EUROPEAN CENTRAL BANK

EUROSYSTEM

Cyber Risk and Financial Stability: *Trends, Drivers and Implications*

5th Annual Nordic Cyber in Finance Conference, Reykjavík

30 September 2022

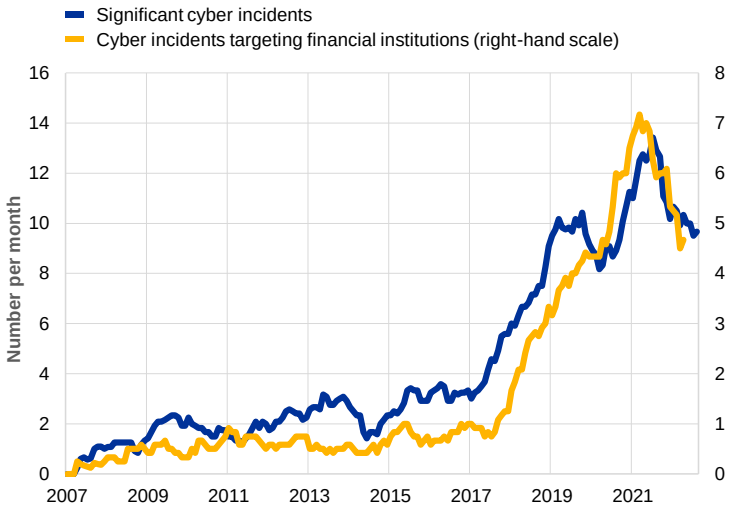
John Fell

Directorate General Macroprudential Policy and Financial Stability

Trends: Cyber attacks have become more frequent …

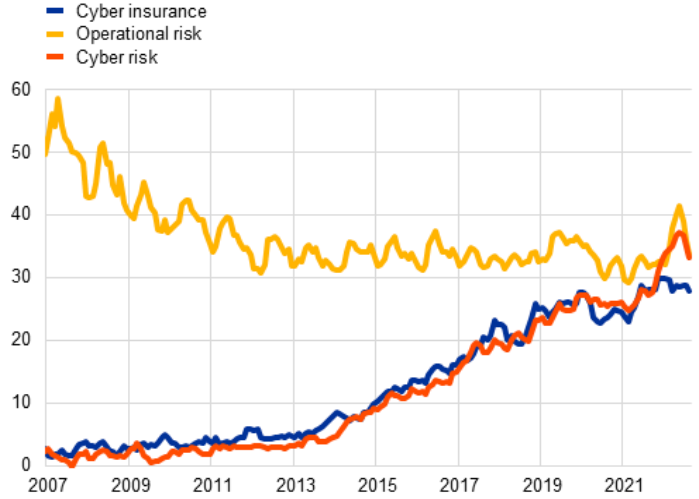
- Even before the pandemic, the number of cyber attacks was increasing …
- …and, looking forward, heightened geopolitical risk calls for vigilance

Significant global cyber incidents, and cyber incidents targeting financial institutions
Jan. 2007-Apr./Aug. 2022; number per month, 12m mov. avg.



Source: Center for Strategic & International Studies (CSIS), Carnegie Endowment for International Peace and ECB calculations.
Note: Significant cyber incidents cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

Interest in operational and cyber risk, and cyber insurance over time
Jan. 2007-Sep. 2022, index



Sources: Google trends, BIS and ECB.

Does cyber risk fall within the purview of financial stability overseers?

In other words, are cyber risks…

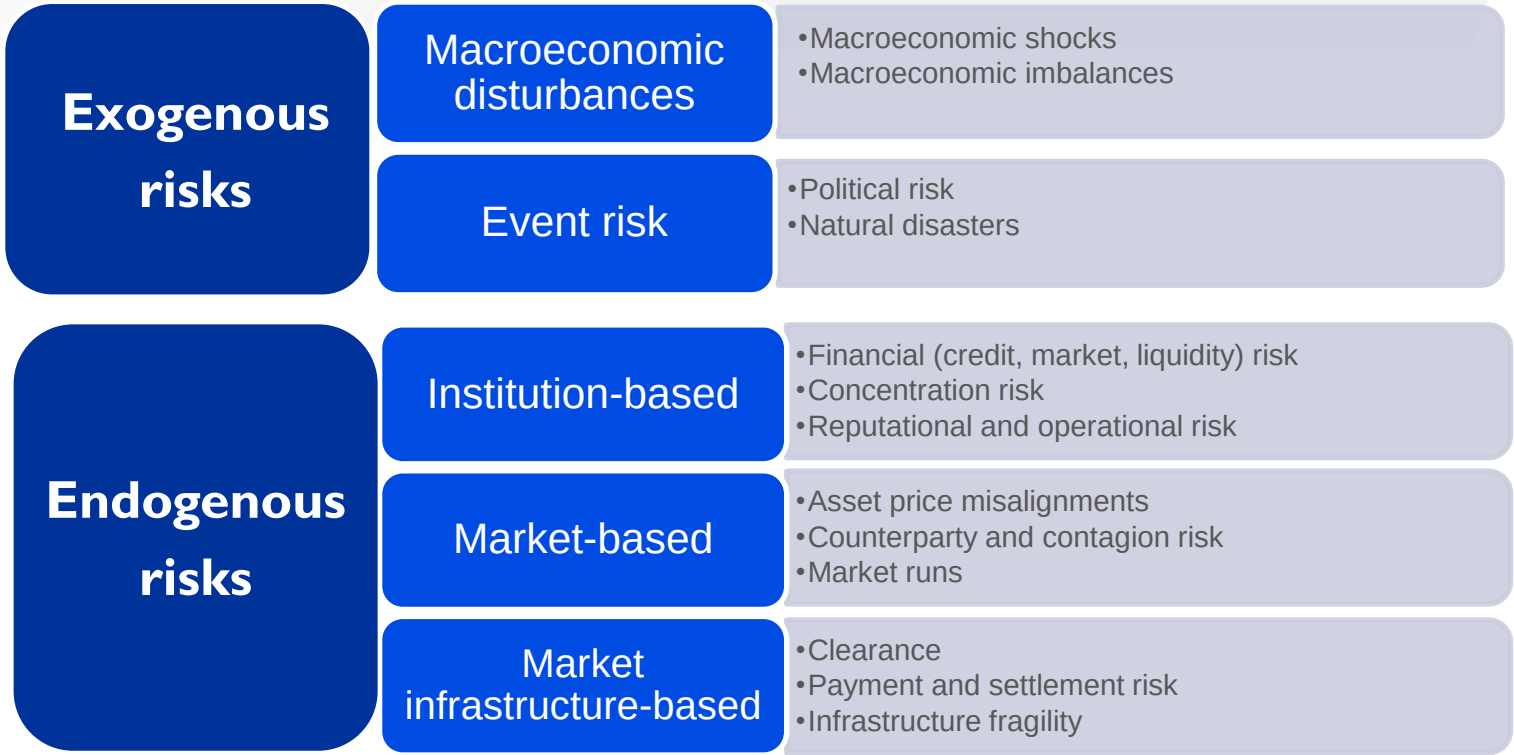
- … mainly idiosyncratic or could they be systemic?
- … random or are there identifiable systematic drivers?
- … best addressed by micro- or macroprudential supervision?

Overview

1. A central banker’s perspective
2. Gauging the threat landscape, potential drivers and costs
3. Macroprudential policy implications
4. Concluding remarks

Overview

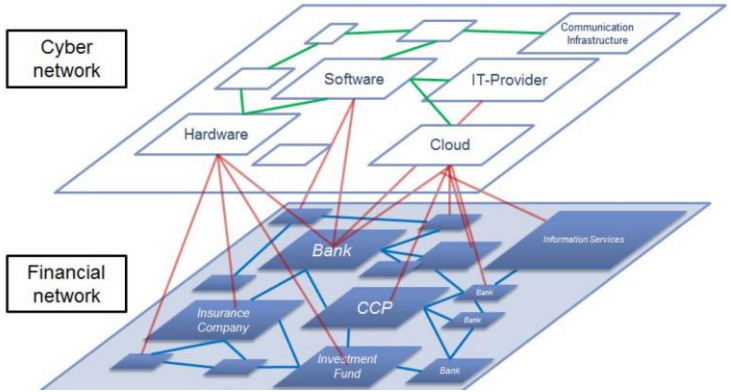
Sources of risk to financial stability



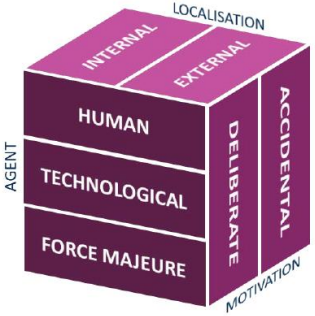
Note: based on Fell and Schinasi (2005).

How cyber risk could matter for financial stability

- Reliance on **digitalization** is increasing, also within the financial system…
- … which gives rise to complex, multi-layered **interconnections** between the financial system, cyber networks/information and communication technology, and the real economy



Source: ESRB (2022)



Source: Ros (2020)

- Where, who, why …
  - Many potential sources of cyber threats
  - Conducting of deliberate cyber attacks has become easier and cheaper over time

Real economy

(Inter)governmental bodies
- Disruption of governmental services
- Disruption of oversight functions

Non-financial corporations
- Ransom, theft, espionage
- Disruption of corporate services/operations

Individuals/households
- Theft/fraud (exploitive)
- Disruption of financial services
- Loss of confidence (potentially disruptive)

Physical infrastructures
- Large scale outages
- Disruption of supply chains

Investment/pension funds
- Operational impairments
- Theft/fraud (exploitive)

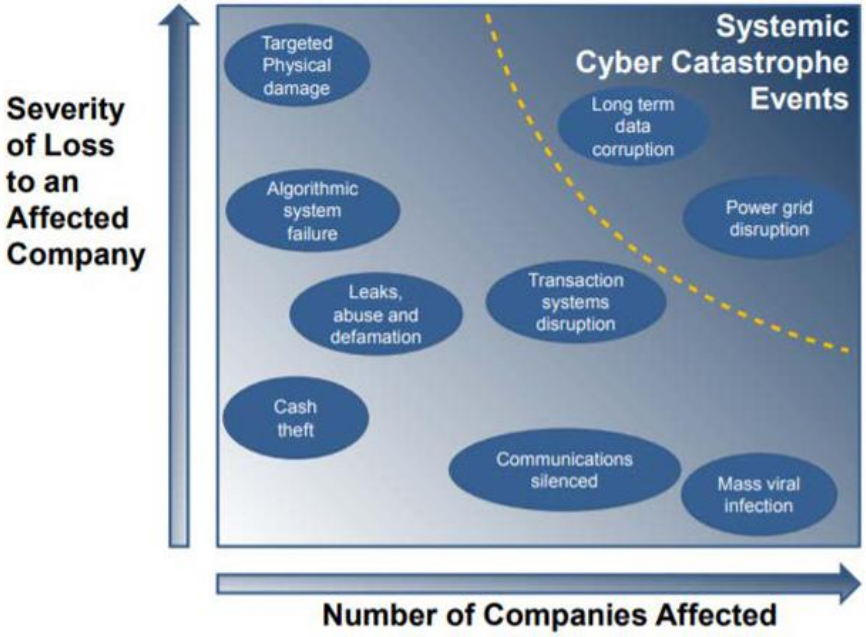
Financial infrastructures
- Disruption in market functioning
- Loss of information (disruptive)

Banks
- Theft (exploitive)
- Operational impairments, loss of information (disruptive)

Insurance corporations
- Operational impairments
- Losses from insured incidents

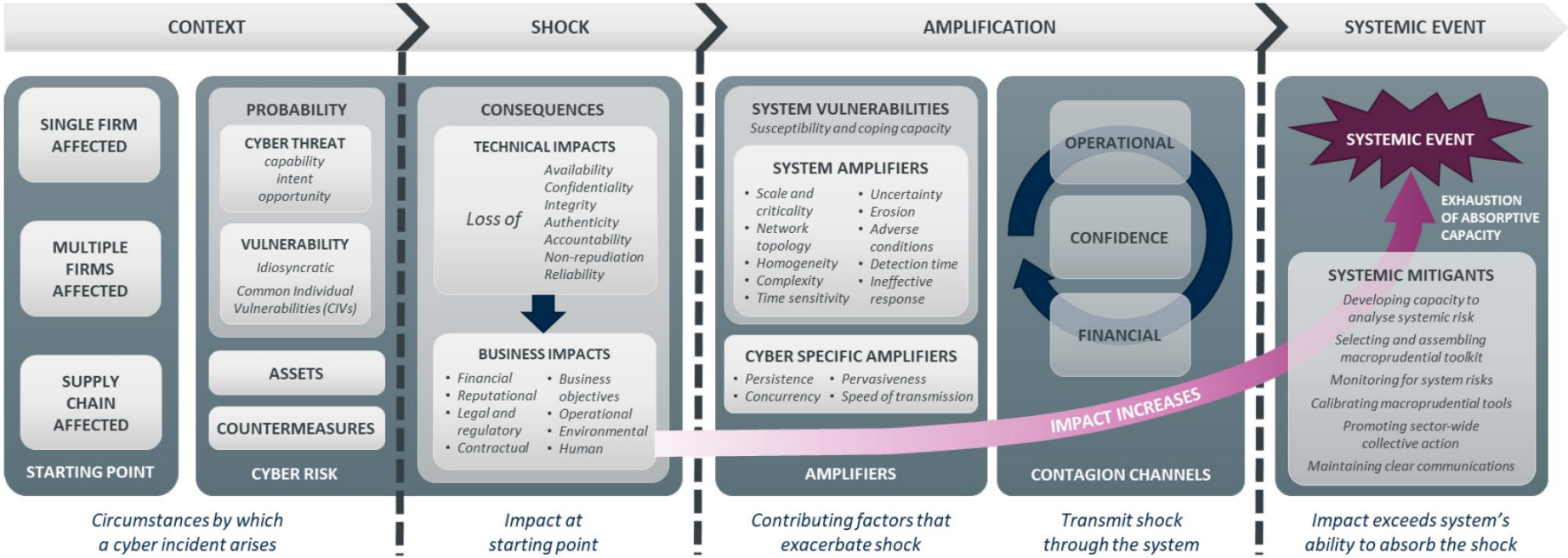
Financial system

What aspects should central banks care about?



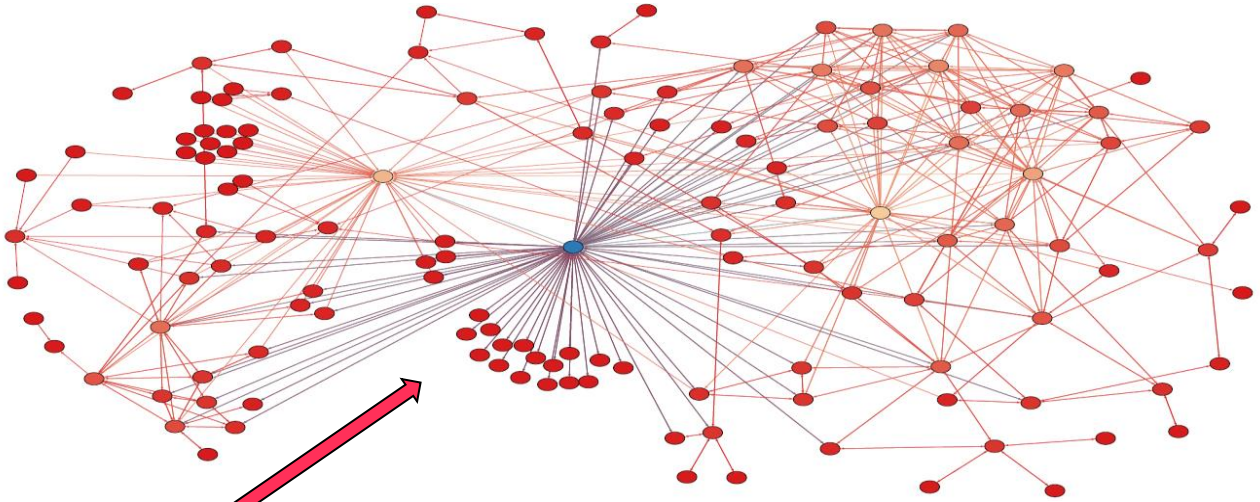
"Cyber incidents, including cyberattacks, could pose a systemic risk to the financial system given their potential to disrupt critical financial services and operations and thereby impair the provision of key economic functions", Mitigating Systemic Cyber risk, January 2022 ESRB

How can cyber incidents become systemic threats to financial stability?



Sources: ESRB (2020).

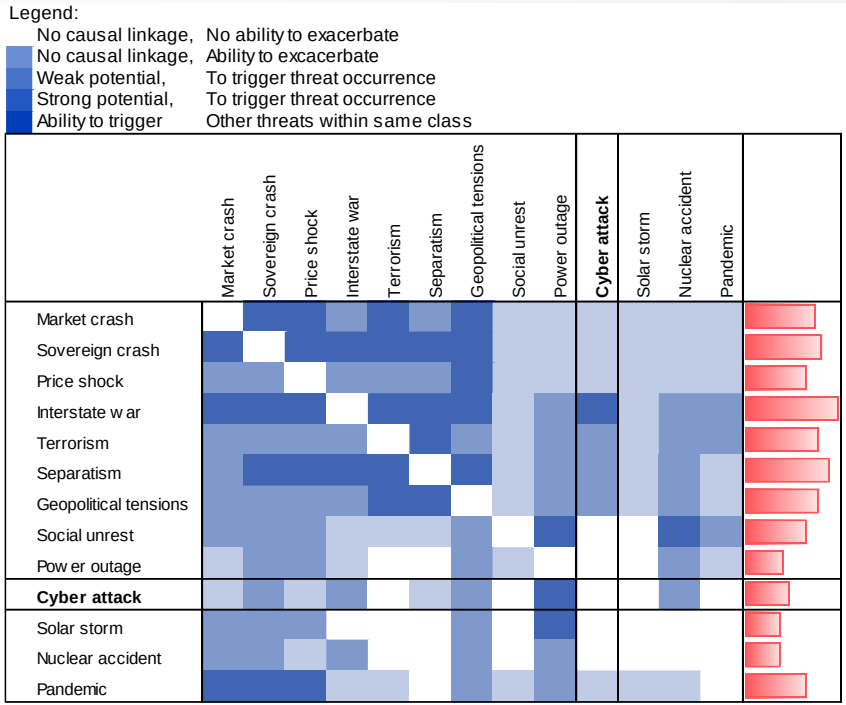
Interdependencies have important implications for the safety and efficiency of the financial ecosystem



This is real

High systemic risk potential of cyber risks

Systemic threat correlation matrix



- There is no uniform view of the link between cyber and systemic risks:
  - Some assume a direct link whereas others imply a connection
- A cyber attack can cascade into other (potentially) systemic threats depending on:

1. Substitutability
2. Risk correlation
3. Interconnectedness

Sources: ECB and Cambridge Centre for Risk Studies.

Note: The correlation matrix summarises the risk of one threat cascading into another. Each threat type has been systematically explored to identify the initiating trigger events that cause loss over the chosen threshold, to ensure that 'correlation' – the likelihood of multiple locations being impacted in the same event – is well represented. For instance, materialisation of one threat which then triggers subsequent threat events in a cascade of escalating consequences. Examples include a war provoking a sovereign crisis, or a natural catastrophe causing a power outage which causes social unrest. See Cambridge Global Risk Index, 2017. Red bars sum the intensity (from 1-4) of the links with other potential threats.

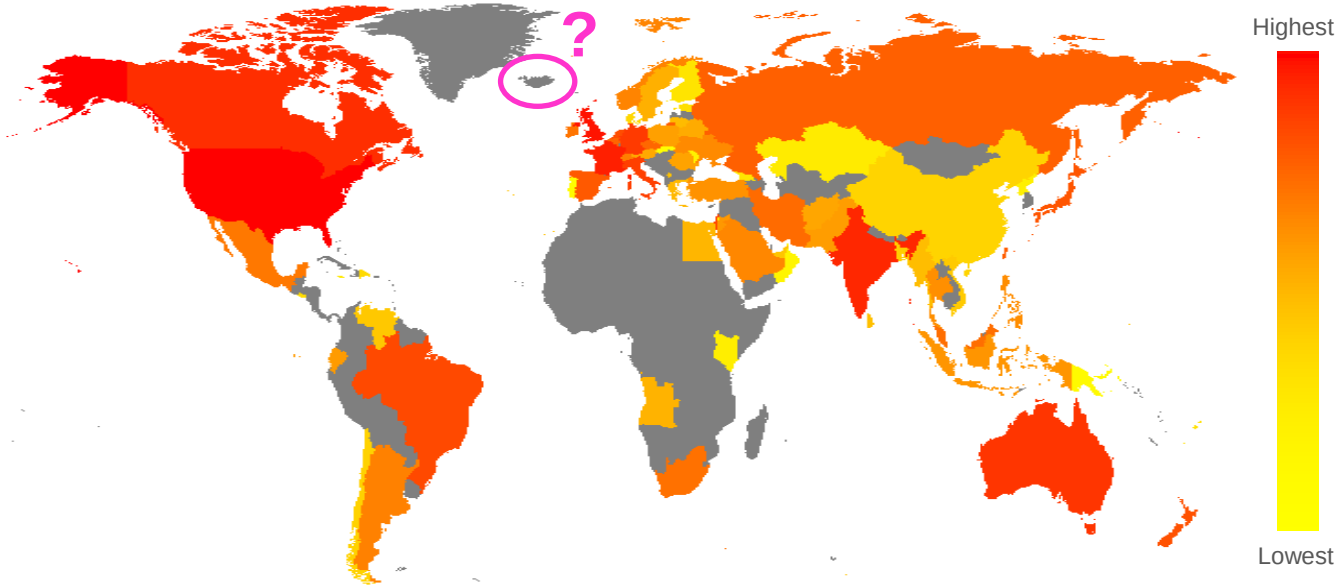
Overview

1. A central banker’s perspective
2. **Gauging the threat landscape, potential drivers and costs**
3. Macroprudential policy implications
4. Concluding remarks

Global cyber threat landscape

- Recorded cyber attacks are highly concentrated in a few large advanced and emerging economies

Global cyber attacks
Ranking, 2021

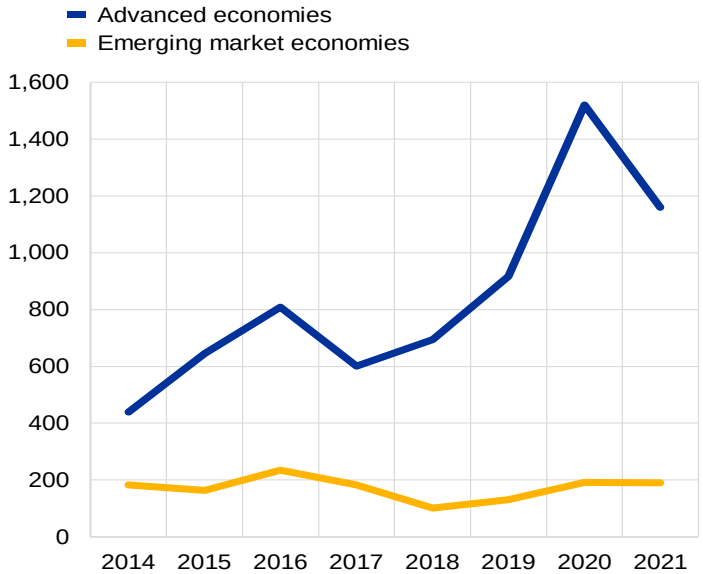


Sources: University of Maryland CISSM Cyber Attacks Database.
Note: The CISSM Cyber Attacks Database brings together open-source information surrounding a range of publicly-acknowledged cyber events on private and public sector organizations. It covers English language sources and contains around 9000 cyber attacks between 2014 and 2022 globally.

Structural drivers: Cyber attacks by stage of economic development

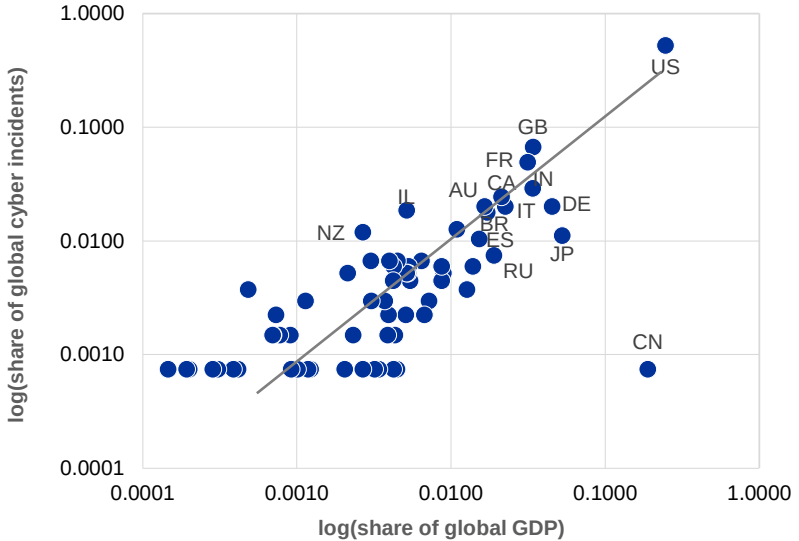
- Reports of cyber attacks appear to be more frequent in advanced economies
- Stage of economic development seems more relevant than economic importance

Cyber attacks in AEs and EMEs
2014-2021, number



Sources: University of Maryland CISSM Cyber Attacks Database.

Cyber incidents and economic importance
2021, log-scales

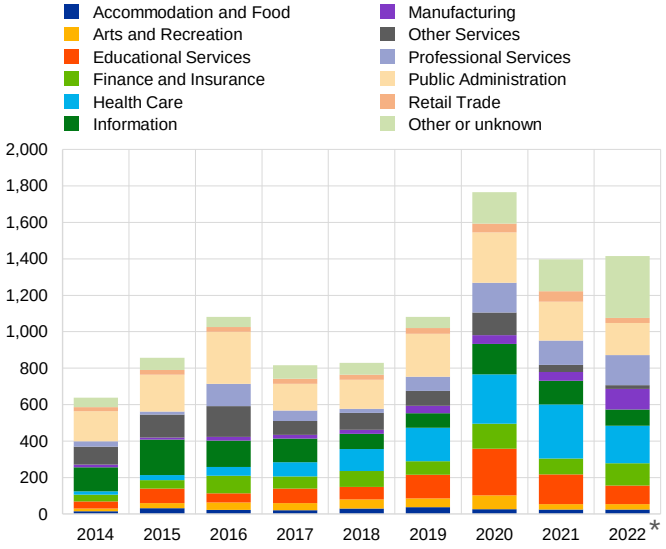


Sources: University of Maryland CISSM Cyber Attacks Database, IMF and ECB calculations.

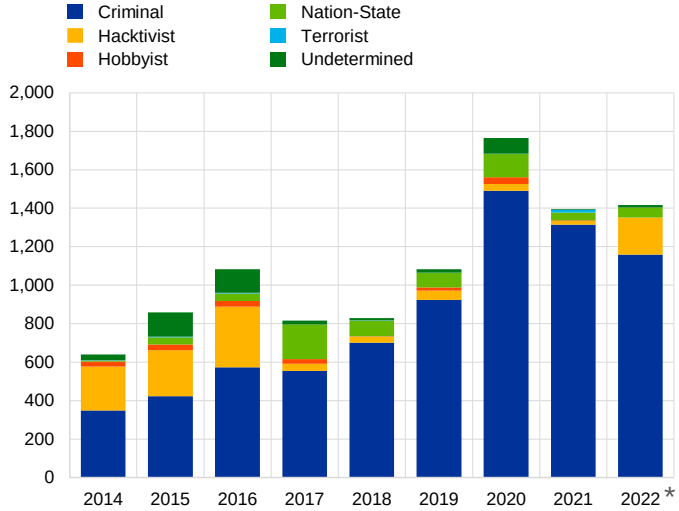
Structural drivers: the financial sector is not the prime target of cyber attacks

- Around 5-10% of cyber attacks are targeted at the financial sector
- Cyber attacks attributed to criminals are predominant

Global cyber attacks by economic sector
2014-2022, number



Global cyber attacks by perpetrator type
2014-2022, number

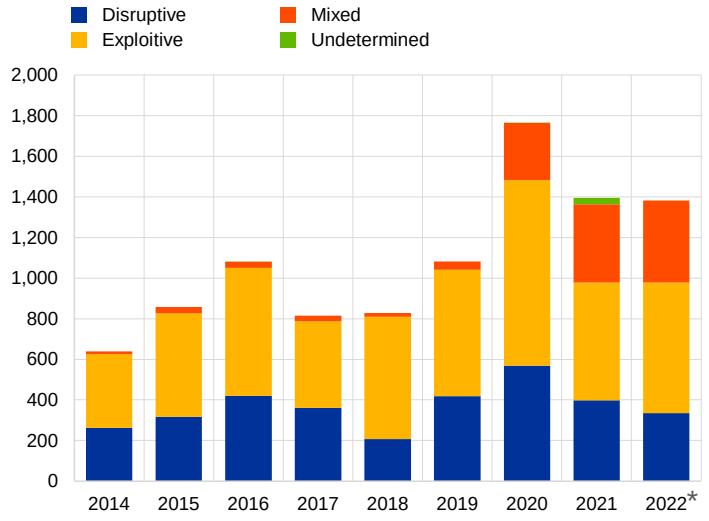


Sources: University of Maryland CISSM Cyber Attacks Database.
Notes: *2022 figures are annualised based on data available until July 2022.

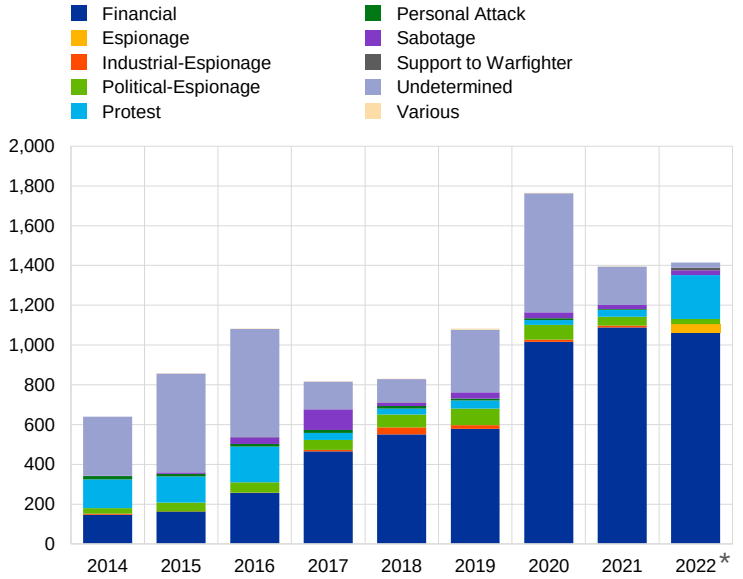
Structural drivers: most cyber attacks are exploitative, with financial motives

- Around 70% of cyber attacks are exploitive and 30% are disruptive
- Financial motives are dominant, but protests, espionage and sabotage also play a role

Global cyber attacks by event type
2014-2022, number



Global cyber attacks by motive
2014-2022, number

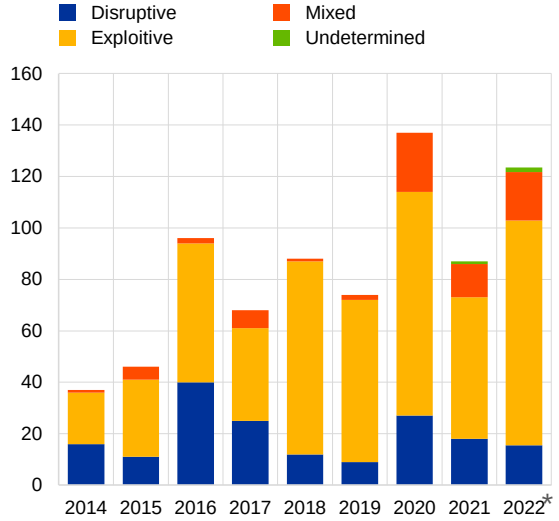


Source: University of Maryland CISSM Cyber Attacks Database.
Notes: *2022 figures are annualised based on data available until July 2022.

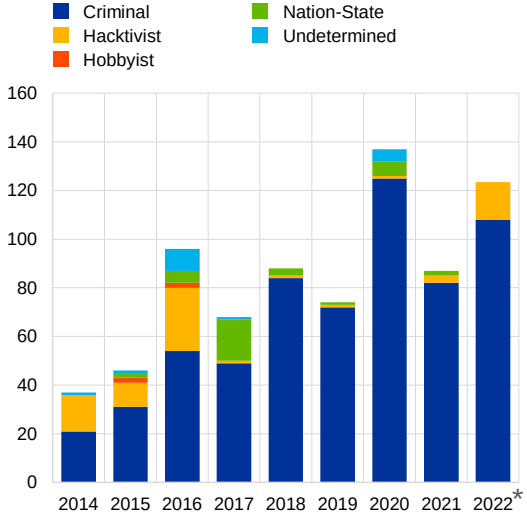
Structural drivers: Cyber attacks on the financial sector are mostly exploitative

- The majority of cyber attacks on the financial sector are exploitive and carried out by criminals
- Cyber attacks are mostly driven by financial motives, but protests by hacktivists have also played a role

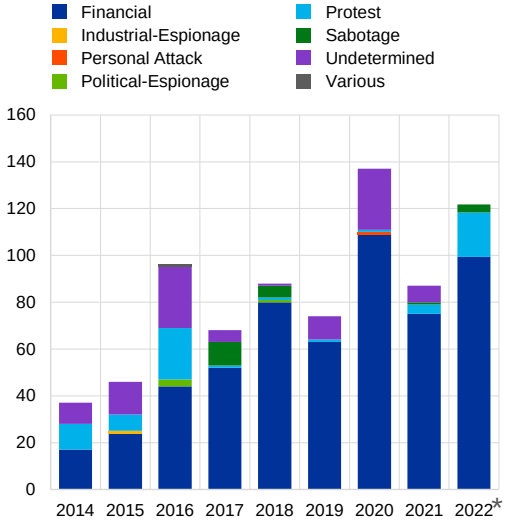
Cyber attacks on financial sector by event type
2014-2022, number



Cyber attacks on financial sector by perpetrator type
2014-2022, number



Cyber attacks on financial sector by motive
2014-2022, number

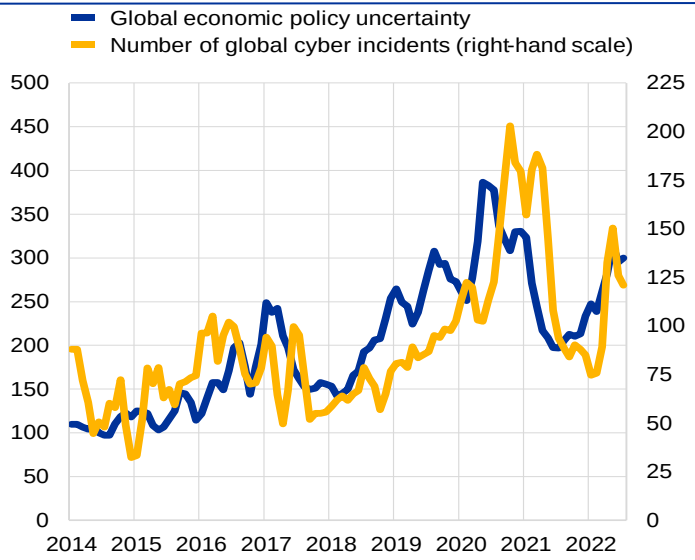


Sources: University of Maryland CISSM Cyber Attacks Database.
Notes: *2022 figures are annualised based on data available until July 2022.

Cyclical drivers: Cyber threats coincide with economic and political cycles

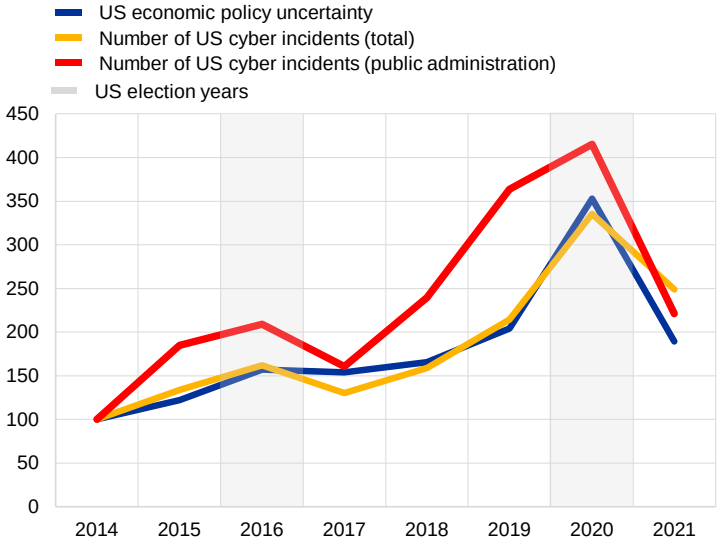
- Cyber activity seems to be driven by similar forces as political and economic policy uncertainty
- Electoral cycles seem to play a role, with more cyber attacks on public administration ahead of elections

Global economic policy uncertainty and number of global cyber incidents
Jan. 2014 – Jul. 2022, index, number



Sources: www.policyuncertainty.com and University of Maryland CISSM Cyber Attacks Database.

US economic policy uncertainty and number of cyber incidents
2014 – 2021, index: 2014=100

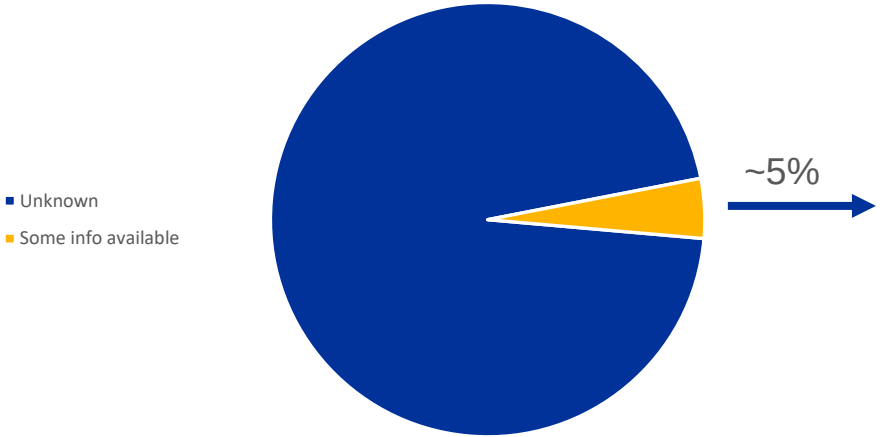


Sources: www.policyuncertainty.com and University of Maryland CISSM Cyber Attacks Database.

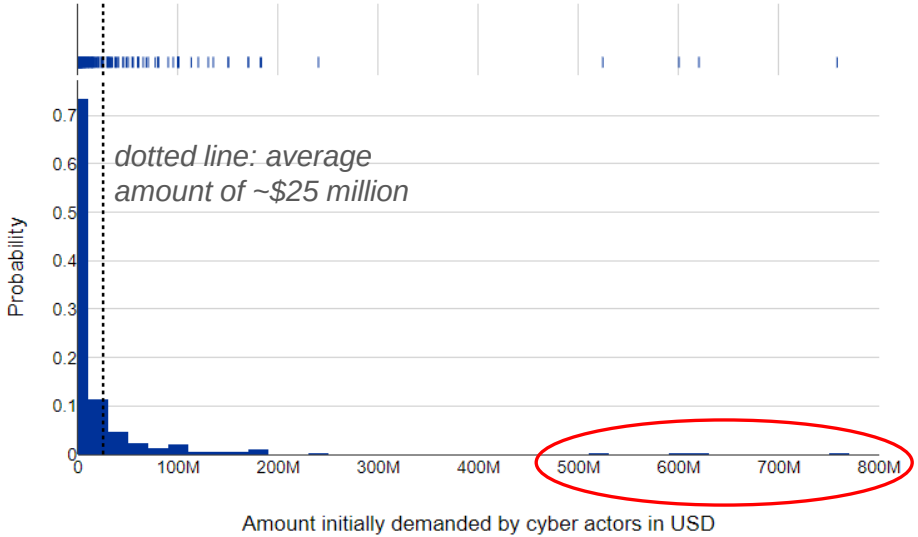
Implications: Little is known about amounts demanded by cyber perpetrators

- For most cyber incidents, no information is available on amounts demanded by cyber perpetrators
- Based on the scarce information available, the average amount initially demanded by cyber perpetrators appears moderate (~$25 million) but amounts have been large in some cases

Amounts demanded by cyber perpetrators
2014-2022, percentage



Distribution of amount demanded by cyber perpetrators
2014-2022, USD, probability

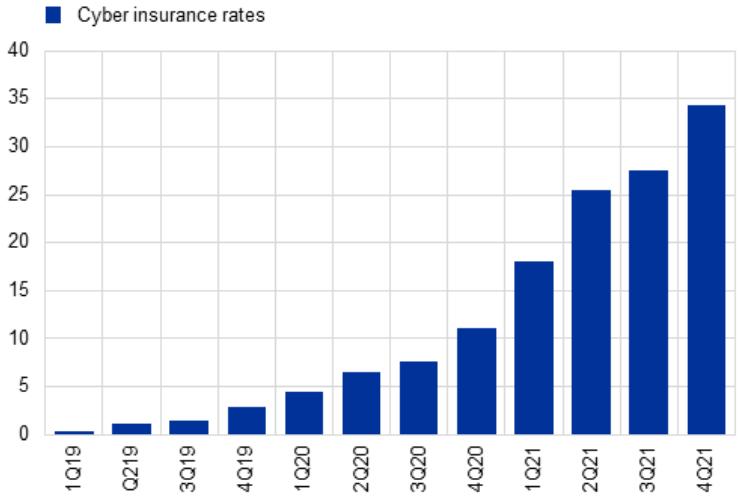


Source: University of Maryland CISSM Cyber Attacks Database.
Notes: Chart shows that ~400 out of ~9000 cyber incidents covered in the CISSM database include information on amounts initially demanded by cyber actors.

Implications: Indirect costs are rising

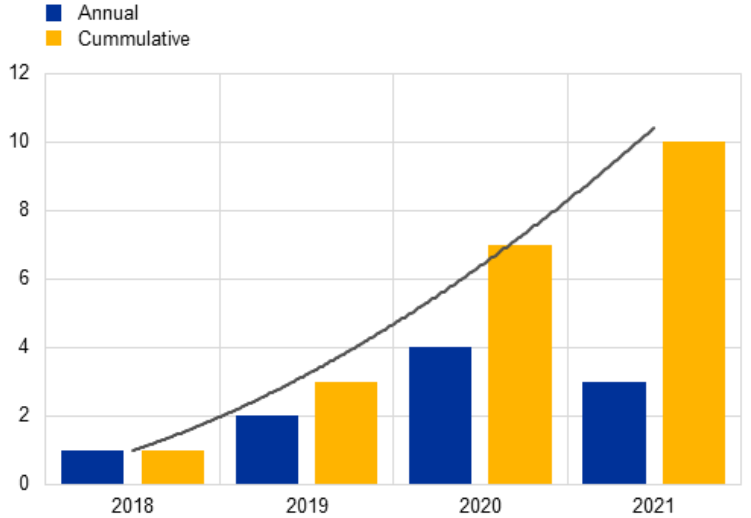
- Cyber insurance costs have been rising, and non-financial firms' funding costs may be adversely affected by credit rating downgrades (via ESG scores)

Cyber insurance renewal premium rates
Q1 2019-Q4 2021, q-o-q change in percent



Source: Fitch ratings.

Negative rating actions for NFC's where cyber incidents played a role
2018-2021, number



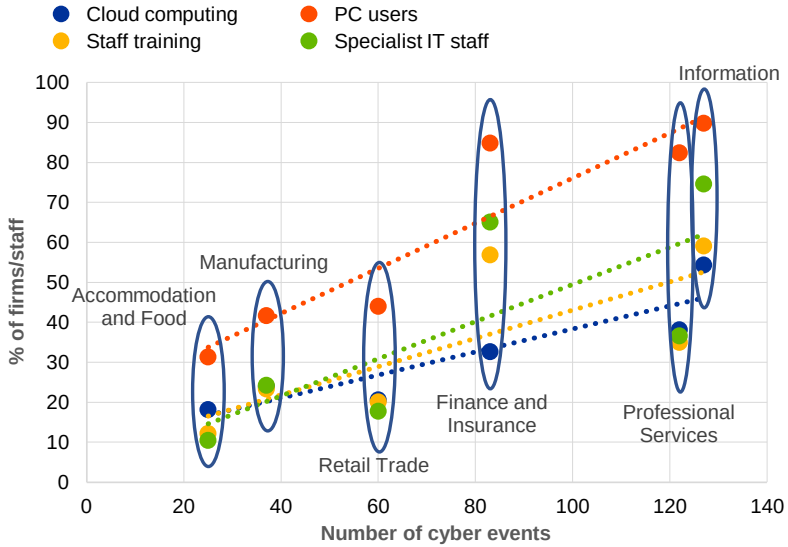
Source: S&P Global.

Overview

Mitigants of cyber risks

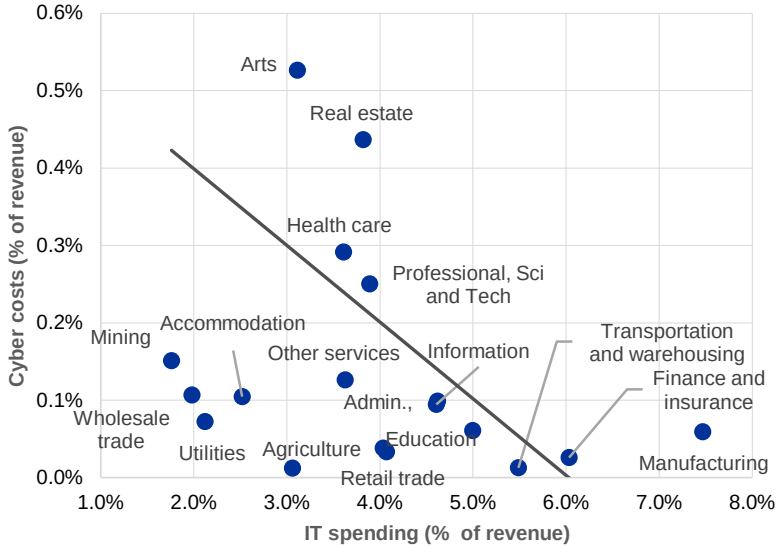
- Sectors with higher rates of digitalisation are more prone to cyber attacks
- Higher frequency of attacks does not necessarily translate into higher losses
- Recent studies find IT spending can effectively mitigate cyber costs

Number of cyber incidents by digitalisation rates
2020, percentages, number of events



Sources: BIS, University of Maryland CISSM Cyber Attacks Database.
Note: Cloud computing: % of firms that have purchased cloud computing services. PC users: % of staff that use a computer in their everyday work. Staff training: % of firms that gives staff a specific IT training. Specialist IT staff: % of firms that employ staff specialized in IT.

Cost of cyber attacks and IT spending by sector
2020, percentage of revenue



Sources: BIS, ECB.
Note: based on Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, 60, 100989.

Policy response: Cyber resilience work of international fora

- **G7 Cyber Expert Group (CEG)** - working on a variety of cybersecurity topics such as Third party risk, Ransomware, Crisis exercising. The G7 CEG has issued “Fundamental Elements” on how to assess cybersecurity in the financial sector, Threat Led Penetration Testing, Third party risk and Cyber Exercise Programs.

- **Financial Stability Board** - working on enhancing the Cyber Lexicon, Third party risk, Cyber incident response and recovery toolkit.

- **Basel Committee on Banking Supervision** - monitoring and assessing developments in banks' cyber risk management and resilience to help safeguard the confidentiality, integrity and availability of banks' systems and data in the face of cyber threats.

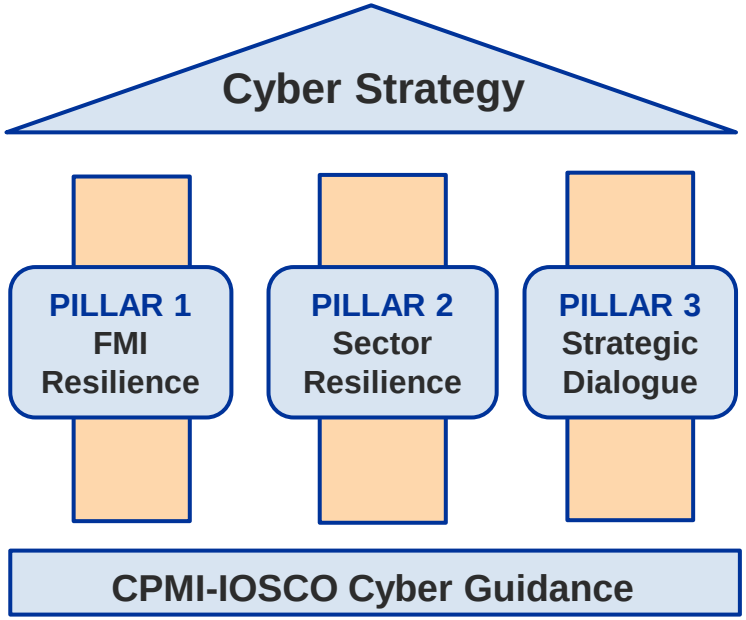
- **Committee on Payments and Market Infrastructures** - working on operational and cyber resilience: 2016 “Cyber Resilience Guidelines for FMIs”

Policy response: Cyber resilience work of European fora

European Systemic Cyber Group

- Working on establishing a pan-European systemic cyber incident coordination framework (EU-SCICF) to mitigate the risk of a coordination failure.
- Providing guidance for cyber resilience scenario stress testing as a tool to assess the impact of a cyber incident and analyse its potential amplification into a systemic event both for institutions and system wide
- Quantifying the maximum acceptable level of disruption to critical economic functions that does not pose a risk to financial stability in severe, or even extreme, but still plausible scenarios
- Identifying macroprudential tools that may mitigate the effect of a systemic cyber incident

Policy response: Eurosystem Cyber resilience strategy for Financial Market Infrastructures (2017)



The **Eurosystem strategy** for ensuring the cyber resilience of the financial ecosystem

Rolled out: 2017 – 2022
Eurosystem and national level

Overview

Conclusions

- Returning to the three initial questions: (1) cyber events could indeed pose systemic risks, and; (2) may not be random, but; (3) the existing macroprudential policy toolkit has limited capacity to address the risks

- Macroprudential authorities can still invest in monitoring frameworks – including early warning tools – and system-wide stress-testing to gauge resilience, identify vulnerabilities, and issue warnings

- Ensuring cyber resilience requires collaboration at both operational and policy levels, while also closing data gaps

EUROPEAN CENTRAL BANK

EUROSYSTEM

Background slides

Eurosystem Cyber resilience strategy for FMIs (2017)
Three Pillars

- **FMI Resilience**
  Strategic objective: Overseers to work with FMIs to enhance their cyber resilience to ensure their safety and soundness.
  Tools: Cyber resilience oversight expectations, European red team testing framework, cyber survey

- **Sector Resilience**
  Strategic objective: Enhance collective cyber resilience capability of the financial sector, through cross-border / cross-authority collaboration, information sharing and exercises.
  Tools: market wide cyber exercises, sector-mapping

- **Strategic Regulator – industry engagement**
  Strategic objective: Establish trust and collaboration amongst participants, catalyse joint initiatives to enhance sector capabilities and capacities, and increase cyber awareness
  Tools: Establishment of “Euro Cyber Resilience Board for pan-European FMIs”