, a cyberattack could lead to more severe operational problems than the ones considered in this scenario. This would clearly increase the risk of the incident becoming systemic.

3.2 Loss of confidence and liquidity stress

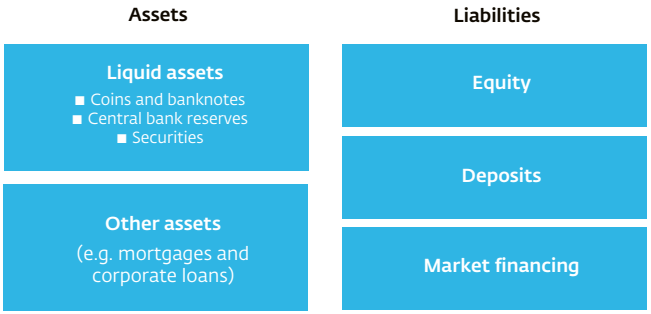
This section analyses a second channel, where a prolonged cyber incident leads to a confidence shock and triggers stressed liquidity outflows.[12] In this section the potential impact of severe cyber incidents on a bank's liquidity position is quantified by using a range of liquidity stress scenarios. This section first provides a stylized overview of a bank's liquidity position and how this liquidity position is affected by inflows and outflows. Then it outlines the hypothetical liquidity stress scenarios and presents the outcomes of each scenario.

Liquidity position, inflows and outflows

A bank's liquidity position can be defined by its counterbalancing capacity. This counterbalancing capacity represents the stock of freely available assets or other funding sources which are available to the bank to cover potential funding gaps. Figure 8 presents a stylised bank balance sheet, where the assets can be split into liquid assets and other assets. The liabilities can be split into deposits and market financing, which make up the bank's debt financing, and equity, which represents the bank's internally available capital.

12 As the ESRB (2020) states, " The anticipation of large financial losses and/or a critical mass of rumours in social media could also prove sufficient to trigger a classic bank run by customers."

Figure 8 Stylized bank balance sheet



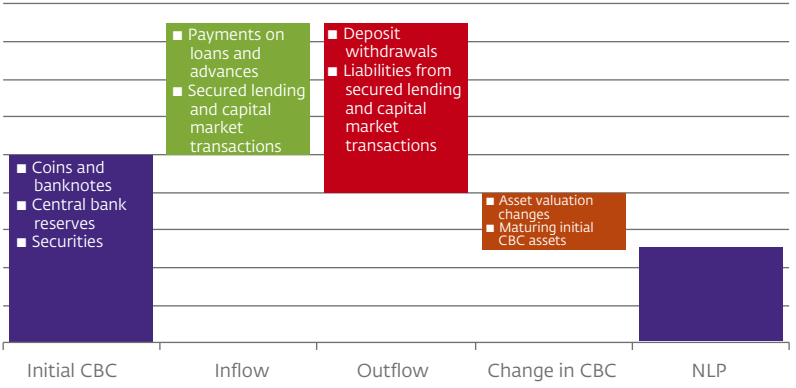
A bank can use coins and banknotes, central bank reserves and high-quality securities to cover liquidity outflows. Physical coins and banknotes are well-known instruments to cover deposit outflows. The same holds for withdrawable central bank reserves, which are excess reserves the bank holds at the central bank above minimum reserve requirements. Besides central bank assets, the bank can also use Level 1 tradable assets, Level 2 tradable assets and so-called Other tradable assets.[13] In addition, non-tradable assets eligible for central banks and undrawn committed facilities received are included in a bank's counterbalancing capacity.

A bank's maturity ladder is an overview of the contractual inflows and outflows the bank expects to receive and pay, respectively, by residual maturity. This maturity ladder is reported by banks to the supervisor at a monthly frequency, as part of the additional monitoring metrics (AMM) for liquidity reporting. Figure 9 shows in a very stylised way how liquidity

13 Level 1 tradable assets are very liquid financial assets such as securities issued by the central bank or domestic government. Level 2 tradable assets are, for example, high-quality corporate bonds (level 2A) or shares (level 2B). Other tradable assets are tradable assets (securities) which do not qualify as Level 1, Level 2a or Level 2b in accordance with European Commission Delegated Regulation (EU) 2015/61.

inflows improve the bank's counterbalancing capacity and how liquidity outflows worsen the counterbalancing capacity. In addition, the counterbalancing capacity can change due to changes in the valuation of assets or because assets mature. The resulting counterbalancing capacity is referred to as the net liquidity position (NLP).

Figure 9 Stylized liquidity waterfall chart



Liquidity inflows arise among other ways through secured lending and capital market driven transactions as well as payments that arise from loans and advances. One example of payments arising from loans and advances are customers' mortgage payments. If a customer has a monthly mortgage payment of one thousand euros, the bank considers these contractual mortgage payments as expected monthly inflows. Another example is a Dutch government bond with a residual maturity of three months. On the maturity ladder, the bank reports the repayment of this bond as an inflow.

Liquidity outflows arise for example from deposit withdrawals and liabilities from secured lending and capital market transactions. As an example, customers can withdraw funds from their current and savings accounts. These are generally seen as overnight deposit outflows, because a customer can in principle withdraw these funds without costs on a single day. On the other hand, if a customer has a term deposit with a residual maturity of one year, the bank considers this term deposit as an expected outflow one year from today because customers need to pay a fee for early withdrawal.

The counterbalancing capacity itself can be affected by asset valuation changes. For example, if a bank provides secured funding with a corporate bond as collateral and the corporate bond decreases in value, the counter-balancing capacity is decreased due to valuation changes.

In order to ensure that banks have sufficient liquid assets they need to satisfy the minimum requirements of the Liquidity Coverage Ratio (LCR). The LCR measures the ratio of high-quality liquid assets (HQLA) to expected liquidity outflows in a significant stress scenario that lasts for 30 calendar days. In general, HQLA are assets that can be easily and immediately converted into cash with little or no loss of value. Level 1, 2A and 2B assets are considered to be HQLA. The liquidity outflows that need to be covered are outflows that arise from deposit withdrawals (3-5% for stable deposits up to 100% for deposits from financial corporations), unsecured and covered bonds as well as credit and liquidity facilities.

Scenarios

We assume that cyber incidents result in loss of confidence in the bank, leading to deposit withdrawals and funding outflows. In the scenarios the actual cyber incident could be solved relatively soon, but the inconveniences

for customers and negative media attention negatively affect confidence in the bank, thereby resulting in stress for one month. Due to loss of confidence, retail and wholesale clients withdraw their deposits.[14] At the same time, the confidence of other counterparties has been impacted. As a result, funding from unsecured lending and other capital market transactions decreases. It is further assumed that events result in some market stress, leading to haircuts on the value of the available assets.

We assess the impact of cyber-induced liquidity stress by comparing the LCR stress scenario with two reverse stress test scenarios. The LCR stress scenario has been applied in earlier studies. For example, Duffie and Younger (2019) analyse how US financial institutions fare when they are hit by a severe cyber incident. The authors focus on the available liquidity to cover wholesale deposit outflows. In their base scenario they consider the stress parameters that are being used for the LCR across all in- and outflows. In more severe scenarios the authors consider wholesale funding as the main channel where additional stress will materialise. In the most severe scenario a 75% cumulative run-off over 30 business days is assumed on wholesale funding. Even in this scenario the modelled average large US bank will be able to cover the outflow with liquid assets. However, the authors assume no stress on retail deposits.

The parameters of the LCR stress scenario form a benchmark of a cyber incident stress scenario and capture already significant stress.[15] In the base stress scenario, we consider the stress parameters as specified in the LCR rules (LCR scenario). These stress parameters contain a haircut on specific assets as well as assumptions on the in- and outflows of funds

14 Note that in the Netherlands the deposit guarantee scheme covers up to EUR 100,000 per account holder, which limits the incentives for savers to withdraw funds.
15 Basel Committee on Banking Supervision (2019), Liquidity Coverage Ratio Application guidance.

during a 30-day period. The haircut applied to the initial stock of liquid assets and the assumed run-off rates are included in the Appendix (tables A1 and A2, respectively). If the LCR stress scenario does not specify haircuts or run-off rates for specific liquidity categories, conservative assumptions have been applied, based on previous liquidity stress tests such as the 2019 Liquidity Stress Test from the ECB.

The reverse stress test scenarios extend the LCR stress scenario to assess the maximum deposit withdrawals a bank can sustain in case of liquidity stress following a cyber incident. The first reverse stress test scenario assumes that a cyber incident causes stress in both market financing and deposits. By keeping the run-off rates of market financing as specified in the LCR scenario, this reverse stress test scenario assumes that the cyber incident leads to similar market stress to that in the LCR scenario. Our analysis answers the question what the maximum run-off rates on deposit withdrawals are that the bank can handle before it runs out of liquidity. The second reverse stress test scenario assumes that uncertainty caused by the cyber incident leads to significantly higher stress in market financing. It assumes run-off rates of 100% on all security financing for both inflows and outflows. In addition, the inflows resulting from retail customers, non-financial corporates and other counterparties are set to 0%. It is assumed that the bank continues to provide financing to these customers, which is relevant from a macroprudential perspective. This second scenario then answers the question of how large deposit withdrawals can be before the bank runs out of liquidity if the cyber incident leads to very severe market stress. In both scenarios the same haircuts on the initial CBC are assumed as in the LCR scenario, since the impact on the value of the collateral should in principle be the same as in the baseline scenario.

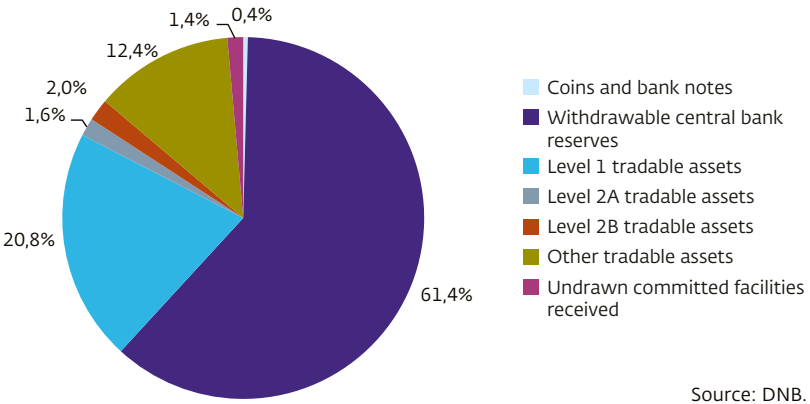
Results

The data used are the COREP liquidity reports from the four largest Dutch commercial banks as at 28 February 2022. These four banks (ABN AMRO Bank, ING Bank, Rabobank and De Volksbank) represent about 85% of the risk-weighted assets of the Dutch banking system, which implies that the data used are representative of the Dutch banking system. The results below do not show individual bank results, but should be interpreted as being representative of a bank with a liquidity position equal to the average of the Dutch banking system.

The majority of the counterbalancing capacity (CBC) is made up of withdrawable central bank reserves (61%) and level 1 tradable assets (21%). These assets are relatively insensitive to market turmoil, with stable prices even in stressed markets. Figure 10 shows the composition.

Figure 10 Composition of the counterbalancing capacity

Percentages



Source: DNB.

The high share of withdrawable central bank reserves is to a large extent driven by the ECB's monetary policy and in particular the asset purchase programmes and the TLTRO III programme. The low interest rates banks pay in the TLTRO-III programme[16] made it attractive for banks to obtain funding from the ECB, which increased central bank reserves (Åberg et al., 2021). For the four Dutch banks in the sample TLTRO-III borrowing amounts to EUR 156 billion[17]. The current ECB monetary policy framework provides ample liquidity to banks. Therefore, the banks' current CBC is probably not representative of historical liquidity positions. This implies that the size and composition of the banks' liquidity buffers is likely to change after the TLTRO-III programme ends. On another note, banks can get access to additional liquidity via main refinancing operations (MROs) and longer-term financing operations (LTROs) from the ECB. Please note that the LCR run-off rates in Appendix A assume, in line with the LCR, no outflows to the central bank due to maturing secured lending operations.

In line with the LCR, we apply a 30-day horizon for the liquidity stress scenario and compare the initial net liquidity position with the position at day 30. We assume the stress associated with the cyber incident lasts for at least 30 days. The starting position is indexed to a value of 100. The bars in the waterfall charts that follow can therefore be interpreted as the percentage increase or decrease in the net liquidity position due to a specific factor.

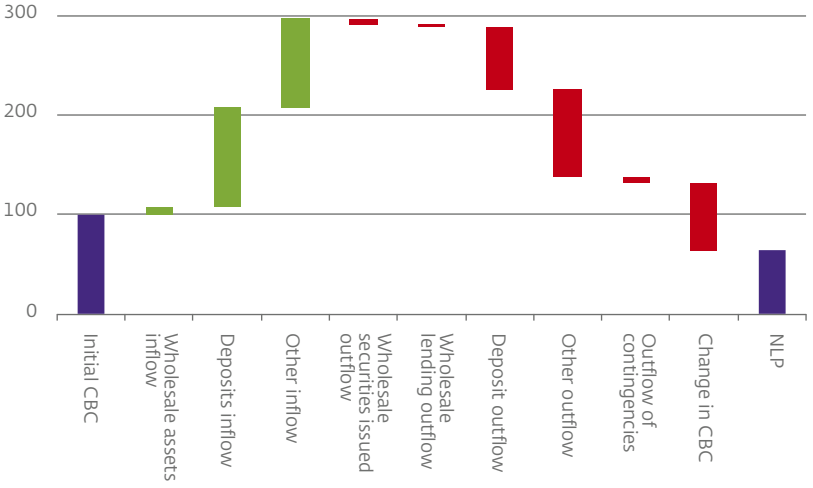
In the LCR scenario, the bank's net liquidity position remains positive. As the LCR regulation requires banks to hold sufficient liquid assets for 30 days, the outcome of this scenario meets the expectation that the net

16 Targeted Longer-Term Refinancing Operations.
17 TLTRO participations as at 31 December 2021 are EUR 35 billion for ABN AMRO (ABN AMRO Bank, 2022), EUR 65.5 billion for ING (ING Bank, 2022), EUR 55 billion for Rabobank (Rabobank, 2022) and EUR 0.8 billion for De Volksbank (De Volksbank, 2022).

liquidity position will be positive. Figure 11 shows results of the LCR scenario, where the inflow of deposits and other inflows lead to an increase in liquidity. On the other side, other outflows account for the largest part of a liquidity decrease, followed by deposit outflow. In addition, the change in the value of the CBC due to the liquidity stress plays a significant role in the resulting net liquidity position. Please note that the change in CBC is driven both by the initial valuation shock (as specified in Table A1) as well as a natural decrease when the assets in the initial CBC lead to liquidity inflows during the scenario horizon.

Figure 11 Waterfall graph net liquidity position in LCR scenario

Index; initial CBC=100

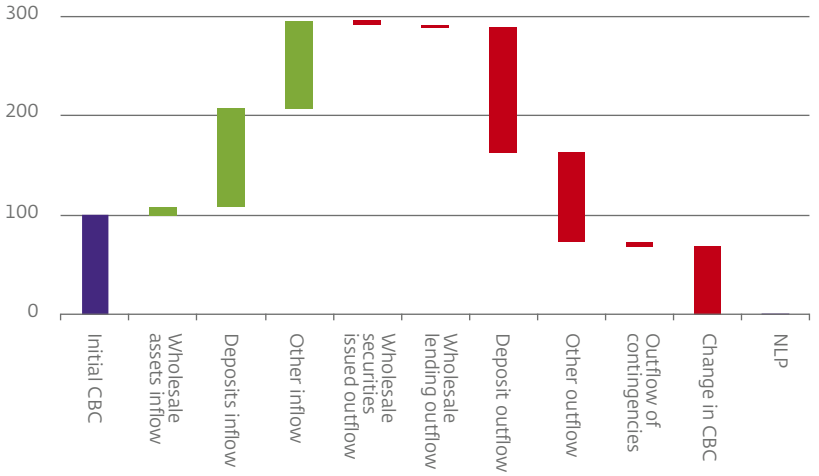


Source: DNB.

The ability of banks to absorb additional stressed deposit outflows differs substantially between the two reverse stress test scenarios. Figure 12 shows that in the first reverse stress scenario, stressed deposit outflows can double compared to the LCR scenario before a net liquidity position of zero is attained after 30 days. Because inflows remain the same, outflows from both wholesale lending and deposits could increase substantially before the bank runs out of liquidity. Figure 13 shows the results of the second scenario, in which additional market stress and lower inflows are assumed. The decreased inflow, in particular in deposits, substantially reduces the ability of the bank to absorb deposit outflows compared to the first reverse stress scenario.

Figure 12 Waterfall graph net liquidity position in LCR based reverse stress test

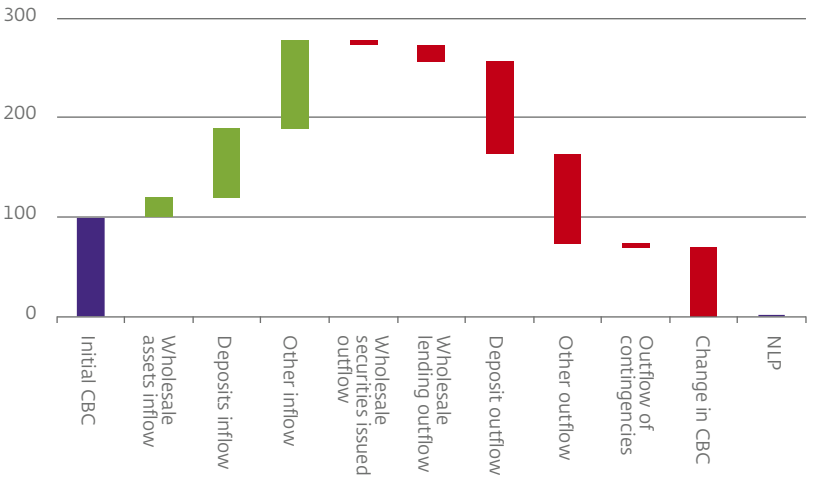
Index; initial CBC=100



Source: DNB.

Figure 13 Waterfall graph net liquidity position in market stress reverse stress test scenario

Index; initial CBC=100



Source: DNB.

Table 1 shows the maximum deposit run-off rates in both reverse stress tests. The run-off rate for stable retail deposits is 25% in the first reverse stress scenario. This is almost five times the stable retail deposit outflow in the LCR stress scenario. For other retail deposits the reverse stress test assumes 39% compared to 10% in the LCR scenario. Also, in order to attain a net liquidity position of zero, much higher outflow rates on operational deposits and non-operational deposits from non-financial corporates need to be assumed. The maximum deposit run-off rates in the second reverse stress scenario with full market stress are 10-12% lower compared to the first reverse stress scenario.

Maximum deposit withdrawal rates are lower for the most vulnerable bank in the sample. Table 1 also shows the maximum deposit run-off rates for the most vulnerable bank. These rates could be considered as the lower bound where one individual bank will become illiquid, which could have an impact on other banks. The maximum run-off rates of the first reverse scenario for the weakest bank come close to that of the representative bank, while the run-off rates for the second reverse scenario are closer to the LCR scenario. Other combinations of the run-off rates can lead to the same outcome. In the reverse stress tests it is assumed that the relative stability between different deposits is maintained, i.e. stable retail deposits have lower run-off rates compared to other retail deposits.

Table 1 Stressed run-off rates for deposits

		Representative bank		Weakest bank	
	LCR	LCR+ deposit withdrawal	Full market stress	LCR+ deposit withdrawal	Full market stress
Stable retail deposits	5%	25%	13%	23%	9%
Other retail deposits	10%	39%	27%	37%	14%
Operational deposits	25%	47%	37%	45%	29%
Non-operational deposits from non-financial corporates	40%	75%	63%	72%	45%

The maximum run-off rates calculated in the reverse stress tests are relatively high compared to historical bank runs and liquidity stress scenarios. For example, in the 2019 Liquidity Stress Test (LiST) the ECB applied two scenarios where in the adverse scenario stable retail deposits faced a run-off rate of 18% and in the severe scenario 27%, both over a

six-month horizon. In its 2017 Financial Sector Assessment Program (FSAP) liquidity stress test for the Netherlands, the IMF used run-off rates of 20% on stable retail deposits after a five-week horizon. With regard to actual bank runs, in October 2009 savers withdrew around 18% of their deposits at DSB Bank in 12 days. In late September 2008, Washington Mutual faced deposit withdrawals equal to 9% in 10 days. The British bank Northern Rock faced deposit withdrawals of 57%, but over a three-and-a-half-month period during 2007.

The results indicate that a representative bank could absorb large stressed liquidity outflows from a confidence shock potentially caused by a cyber incident. For a cyber incident to affect financial stability via the confidence channel, very large liquidity stresses are needed of magnitudes comparable to historical bank runs. However, the results show that there could be potential weaker players in the system that may be more susceptible to confidence shocks. In combination with other transmission channels, this might increase the impact on financial stability.

When interpreting the above results it is important to highlight several key assumptions that can mitigate or amplify the outcomes of the liquidity stress the bank faces. First, with cyber incidents in place it could be possible that the online banking environment is not accessible to customers. It is assumed in the scenarios that customers are able to withdraw funds from their bank account either by bank transfer or cash withdrawal. In a similar way, the bank has access to markets to conduct transactions despite the cyber incident. Second, in the event of multiple bank attacks, it is more difficult to withdraw and transfer funds to other bank accounts. While the stress would in this case have a more systemic nature, deposit withdrawals at the bank level are likely to be lower. Third, it is assumed that markets are generally liquid, i.e. that assets can be sold with no or little loss of value,

or that the losses do not exceed the regulatory haircuts. Fourth, we assume that no management actions are taken and that no use is made of additional available central bank liquidity programmes such as borrowing at MRO or LTRO rates. Lastly, our analysis chose a specific set of stress parameters for a period of 30 days. Other combinations of stress parameters could also lead to a zero net liquidity position. The effect could also be different for a different time period. Further analysis could be done to better understand the sensitivity of the results to the duration of the scenario.

Overall, we conclude that cyber incidents can have a systemic impact in extreme scenarios through either the operational or confidence channel. An important caveat to our results is that we analyse only two transmission channels, whereas many other cyber-related scenarios that potentially put financial stability under pressure are conceivable. Going forward, rather than assessing these two channels in isolation, it would be relevant to consider the interaction between multiple channels. For example, issues in TARGET2 affect the transactions between banks. This leads to more stress on the expected in- and outflows and impacts the counterbalancing capacity to absorb these shocks. Moreover, further analysis could explore the role of liquidity provision by the ECB as last lender resort in stress scenarios arising from cyber incidents. Specifically, the ECB has a fixed rate full allotment policy where banks can borrow at the fixed MRO rate from the ECB as long as the bank has eligible collateral available.

4 Policy

The potentially systemic nature of cyber risk calls for a macroprudential policy perspective in addition to the existing supervisory measures aimed at strengthening the cyber resilience of individual financial institutions. The development of such a perspective is still at an early stage and the ability of existing macroprudential tools to prevent amplification of cyber incidents appears limited. As a first step, macroprudential authorities need to develop their systemic cyber risk monitoring, specifically of potential amplification channels.

4.1 Macroprudential policy

Systemic cyber risk requires a concurrent mitigation by both micro- and macroprudential policies. The risks arising from the aggregate impact of cyber risk at individual institutions can be reduced and mitigated by microprudential supervision, which makes it an essential tool in reducing the threat of cyber risk to financial stability. Microprudential policies are already relatively mature and have been developed to deal with cyber risk from different angles. For example, according to the EBA Guidelines on ICT and security risk management, banks have to carry out scenario analyses as part of sound business continuity management, also taking into account cyber-attacks. At the same time, microprudential policy will not prevent cyber incidents from happening. Moreover, microprudential and oversight approaches cannot fully address the concerns for the stability of the financial system as a whole.

The threats posed by systemic cyber risk require further work on developing macroprudential policy. Compared to microprudential regulation on cyber risk, macroprudential policies have not yet focused strongly on cyber risk. Until now, macroprudential policy has mainly been targeted at increasing the resilience of financial institutions to financial risks.

The lack of incorporation of cyber risk in macroprudential policies can be explained by the fact that cyber risk has long been seen as a type of operational risk that has to be mitigated by microprudential policies. Another explanation could be that we have not yet witnessed an actual systemic cyber incident with a profound impact on financial stability. However, as discussed in Chapter 2, cyber risk has evolved from an operational risk with only a limited potential impact on financial stability to a systemic risk with the potential for disruptive effects on financial stability and critical functions of the financial system. Cyber incidents particularly differ from other operational risks in terms of speed and scale of propagation. The potential systemic impact of cyber risk therefore calls for the attention of macroprudential authorities. Microprudential and oversight regulations should be complemented by a macroprudential perspective.

Existing macroprudential tools are not designed for the mitigation of cyber risks and may prove ineffective for dealing with the impact of cyber incidents. For instance, instruments such as systemic risk buffers (CRD Article 133), countercyclical capital buffers (CRD Article 130) and liquidity tools (laid down in CRR Part Six) may not be the right instruments to prevent a systemic event if a systemically important bank loses access to its account balance data due to a cyber incident. In a similar vein, such instruments will not be effective if a cyber incident paralyses the operations of a critical financial market infrastructure for a prolonged period. At the same time, when financial tools are adapted to systemic cyber risk, they could contribute to loss-absorbing capacity in the event of a systemic cyber event. These kinds of tools could play a role in preventing amplification of a cyber incident (see Chapter 2). Capital and liquidity tools can serve as a buffer for cyber-related losses, and thus may help contain amplification. For example, the availability of central bank liquidity as a lender of last resort, e.g. with the fixed rate full allotment policy, can be an important tool

to reduce the risk of bank runs spreading through the system. However, they may not do much to prevent runs, for example, if customers fear a loss of access to their funds (Federal Reserve, 2021). They may also not speed up the restoration process after a cyber incident and the operational dimension of cyber risk would remain unaddressed. As such, the suitability of existing macroprudential instruments to serve as cyber risk mitigants is limited. Applying existing tools to mitigate systemic cyber risk may also overburden these tools by assigning them a role for which they are not designed and implemented. Therefore, macroprudential tools ideally target the source of the cyber risk directly and not at the end of the chain when impact following the cyber incident has already become significant.

Macroprudential policies to mitigate systemic cyber risk need to be applied beyond banks. Systemic cyber risk is perceived as a structural risk that any entity providing services in or to the financial system is exposed to (ESRB, 2022). As such, the macroprudential policies do not only need to cover credit and other financial institutions, but need to be expanded to include third-party providers, as is also foreseen for microprudential supervisory authorities in the forthcoming Digital Operational Resilience Act (DORA).

Macroprudential tools can be of particular use to prevent or reduce amplification and contagion once a systemic cyber incident has occurred. Macroprudential instruments can assist in preventing a cyber incident becoming systemic and jeopardising financial stability, for instance by preventing a spillover from the operational to the financial level or from affecting confidence in the financial system. For example, the adaptation of financial tools to systemic cyber risk could contribute to loss-absorbing capacity in the event of a systemic cyber event. The difference with most microprudential tools is that these tools address a cyber incident in an early phase (Chapter 2), but do not prevent or mitigate amplification or contagion once the incident has occurred.

4.2 Monitoring and stress testing

As a first step, macroprudential authorities need to develop or expand their systemic cyber risk monitoring. To guide the implementation of policies to address systemic cyber risk, a set of indicators needs to be developed. For instance, the financial stability surveillance framework of the Financial Stability Board (FSB, 2021) proposes multiple indicators to monitor cyber vulnerabilities. A monitoring framework of cyber indicators helps to improve insight into the development of cyber risks. However, combining the available information into a system-wide monitoring framework has proven to be difficult (see also Box 1 in Chapter 1). Moreover, in the event of a serious cyber incident, the implications need to be assessed quickly to enable a timely activation of systemic cyber risk mitigants and to minimise the degree of amplification and contagion. Therefore, regular monitoring of the contagion channels among operational systems and within the financial system is needed to understand the amplification mechanisms that could lead to a systemic cyber crisis (ESRB, 2022). This requires a better understanding of the risks as well as a higher level of analytical and monitoring capability for systemic cyber risk.

Cyber stress tests provide a useful tool to examine the impact of a severe but plausible cyber incident. Stress tests aim to reveal financial institutions' capacity to respond to and recover from a severe but plausible cyber incident scenario. These stress test exercises can explore how shocks stemming from cyber incidents in a hypothetical stress scenario work out for systemic institutions and for the system as a whole. As such, stress tests can help in identifying cyber-related vulnerabilities in the financial system. The ESRB (2022) distinguishes two approaches for testing financial institutions' resilience in severe but plausible cyber scenarios. The first approach incorporates systemic cyber risk scenarios into existing financial stress testing to assess the capacity to absorb losses resulting from cyber incidents.

The focus is on the analysis of cyber related losses and liquidity stress testing, to assess the financial impact of a cyber incident and to model financial contagion and amplification. The second approach is a systemic cyber resilience stress test, which examines the operational capability at an earlier stage of the cybercrisis to absorb a cyber incident (see e.g. Bank of England, 2021). These kinds of tests can complement each other and can help to strengthen the financial system's resilience and its ability to support the continuity of critical economic functions.

Tolerance levels for disruption can be a useful benchmark against which systemic cyber stress test results can be evaluated. Regular stress tests typically use benchmarks related to the solvency of financial institutions (e.g. minimum capital requirements for banks) to assess the outcomes. In a similar vein, the ESRB proposes the development of tolerance levels for the impact of cyber incidents. The aim of impact tolerances is to quantify the maximum acceptable level of disruption to critical economic functions that does not pose a risk to financial stability in severe but plausible scenarios. On a macroprudential level, the tolerance for disruption can be set to reflect the tipping point at which the financial system is no longer able to absorb a cyber-related shock and financial stability is in danger. For implementation, impact tolerances should be expressed in terms of concrete metrics, such as the maximum duration of a certain disruption or the number of customers affected. By benchmarking stress test results against these expectations, systemic cyber stress tests could provide useful information about the cyber resilience of institutions and reveal potential vulnerabilities. However, setting tolerance levels for disruption is still a novel and relatively conceptual topic and further considerations are needed on how it can be incorporated into systemic cyber stress tests.

Systemic cyber risk monitoring and stress tests can be used for the development and calibration of mitigating tools. First, to develop cyber risk mitigants, insights from systemic cyber indicators and stress tests are useful input. In the second phase, they can be used to inform the actual implementation of cyber risk mitigants and to guide and evaluate cyber policy interventions.

The further development of a macroprudential perspective on cyber risk is an important challenge for the coming years. As this study has shown, both the assessment of systemic cyber risks and the policy framework for mitigating these risks are currently still in their infancy. More analysis is needed to draw conclusions about the potential impact of cyber incidents on financial stability and to design and implement macroprudential policies to strengthen systemic cyber resilience.

References

Åberg, P., M. Corsi, V. Grossmann-Wirth, T. Hudepohl, Y. Mudde, T. Rosolin and F. Schobert (2021, Demand for central bank reserves and monetary policy implementation frameworks: the case of the Eurosystem. ECB Occasional Paper Series No 282 / September 2021.

Accenture (2021), Cyber Threat Intelligence Report.

ABN AMRO Bank N.V. (2022), Integrated Annual Report 2021.

Aldasoro, I., Gambacorta, L. Giudici, P. and Leach, T. (2022), The Drivers of Cyber Risk. Journal of Financial Stability 60, June 2022, 100989.

Bank of England (2021), Financial Policy Summary and Record of the Financial Policy Committee Meeting on 11 March 2021.

Bank of International Settlements (2020), The drivers of cyber risk.

De Volksbank (2022), De Volksbank Annual Report 2021.

DNB (2020), Financial Stability Report Autumn 2020.

Duffie, D. and Younger, J. (2019), Cyber Runs, Hutchins Center Working Paper #51.

Dutch Payments Association (2021), Facts and Figures on the Dutch Payment System in 2021.

ECB (2021), Annual report on the outcome of the 2020 SREP IT Risk Questionnaire.

Eisenbach, T. M., Kovner, A. and Lee, M. J. (2022), Cyber Risk and the US financial system: A pre-mortem analysis, Journal of Financial Economics, forthcoming.

ESRB (2020), Systemic Cyber Risk.

ESRB (2022), Mitigating Systemic Cyber Risk.

ESRB (2022), Review of the EU Macroprudential Framework for the Banking Sector, Concept Note.

Federal Reserve Board (2021), Financial Stability Report.

Financial Stability Board (2021), Financial Stability Surveillance Framework.

ING Bank (2022). ING Bank Annual Report 2021.

Kosse, A. and Lu, Z. (2022), Transmission of Cyber Risk Through the Canadian Wholesale Payments System, Bank of Canada Working Paper.

Rabobank (2022), The cooperative Rabobank Annual Report 2021.

Euro zone banks left flying solo by new glitch in ECB payment system | Reuters.

Appendix

Table A1 - Shocks to the initial stock of liquid assets in the LCR scenario

Counterbalancing capacity	
Coins and banknotes	100%
Withdrawable central bank reserves	100%
Level 1 tradable assets	100%
Level 2A tradable assets	85%
Level 2B tradable assets	50%
Other tradable assets	
Central government (CQS1, 2 & 3) (cbc)	90%
Shares	50%
Covered bonds and ABS	70%
Other tradable assets (cbc)	50%
Non tradable assets eligible for central banks	90%
Facilities	
Undrawn committed facilities received	100%
Other facilities	100%

Table A2 Shocks to the inflows and outflows in the LCR scenario

Outflows	
Liabilities resulting from securities issued (if not treated as retail deposits)	100%
Liabilities resulting from secured lending and capital market-driven transactions collateralised by Level 1, 2A, 2B tradable assets and other assets	
Level 1 tradable assets	0%
Level 2A tradable assets	15%
Level 2B tradable assets	50%
Other tradable assets (out)	100%
Other assets (out)	100%
Liabilities not reported in 1.2, resulting from deposits received (excluding deposits received as collateral)	
Stable retail deposits	5%
Other retail deposits	10%
Operational deposits	25%
Non-operational deposits from credit institutions	100%
Non-operational deposits from other financial customers	100%
Non-operational deposits from central banks	40%
Non-operational deposits from non-financial corporates	40%
Non-operational deposits from other counterparties	100%
FX swaps maturing (out)	100%
Derivatives amounts payable other than those reported in 1.4	100%
Other outflows	100%
Committed credit facilities	
Considered as Level 2B by the receiver	6%
Other (con)	6%
Liquidity facilities	38%
Outflows due to downgrade triggers	100%

Inflows	
Monies due from secured lending and capital market-driven transactions collateralised by:	
Level 1 tradable assets	0%
Level 2A tradable assets	15%
Level 2B tradable assets	50%
Other tradable assets (in)	100%
Other assets (in)	100%
Monies due from loans and advances granted to:	
Retail customers	50%
Non-financial corporates	50%
Credit institutions	100%
Other financial customers	100%
Central banks	100%
Other counterparties	50%
FX swaps maturing	100%
Derivatives amounts receivable other than those reported in 2.3	100%
Paper in own portfolio maturing	100%
Other inflows	100%

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 20 524 91 11
dnb.nl