Panel #3: The Role of the Federal Reserve System

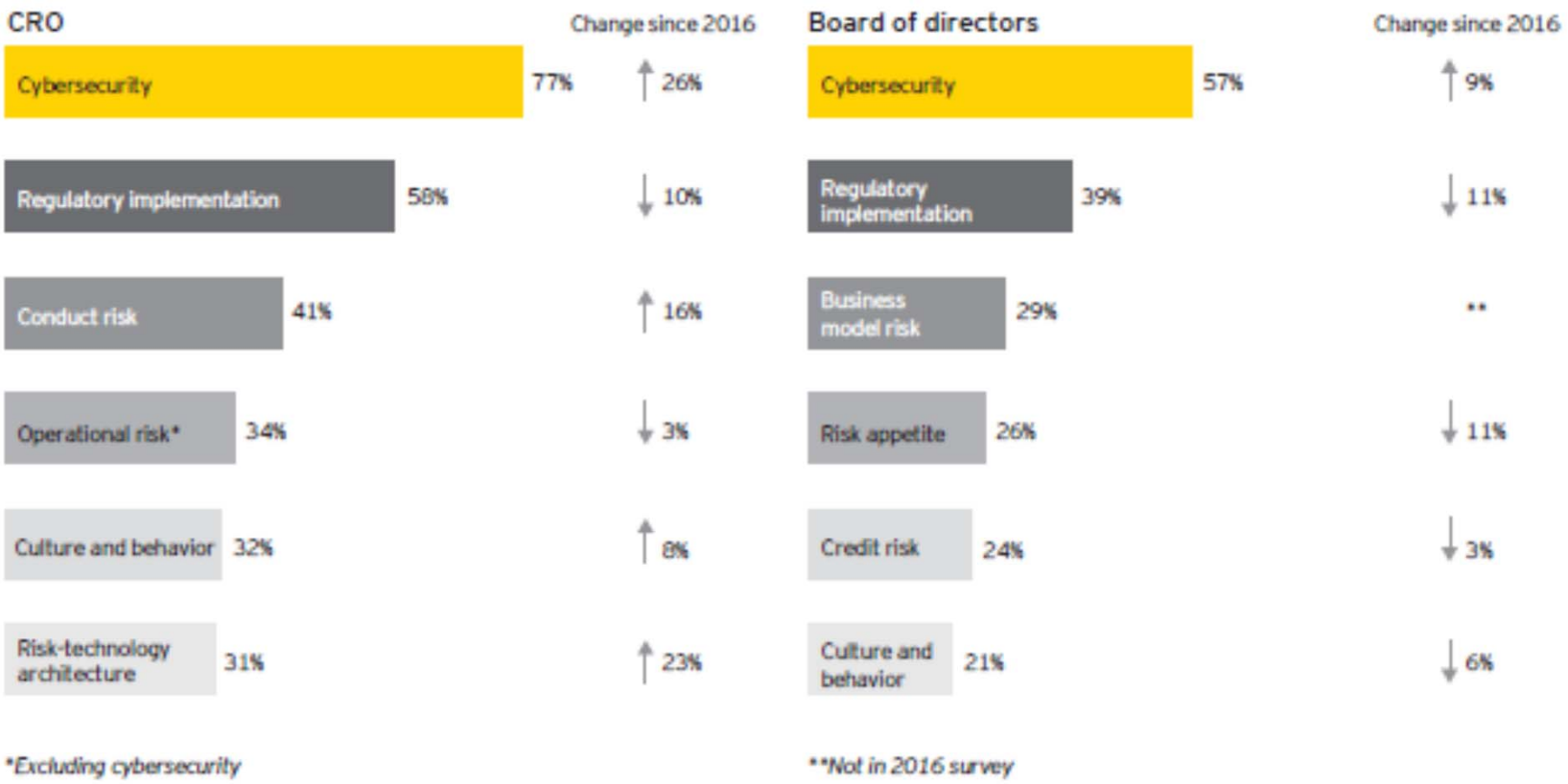
- **René Stulz**, *Everett D. Reese Chair of Banking and Monetary Economics, The Ohio State University*
- **Todd Vermilyea**, *Senior Associate Director, Risk & Surveillance, Board of Governors of the Federal Reserve System*
- **Keith Gordon**, *Chief Information Security Officer, Ally*
- **Nida Davis**, *Associate Director, Systems and Operational Resiliency Policy, Board of Governors of the Federal Reserve System*
- **Gara Afonso**, *Assistant Vice President, Financial Intermediation, Federal Reserve Bank of New York*

Cyber risk and the Federal Reserve System

René M. Stulz

The Ohio State University and NBER

Figure 1: Top-of-mind risks for CROs and boards



E&Y Survey, 2018

Issues

- Focus is on systemic risk
- Different types of cyber risks have different implications for systemic risk
- Bank-level versus interbank risks
- Network issues
- Concentrating risks in the cloud
- Bank supervision is not enough

Types of risks

- Single-institution risks:
  - Risk of theft of personal data.
  - Risk of theft of assets.
  - Risk of operational disruption.
- Multi-institution risks:
  - Disruption in financial plumbing.
  - Disruption in facilities used by multiple institutions.

Impact of successful cyberattacks (Part I)

- Looked at sample including financial and non-financial involving personal data theft.
- Good sample because of reporting requirement.
- From 2005 to 2017, 307 successful attacks against Compustat firms; 23.45% in finance industry.
- Targeted firms are more successful.
- Finance is actually less likely to be targeted.
- Firms with board risk committee are less likely to be targeted.

Impact of successful cyberattacks (Part II)

- Stock-price impact: 1.1% with financial information loss.
- Impact on financial firms: Not different.
- Sources of impact:
  - Out-of-pocket costs are small compared to impact
  - Most of impact is reputation loss
  - Sales growth drops for retail firms
  - Reputation loss is negatively related to risk management

Systemic risk of single-institution attacks

- For almost all financial institutions , single institution attacks do not create a systemic risk.
- Successful attacks are costly for institutions, so they have strong incentives to manage their risk.

Largest institutions

- A short-lived localized attack on a large bank is unlikely to be a systemic event even if it affects the ability of the bank to make some payments.
- Many types of attacks on the largest institutions do not create systemic risk – for instance, stealing personnel records.
- An attack that seriously disrupts the operations of one of the largest institution in a way that prevents it to make the payments that are due across the institution would be a systemic event.
- Such an attack could have dramatic knock-on effects as other institutions have to cope with not receiving expected payments.
- Would be worse than Lehman.

Risk management

- Attention should be paid to how cyber risks are treated
  - What is the role of the board?
  - What is the role of the CRO?
  - How are the risks assessed?
  - Who owns the risks?
  - Are supplier risks assessed?
  - Is there a risk appetite statement for cyber risks?

Role of Fed and supervisors

- Supervisors can assess cyber risk at the institution level.
  - Cyber risk reverse stress tests.
  - The key question is: What does it take to immobilize the institution?
- The infrastructure of the financial system is exposed to cyber risks in a way that is beyond purview of bank supervisors.
- Those cyber risks should be assessed and monitored by the Federal Reserve System because they are a source of systemic risk.
- These risks are likely to be a bigger source of systemic risk than a bank's market risk.

Network effects

- There are constant transfers of funds and data from banks to other banks and clients.
- These transfers can be interrupted by attacks when they are between institutions.
- Such interruptions can create systemic risks as they can prevent the financial system from functioning normally.

Common suppliers

- Many financial institutions use the same suppliers for critical parts of their operations.
- Attacks can come from suppliers.
- Attacks on suppliers can have a systemic impact as they can affect the operations of all the banks that use these suppliers.
- The official sector should develop a program to identify suppliers that are systemic and assess the extent to which they are vulnerable.
- An obvious example is the cloud.

Why focus on risks outside of institutions?

- These risks are critical for the functioning of the financial system.
- During the crisis, the weaknesses of the plumbing of the financial system were exposed and worsened the crisis. They were close to failing.
- Same could happen with cyber. Would be much better to prevent than cope ex post.

Conclusion

- Cyber risk can create systemic risk.
- It could do so by disabling one of the largest institutions.
- It could do so by disabling the way financial institutions interact with one another and with their clients and hence by crippling the financial system.
- It could do so by attacking common suppliers.
- Regulation and monitoring of cyber risk concerning the plumbing of the financial system understood broadly and critical service providers should be part of the mandate of the Fed given its systemic risk implications.

Panel #3: The Role of the Federal Reserve System

- **René Stulz**, *Everett D. Reese Chair of Banking and Monetary Economics, The Ohio State University*
- **Todd Vermilyea**, *Senior Associate Director, Risk & Surveillance, Board of Governors of the Federal Reserve System*
- **Keith Gordon**, *Chief Information Security Officer, Ally*
- **Nida Davis**, *Associate Director, Systems and Operational Resiliency Policy, Board of Governors of the Federal Reserve System*
- **Gara Afonso**, *Assistant Vice President, Financial Intermediation, Federal Reserve Bank of New York*

Todd Vermilyea

Senior Associate Director, Risk & Surveillance, Board of Governors of the Federal Reserve System

Panel #3: The Role of the Federal Reserve System

- **René Stulz**, *Everett D. Reese Chair of Banking and Monetary Economics, The Ohio State University*
- **Todd Vermilyea**, *Senior Associate Director, Risk & Surveillance, Board of Governors of the Federal Reserve System*
- **Keith Gordon**, *Chief Information Security Officer, Ally*
- **Nida Davis**, *Associate Director, Systems and Operational Resiliency Policy, Board of Governors of the Federal Reserve System*
- **Gara Afonso**, *Assistant Vice President, Financial Intermediation, Federal Reserve Bank of New York*

Keith Gordon

Chief Information Security Officer, ALLY

The role of the Federal Reserve System in Cyber Risk

- Providing horizontal perspectives to financial institutions
- Increasing visibility of cyber career path
- Provide consistency in the development of new cyber-based laws or regulations.

Panel #3: The Role of the Federal Reserve System

- **René Stulz**, *Everett D. Reese Chair of Banking and Monetary Economics, The Ohio State University*
- **Todd Vermilyea**, *Senior Associate Director, Risk & Surveillance, Board of Governors of the Federal Reserve System*
- **Keith Gordon**, *Chief Information Security Officer, Ally*
- **Nida Davis**, *Associate Director, Systems and Operational Resiliency Policy, Board of Governors of the Federal Reserve System*
- **Gara Afonso**, *Assistant Vice President, Financial Intermediation, Federal Reserve Bank of New York*

Nida Davis

Associate Director, Systems and Operational Resiliency Policy, Board of Governors of the Federal Reserve System

Discussion & Questions