EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Cyber risk – a supervisory perspective

SCION Day

22 October 2024

Elizabeth McCaul

ECB representative to the Supervisory Board

Overview

1 Introduction

2 Cyber risk landscape

3 Cyber resilience stress test

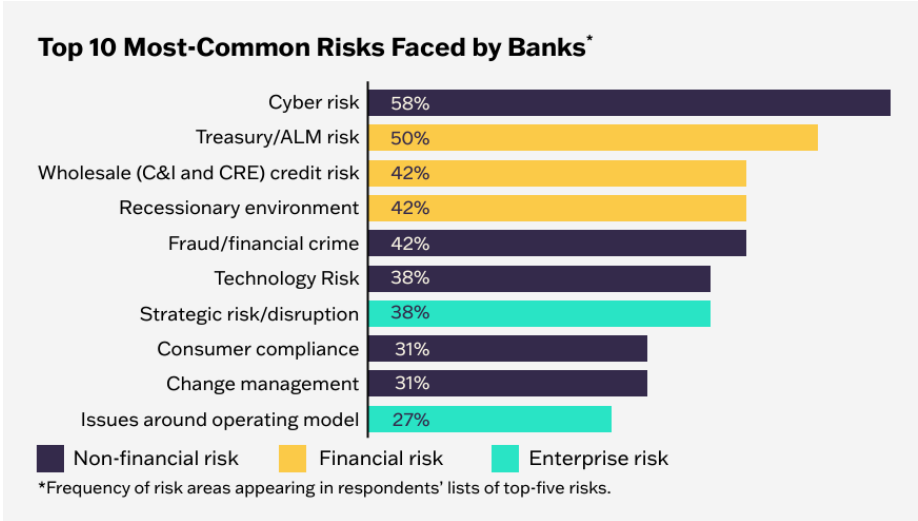
4 Conclusion

1

Introduction

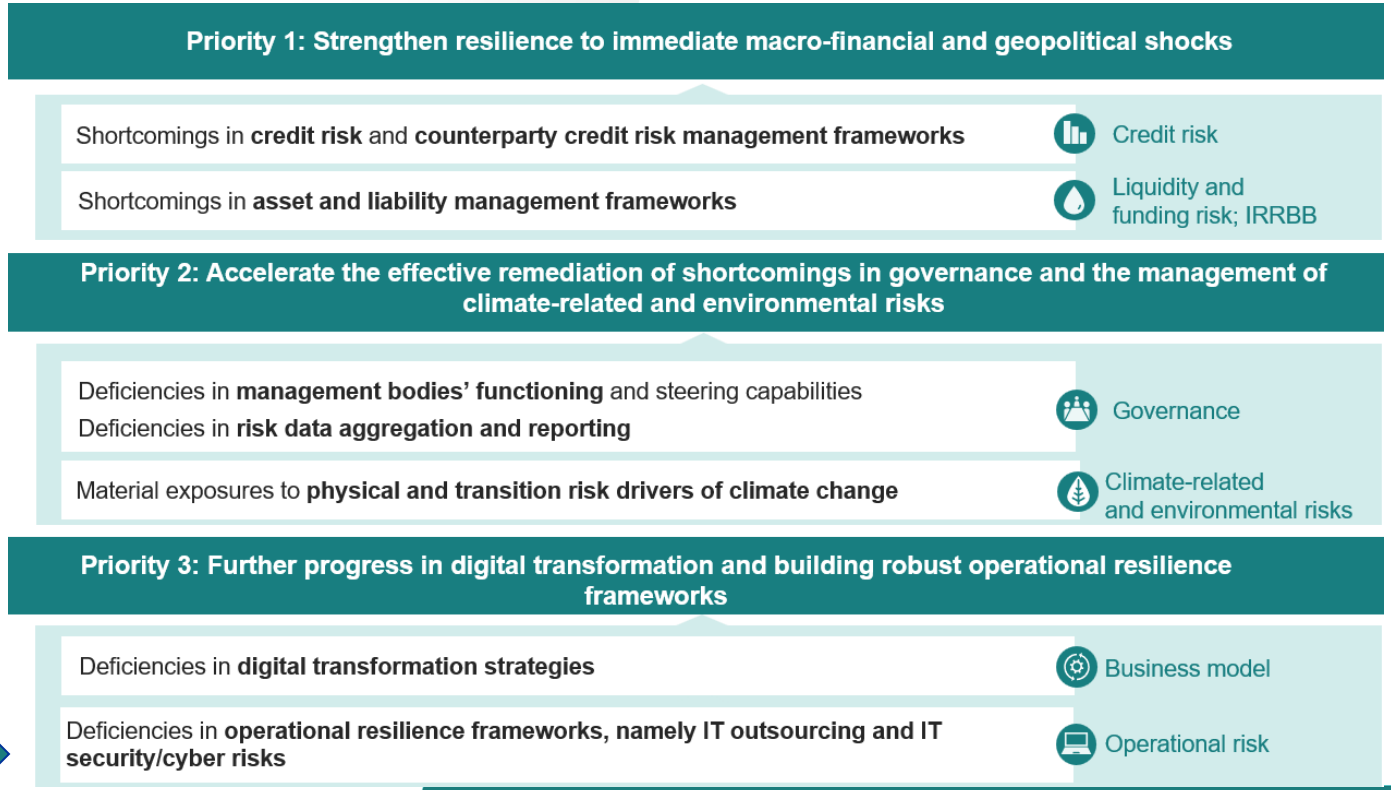
Cyber risk: one of the biggest threats facing banks today

- In a world of accelerating digitalisation and increasing geopolitical uncertainty, cyberattacks pose a significant risk to banks' stability
- Strengthening cyber resilience is vital for safeguarding trust in and the integrity of the financial system
- No IT environment is ever fully secure, so banks need to make sure they can adequately monitor and respond to the constantly evolving cyber threat environment



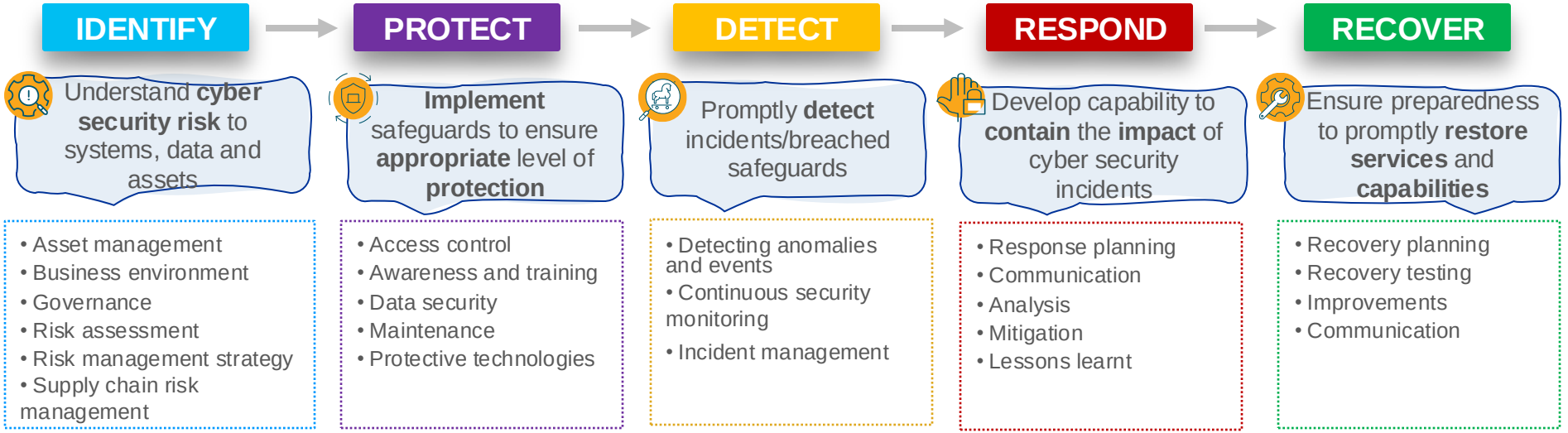
Source: Shifting Priorities, Enduring Risks: The 2024 RMA and Oliver Wyman CRO Outlook Survey

Cyber risk is a supervisory priority for 2024-26



What is cyber security?

- Cyber security focuses on preserving the confidentiality, integrity and availability of information through interconnected information infrastructures.
- The NIST* framework consists of the following phases:



***NIST** – US National Institute of Standards and Technology

ECB Banking Supervision's role in enhancing cyber resilience

- Continuous off-site supervision and risk assessments
  - Ongoing supervision of cyber and IT risks as part of the Supervisory Review and Evaluation Process (SREP) and follow-up on individual cyber incidents if needed
- Cyber incident reporting framework
  - Requires significant banks to report major cyber incidents
  - Enables the ECB to monitor and assess cyber threats in real time
- Thematic and horizontal reviews
  - Data collection and horizontal analysis of outsourcing registers
  - Targeted reviews of outsourcing arrangements and cyber resilience
- On-site inspections (OSIs)
  - Targeted OSIs of outsourcing, cyber security and IT risk management
- Cyber resilience stress test in 2024
  - Focusing on response and recovery capabilities

ECB’s role under the Digital Operational Resilience Act (DORA)

DORA aims to harmonise ICT risk supervision at European level via a directly applicable EU regulation

Oversight framework for critical third-party providers

- European Supervisory Authorities (EBA, ESMA, EIOPA) to identify third-party service providers that are critical for financial entities and designate a lead overseer (an ESA)
- ECB to participate in joint examination team (JET) activities
- ECB to integrate recommendations from the JETs in its supervision of credit institutions

ICT-related incident management

- Adjustment of SSM cyber incident reporting framework:
  - Additional reception of cyber threats (voluntary for banks)
  - Provide feedback to supervised banks

Advanced digital operational resilience testing

- Regular review of which banks are required to perform threat-led penetration testing (TLPT) (at least every three years)
- Validation of scope of each TLPT
- Attestation of TLPTs
- Follow-up of findings and recommendations resulting from TLPTs

ICT risk and ICT third-party risk management

- Supervision of IT and ICT third-party risk management in banks, based on legal requirements from DORA

2

Cyber risk landscape

Cyber risk threat landscape

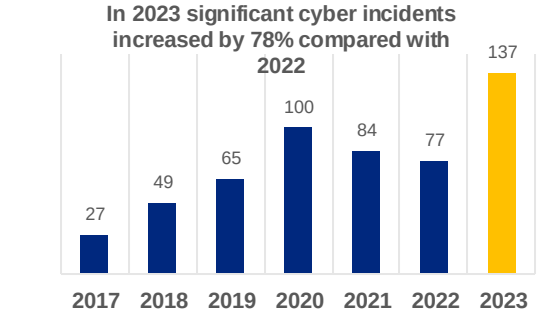
- **Ransomware:** type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability or in exchange for publicly exposing the target's data
- **Malware**: any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system
- **Social engineering**: a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services
- **Threats against availability - denial of service**: users of a system or service are not able to access relevant data, services or other resources, usually done by exhausting the service and its resources or overloading the components of the network infrastructure
- **Information manipulation**: a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively affect values, procedures and political processes
- **Threats against data**: any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed
- **Supply-chain attacks:** attacking a company's supply chain or third-party vendors to compromise the security of the final target

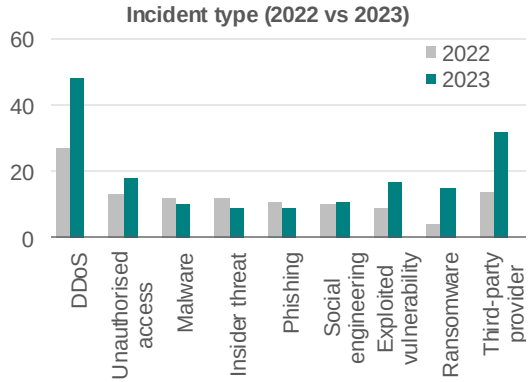
ENISA Threat Landscape 2024 - Prime threats

Source: European Union Agency for Cybersecurity (2024), *ENISA Threat Landscape 2024*.

Increasing cyber threats in a complex geopolitical environment and reliance on common third-party service providers continue to challenge banks

- **Cyberattacks** and reported **significant cyber incidents increased considerably**, with **ransomware attacks** on **service providers** soaring.
- **Distributed denial-of-service (DDoS)** attacks remain the most prevalent type of incident.
- **Increasing outsourcing of critical functions** to a globally concentrated group of third-party providers may expose banks to (potentially simultaneous) operational disruptions.
    - Banks report increasing dependency on third-party providers for critical functions, with a large share of services offered from a non-EU country.
    - Recent examples like the CrowdStrike incident and a DDoS attack on Microsoft services show the many interdependencies between sectors and the heavy reliance on common providers.





3

Cyber resilience stress test

What is a cyber resilience stress test?

In line with the high-level framework developed by the European Systemic Risk Board…

… a cyber resilience stress test is a tool through which tested entities:

- are presented with a **common, severe but plausible cyber-related scenario** that disrupts some critical functions;
- **identify and report what the impact and consequences** of the scenario would be on their organisation;
- report how they would **respond to and recover from that scenario.**

… a cyber resilience stress test is **not**:

- a penetration test (e.g. threat intelligence-based ethical red-teaming – TIBER) or an assessment of controls to prevent cyberattacks;
- conducted in real time;
- an assessment of the financial capacity (capital or liquidity) of the tested entities.

Objective: to assess the operational capacity of individual tested entities to cope with the scenario. It focuses on how banks respond to and recover from a cyberattack, rather than on how they would prevent one.

Overview of 2024 cyber resilience stress test

Key objective

- To assess **banks' ability to recover from a severe cyberattack** and ensure the continuity of critical services under stress.

Scope

- **109 banks**
- **28 of the 109 banks** were subject to more extensive testing

Methodology

- Fictitious **stress test scenario** under which all preventive measures failed and a cyberattack **severely affected the databases of each bank's core systems.**
- Scenario assumed that preventive actions and protection measures were bypassed or failed and a cyberattack successfully disrupted the bank's daily business operations.
- Banks then tested their **response and recovery measures**, including activating emergency procedures and contingency plans and restoring normal operations.
- All banks had to answer a **questionnaire** and **submit documentation** to the ECB.
- 28 banks were asked to perform an **actual IT recovery test**, provide evidence and were subject to an **on-site quality assurance review.**

The stress test showed that while banks do have high-level response and recovery frameworks in place, there is still room for improvement

- **Banks need to ensure that their recovery capabilities are sufficient to handle complex scenarios** and that they can **meet their recovery objectives** to protect customer assets and customer data.
- **The stress test increased awareness** and **enhanced banks' preparedness for a cyber crisis,** as the stress test process prompted banks to assess and further develop their cyber response and recovery capabilities.
- **The exercise steered banks in the right direction** by providing them with individual findings and recommendations with deadlines for follow-up.
- The outcome of the exercise **will feed into the 2024 SREP**. The cyber resilience stress test does not focus on banks' capital, so the results will not affect banks' Pillar 2 guidance.

4

Conclusion

Looking ahead: improving cyber resilience further

- Cyber risk has been a **key risk** for the banking sector for several years. Yet, some banks still show deficiencies in **basic cyber security measures.**
- We expect banks to **continuously improve their cyber resilience** to adapt to the evolving threat landscape.
- The **Digital Operational Resilience Act**, which is applicable from 17 January 2025, establishes a framework aimed at strengthening the resilience of the financial sector, including as regards relationships with critical third parties, and will require banks to strengthen their cyber risk management.
- Addressing emerging cyber threats is a **collaborative effort**. By working closely with banks and stakeholders across sectors, we want to build a more resilient banking system.

Thank you!

Annex

Cyber definitions and terminology

Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
Cyber event	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
Cyber incident	A cyber event that: i. jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
Cyber risk	The combination of the probability of cyber incidents occurring and their impact.
Cyber security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium.
Cyber resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.
Cyber threat	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.

Source: Financial Stability Board Cyber Lexicon.