

# DNB 2025 | Cyber strategy

DeNederlandscheBank

EUROSYSTEM

# Table of Contents

Introduction

External developments

How we strengthen cyber resilience

How we make ourselves cyber resilient

# Introduction

At DNB we work on trust. We want to safeguard financial stability and thus contribute to sustainable prosperity in the Netherlands. We are pursuing this objective in an environment that is more dynamic than ever. Digitalisation, rising geopolitical tensions and similar developments fuel the cyber risks to which the financial sector is exposed. This is why we are committed to boosting the cyber resilience of the financial sector.

## A resilient financial sector

The increasing digitalisation of society, remote working and rising geopolitical tensions are making the contours of the risk landscape more complex and dynamic, while the cyber risks to society and the financial sector are becoming ever more real. Financial institutions are an attractive target for cyberattacks because of their high-value assets, sensitive customer information and the pivotal role they play in the economy. DNB itself is not immune to cyber risks.

These risks can lead to substantial losses and even jeopardise the security and continuity of the payment system. Criminals sometimes launch cyberattacks directly on financial institutions themselves, but they have also stepped up attacks on the ICT service providers that institutions increasingly rely on. This can give rise to concentration risks when multiple institutions source services from the same provider. A major cyber incident not only damages the institution, but can also undermine confidence in the financial sector, with potential implications for financial stability. As the use of cash declines, any disruption in digital payment systems can therefore have increasingly serious consequences. Cyber risks are in fact nothing less than a systemic risk.

In this cyber strategy, we clarify how, as a central bank, supervisory authority and resolution authority, we contribute to strengthening the financial sector's cyber resilience. This cyber strategy fleshes out the DNB2025 vision and strategy in further detail.

External developments	4
How we strengthen cyber resilience	8
How we make ourselves cyber resilient	12

# External developments

## Changing cyber landscape

### Key cyber risks in 2023

#### 1. Ransomware

A type of cyberattack in which systems and data are encrypted using malware. Decryption is possible only after paying a ransom to the criminals. Besides being encrypted, data is often stolen. Its public release can then be prevented by paying a ransom.

#### 2. Attack on third parties

A cyberattack on third-party providers of vital services. System failure or data theft at the third party can have far-reaching consequences for the financial institution.

#### 3. Attack through third parties

A cyberattack in which a criminal gains access to the financial institution's systems through a third-party service provider.

#### 4. Advanced phishing through artificial intelligence

From time to time, Dutch financial institutions have been the victim of sophisticated phishing attempts targeting executives and (critical) employees. This type of phishing may become even more sophisticated and targeted in the near future with the emergence of readily available AI techniques, such as face and voice cloning.

#### 5. Insiders

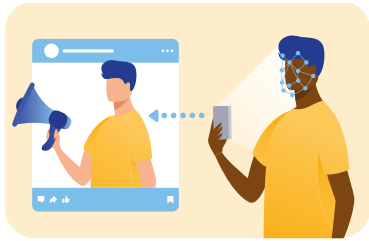
A malicious employee may be placed inside an organisation or recruited by criminals, thereby posing a threat to the organisation.

With ongoing digitalisation and close interconnectedness, financial institutions are more exposed to cyber risks than ever before. In addition, these risks are in constant flux.

Key trends affecting the risks to which institutions are exposed include advancing technological development, rising geopolitical tensions and increased outsourcing of digital business processes to IT service providers.

## Technological development leads to rapidly evolving cyber risks

Technological developments in the financial sector follow each other in rapid succession, offering opportunities such as cost savings and increasing consumer convenience. At the same time, technological advancements enable malicious operators to carry out increasingly sophisticated cyberattacks and give them access to new working methods.



For example, artificial intelligence can be used to create deep fakes to launch disinformation campaigns, which can go viral via social media.



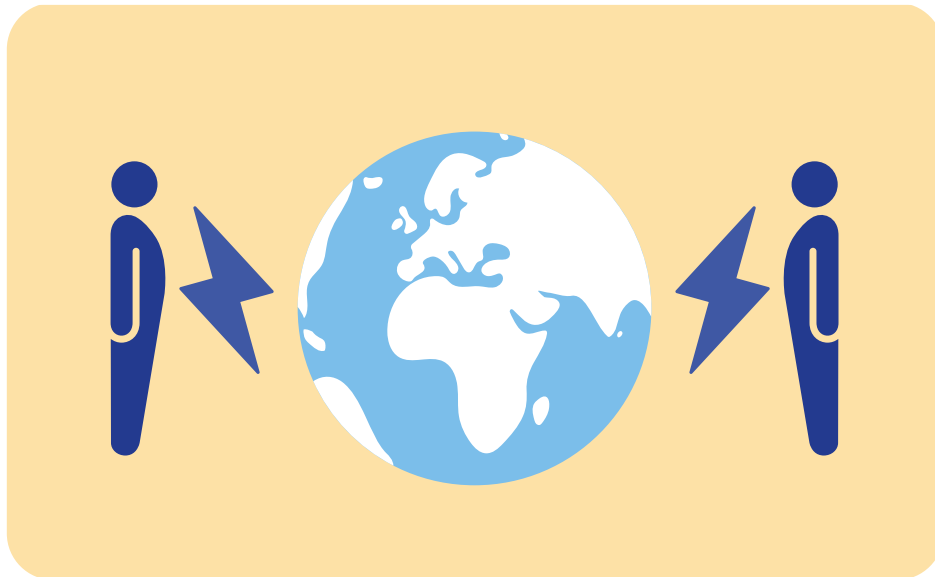
In the future, quantum computing may be able to break the encryption that institutions use. This has consequences for confidential customer data, vital systems, authentication processes and the encryption and decryption of payments.



Lastly, sophisticated technologies are also becoming accessible to an increasingly wide audience, some of which are offered by criminals for a fee (crime as a service).

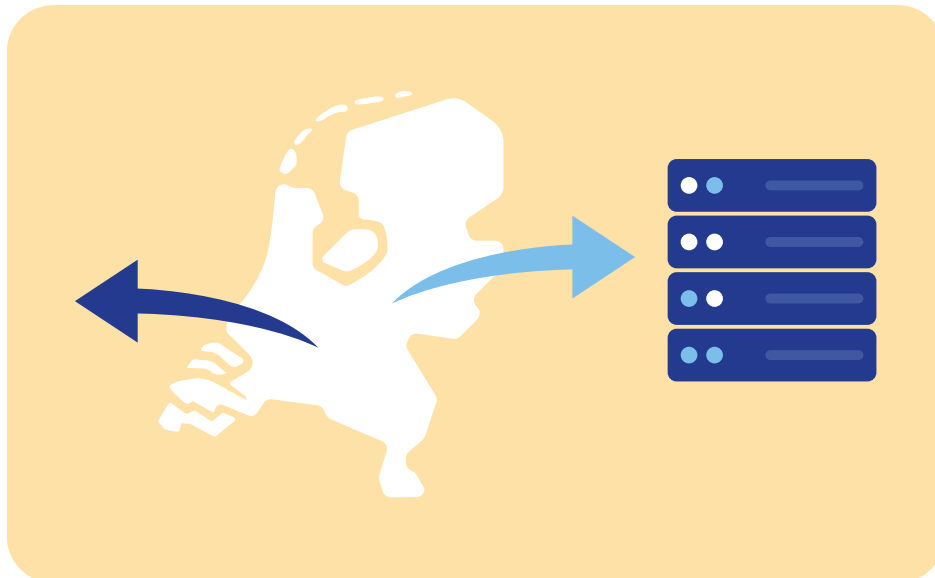
## Rising geopolitical tensions are exacerbating cyberthreats

Current political tensions (such as the situation in Ukraine) have changed the global landscape. Current events match longer-term trends, such as the shift from a unipolar world order, with the United States playing a central role, to a multipolar world order, with influential countries and regions committed to making fundamental changes to the world order. The accompanying tensions on the global stage give rise to potential threats to institutions in the digital domain. Such threats include disruptive cyberattacks by state actors, cyber espionage and insider threats.



## Outsourcing creates chain dependencies and potential concentration risks

Financial institutions are increasingly engaging the services of third parties to run their digital business processes, such as IT firms and cloud service providers. While many of these parties have considerable expertise and maintain high standards of cyber security and information security, outsourcing also introduces chain dependencies and complexity. Due in part to outsourcing trends, cyber attacks are therefore shifting to third parties. Outsourcing can also give rise to concentration risks if multiple institutions outsource to the same service providers. The failure of one crucial party could shut down services at a large part of the financial sector. Clearly, cyber resilience across the outsourcing chain must be understood and adequately managed.



# How we strengthen cyber resilience

## Strengthening the financial sector's cyber resilience

Cyber risks are evolving rapidly. This requires financial institutions, among other things, to actively monitor which cyber risks are relevant to them, keep their IT system security up to date, and periodically stress-test their cyber resilience. In sum, a cyber resilient financial sector requires a sustained effort.

As a central bank, supervisory authority and resolution authority, we contribute to strengthening cyber resilience by:

### **Monitoring institutions' cyber risk management**

- Targeted use of supervisory instruments
- Monitoring chain dependencies and concentration risks

### **Testing and organising drills together to boost cyber resilience**

- TIBER testing and sector-wide information sharing
- Cybercrisis drills and a readiness crisis structure for the financial core infrastructure

### **Sharing our knowledge with the sector and other stakeholders**

- Sharing knowledge and expertise with the financial sector, the public sector, critical infrastructure and EU





## Monitoring cyber risk management

For financial institutions' to conduct their business operations in a sound and ethical manner, they need to manage information security and cyber security risks, including in the event of outsourcing. We monitor that institutions are and remain cyber resilient. The Digital Operational Resilience Act (DORA) has come into force in January 2025, giving us additional tools to further strengthen the cyber resilience of the financial sector, including that of third parties.



### Targeted use of supervisory instruments

While cyberthreats are increasing, it appears that institutions do not always have basic measures in place. With our surveys and targeted examinations at multiple institutions, we see to it that institutions comply with laws and regulations. The overall lessons learned from these examinations are shared with the sector. It is important to ensure that executive and non-executive directors alike are sufficiently alert to cyber risks and knowledgeable about these risks. The updated corporate governance code covers this more explicitly. As part of our supervision, we devote specific attention to the required level of knowledge. In the context of the Single Supervisory Mechanism (SSM), we also conduct cyber stress tests. These tests reveal vulnerabilities, prompting lagging institutions to boost their cyber resilience.



### Monitoring chain dependencies and concentration risks

We see financial institutions increasingly outsource services. It is essential that they adequately manage the corresponding outsourcing risks and liabilities. Understanding and managing cyber resilience across the outsourcing chain is important and, partly due to the advent of DORA, is an important element of our supervision. This includes receiving adequate assurance reports covering the entire outsourcing chain that also report on an ex-ante basis, in addition to ex-post. DORA allows important steps to be taken in this respect, such as exercising direct oversight of critical third-party providers of ICT services despite not being financial institutions. Furthermore, potential concentration risks can be revealed as institutions will be required to report on their dependency on ICT service providers.

## Drills and tests to boost cyber resilience

To increase cyber resilience, it is important to test institutions' resilience to advanced cyberattacks and to conduct cybercrisis drills. Doing so will help identify strengths and weaknesses and help them learn how processes can be quickly recovered following an attack.



### TIBER testing and sector-wide information sharing

In the TIBER-NL programme, we coordinate threat-based testing of the digital resilience of (critical) financial institutions. Participants in the TIBER-NL programme include major banks, pension providers and insurers. The aim is to increase the cyber resilience of the Dutch financial sector against advanced cyber attacks. To this end, participating institutions also exchange experiences among themselves. The TIBER programme is being implemented in a growing number of European countries. We share our knowledge and experience with European countries that want to start their own TIBER programme. Through DORA, threat lead penetration testing may become mandatory for financial institutions.



### Cybercrisis exercises

Crisis coordination, communication and recovery drills to simulate a situation following a cyberattack are another focus area. Quick recovery and clear communication after a cyberattack help maintain trust in the financial sector. We therefore initiate and participate in cybercrisis drills to ensure everyone is better prepared. The scenarios simulated in these drills are based on current threats and developments, such as the declining use of cash and its implications as an alternative to digital payments. Experiences gained will provide guidance on boosting cyber resilience.

We coordinate the Operational tripartite crisis management body (Tripartiet Crisismanagement Operationeel – TCO) for the financial sector, in addition to focusing on sector crisis management in the event of operational disruptions in payments and securities. To this end, DNB, we work with the Dutch Authority for the Financial Markets (AFM) and the Ministry of Finance to organise drills and coordinate participation in (inter)national exercises, such as ISIDOOR.

## Sharing our knowledge with the sector and other stakeholders

As cyberattacks become more complex, sharing knowledge and experience between institutions in the financial sector is more important than ever. We share our knowledge and insights on cyberthreats and how to boost cyber resilience, including with the public sector, other supervisory and regulatory authorities and professional bodies.



### Widely sharing knowledge and expertise

We gain and share our insights through various means, including the following:

- Acting in tandem with the sector, we periodically plot the various threats in the One Financial Threat Landscape. This provides insight into the most current cyberthreats that institutions can act on. Furthermore, we share information on IT security and cybercrime-related incidents in trusted communities, such as FI-ISAC.
- From time to time, we issue news releases addressing our observations on IT and cyber risks. We also share benchmark data and results of sector-wide surveys, such as the Good Practices for Information Security. We share this information in addition to providing specific feedback to individual institutions.
- We contribute to conferences and take part in working groups in the public sector, professional bodies, European supervisory and regulatory authorities, and central banks. In addition, we advise on new laws and regulations, such as DORA.

We focus primarily on the financial sector. We also support the vital sectors most critical to the financial sector, such as the energy and telecom sectors, where mutual dependencies exist that affect the financial sector and where doing so is in alignment with our mandate. In a similar vein, we provide assistance to the public sector and the National Cyber Security Centre (NCSC), e.g. by providing advice on setting up a TIBER framework for the central government. Lastly, we work with ECB and other European central banks and supervisory and regulatory authorities, we invest in TIBER-EU (DORA TLPT) and monitor European cyber tests of the most vital systems for the EU. We are also an active liaison between Dutch financial institutions and ESCB/EU institutions.

# How we make ourselves cyber resilient


## What is DNB doing to be and remain cyber resilient?

DNB, as part of the Dutch financial sector, also faces the rapidly changing environment and the associated risks. This requires a continuous effort to keep our cyber resilience at the required level. We therefore impose on ourselves the same standards we apply to the financial sector, and are taking various measures. For instance, based on Good Practices on Information Security, we assess how DNB scores in the benchmark compared to other financial institutions. In addition, we participate in the FI-ISAC and work with intelligence and security agencies to address physical and digital threats. We also participate in the TIBER programme in which we are rigorously tested. Finally, we assess how DNB scores against international standards, and we exchange knowledge such as best practices with other central banks.



De Nederlandsche Bank N.V.  
PO Box 98, 1000 AB Amsterdam, the Netherlands  
+31 (0)20 524 91 11  
dnb.nl/en

**Follow us on:**

 Instagram

 LinkedIn

 X

**DeNederlandscheBank**

EUROSYSTEEM