Some Principles for Regulating Cyber Risk

Anil Kashyap and Anne Wetherilt*

Atlanta, 6 January 2019

* All views here are our own and do not necessarily reflect the views of the Bank of England or the Financial Policy Committee.
Outline

1. What is special about cyber?
   – The shock
   – Its impact

2. Why is regulation needed?
   – Microprudential policy
   – Macroprudential policy

3. Regulatory principles and microprudential policy

4. Regulatory principles and macroprudential policy

Kashyap and Wetherilt (2019)
1. What is special about cyber?

- Cyber shocks are different:
  - Intent – maximum damage
  - Probability – success of a high impact attack is inevitable
  - Timing – hidden phase
  - Adaptability – declining costs of attack, rising costs of defence

- Cyber impact is unique:
  - Scale – can damage a large part of the system
  - Hidden damage – difficult to know what is compromised or when it was compromised, complicates recovery

Kashyap and Wetherilt (2019)
2. Why is regulation needed?

• Firms and society may have different risk tolerances because
  
  i. Firms may not prioritize protecting against **systemic** shocks over **idiosyncratic** ones
  
  ii. Firms may not have incentives to avoid shared exposures
  
  iii. Firms plan for idiosyncratic attacks ➔ assume external resources will be available
  
  iv. Firms’ incentives to share information with other firms and with regulators may be limited

Kashyap and Wetherilt (2019)
3. Regulatory principles: microprudential policy

1. Assume successful attack is inevitable and, plan for recovery
   - Firms need to identify critical systems and processes

2. Insist that firms have plans for systemic attacks
   - Firms need to plan for wide range of scenarios/external resource constraints

3. Aim for a two-way supervisory dialogue about appropriate recovery times
   - Firms need to internalize social concerns

Kashyap and Wetherilt (2019)
4. Regulatory principles: macroprudential policy

4. Conduct cyber stress tests that explore common vulnerabilities
   - Consider risks from common infrastructure, software, shared services etc.

5. Plan for system-wide disruption by setting appropriate recovery expectations for the delivery of critical economic functions.
   - Focus on the delivery of critical economic functions

Kashyap and Wetherilt (2019)
4. Regulatory principles: macroprudential policy (ctd)

6. Encourage firms to avoid common vulnerabilities and to make more diverse infrastructure or software choices
   - Regulators cannot control prices to affect these incentives
   - They can ‘tax’ by designing stress tests that link severity of the test to the degree of concentration that is present

Kashyap and Wetherilt (2019)
Concluding thoughts

• Cyber continue to present a challenge, despite significant investments by firms (individually & collectively)

• Preventing all attacks is prohibitively expensive ➔ focus on recovery

• How do we reconcile the preference for fast recovery with complications from hidden attacks?

Kashyap and Wetherilt (2019)