

# Opening remarks

3rd Annual Nordic Cyber in Finance  
Conference, 28 November 2019

Stefan Ingves

Governor

# Rising operational risks for financial firms

- Digitalisation
- Interconnectedness and complexity
- Cyber risk



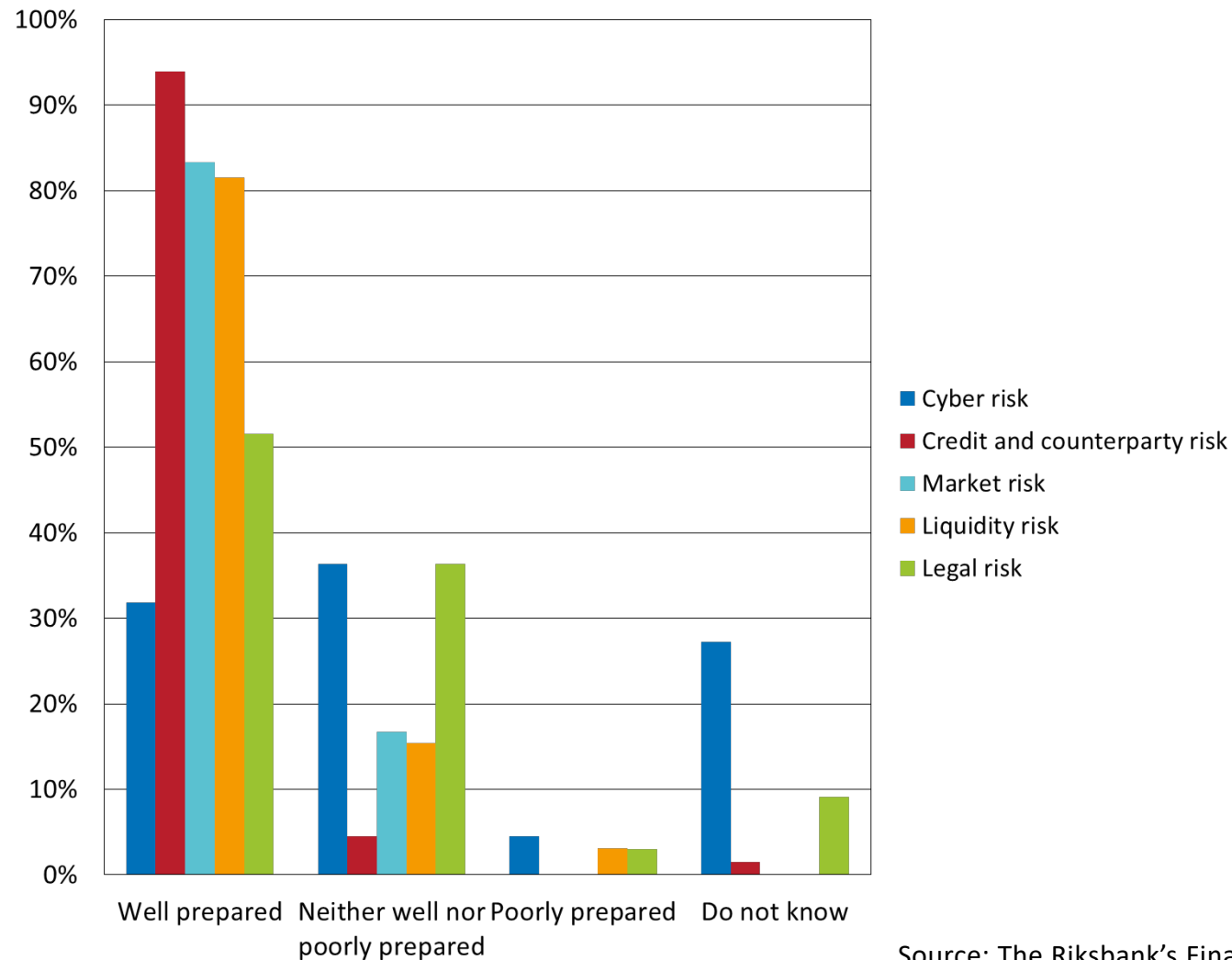
# Cyber risk poses new challenges

- Cyber attacks will be successful
- Cyber threats are both cross-sectoral and cross-border
- A potential systemic risk



# Resilience to cyber risks must be improved

“How prepared do you feel you are with regard to cyber risks?”



# Nordic cooperation

- Many pan-Nordic financial entities
- Threat actors cooperate
- Cooperation needs to be strengthened further



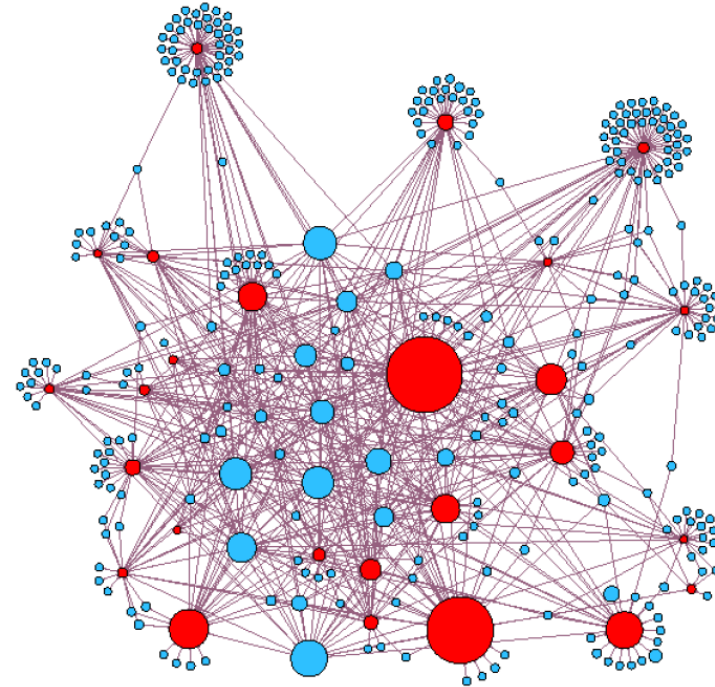
# A priority for the Riksbank

- Strengthened preparedness
- Improving our cyber resilience
- National and international cooperation



# Cyber resilience in the Swedish financial system

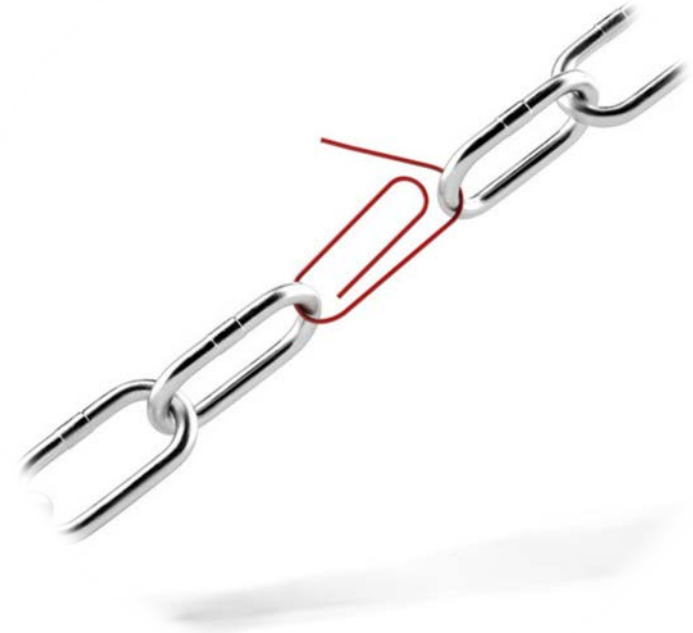
- The importance of cyber risk has increased in the financial stability analysis
- Important that the financial sector achieves a baseline resilience level



Source: Analysis of Central Clearing Interdependencies, August 2018.  
BIS, CPMI, FSB and IOSCO.

# The threat actors search for the weakest link

- The importance of endpoint security
- Know your customer's customer





# The Riksbank is coordinating TIBER-SE<sup>1</sup>

- Tests resilience in a standardised manner
- The Riksbank has a driving and coordinating role
- External suppliers used to carry out the actual tests



## TIBER-EU FRAMEWORK

How to implement the  
European framework for Threat  
Intelligence-based Ethical  
Red Teaming

May 2018

1. TIBER is short for Threat-Intelligence-based Ethical Red Teaming.

# Way forward

## Two key questions:

- How should organisations be governed to address cyber risk?
- What should we do in practice?



**Thank you!**