

Trends in Determining Systemic Cyber Risk for the Financial Services Industry

Matt Tolbert

Federal Reserve Bank of Cleveland

Nonconfidential - External

***The views stated herein are those of the
presenter***

***and not necessarily those of the Federal
Reserve Bank of Cleveland***

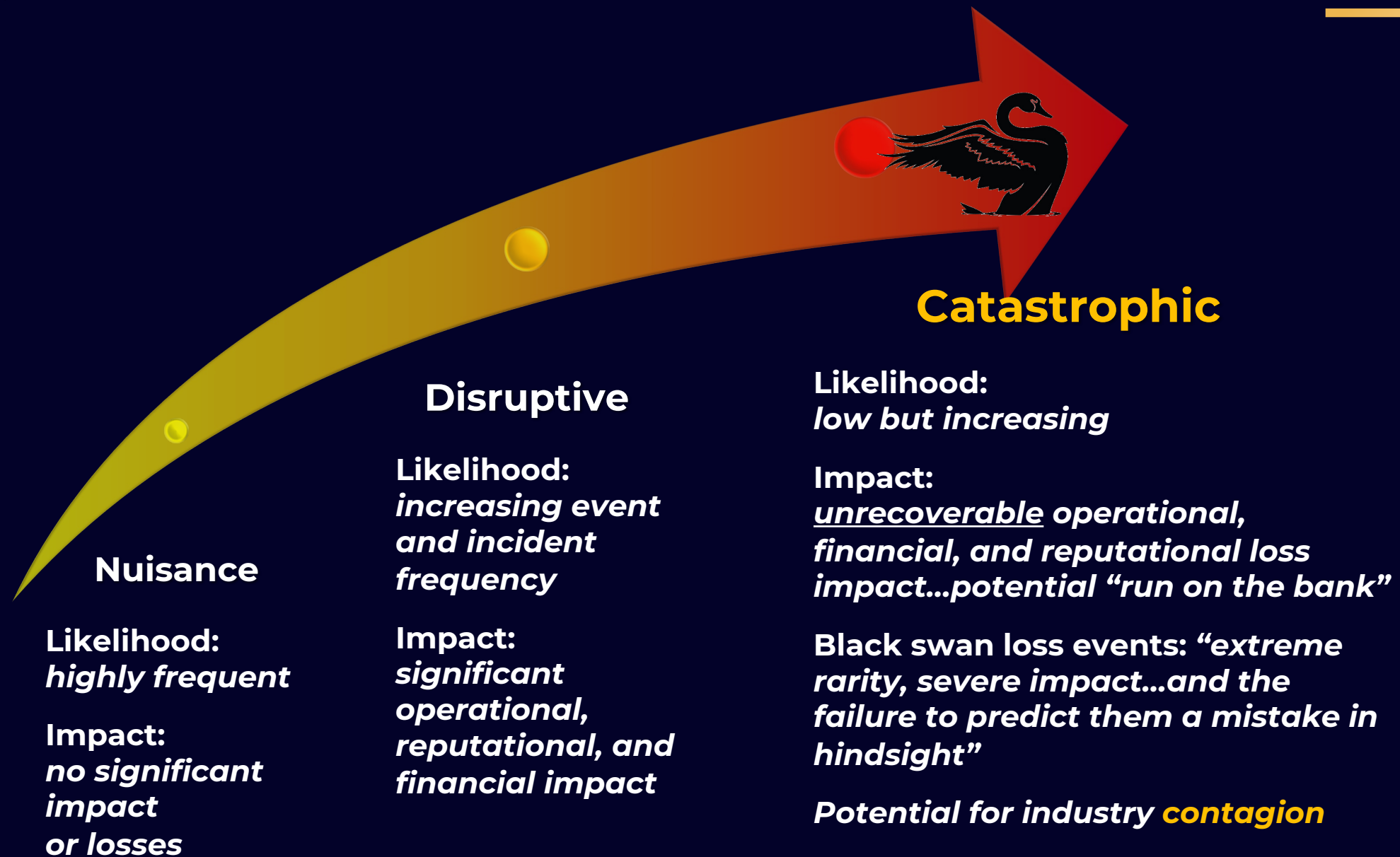
***or of the Board of Governors of the Federal
Reserve System.***

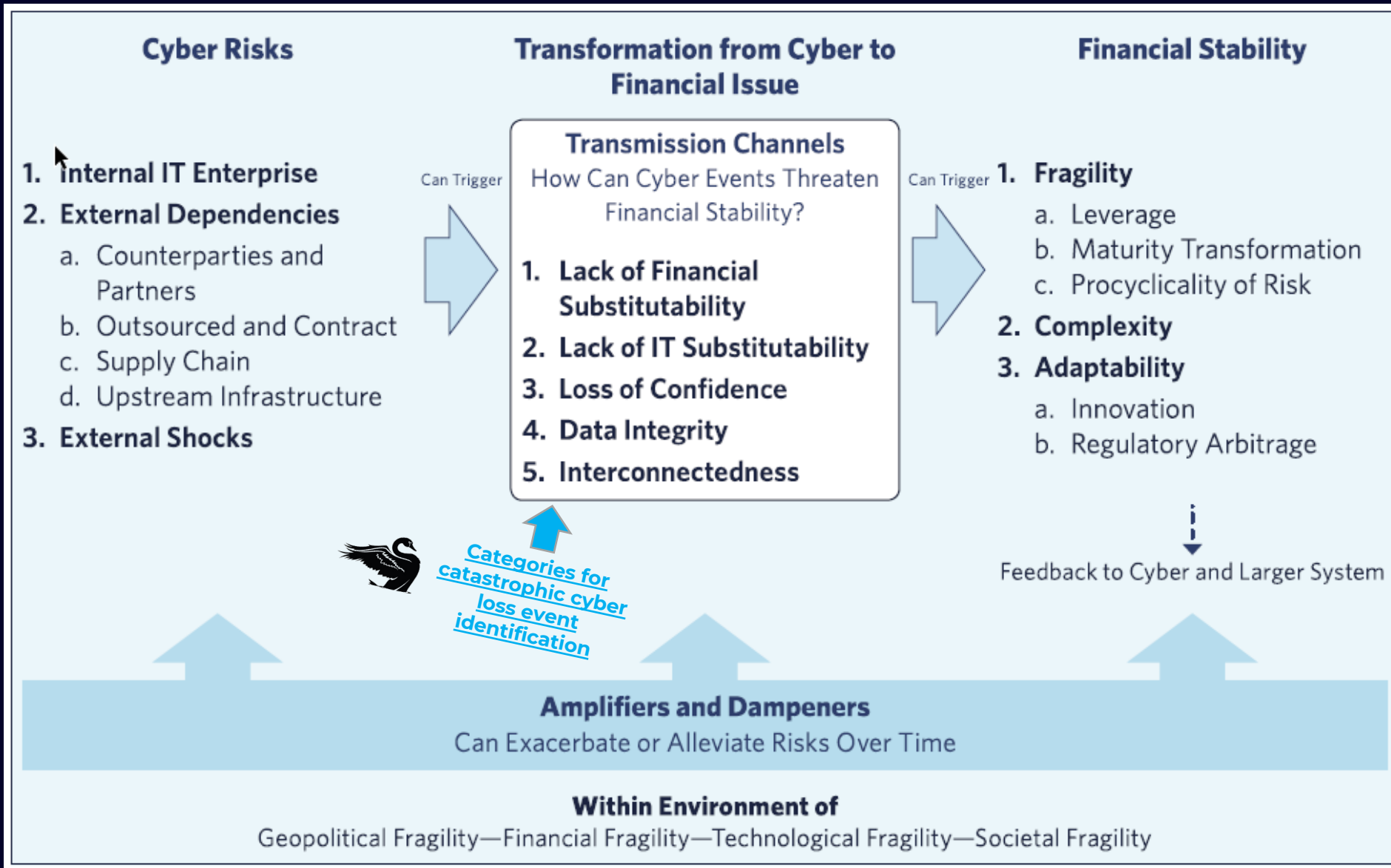


“As the financial system increases its reliance on information technology, the risk increases that a cybersecurity event in the industry will have severe negative consequences, potentially entailing systemic implications for the financial sector and the U.S. economy.”

FSOC

FINANCIAL STABILITY OVERSIGHT COUNCIL





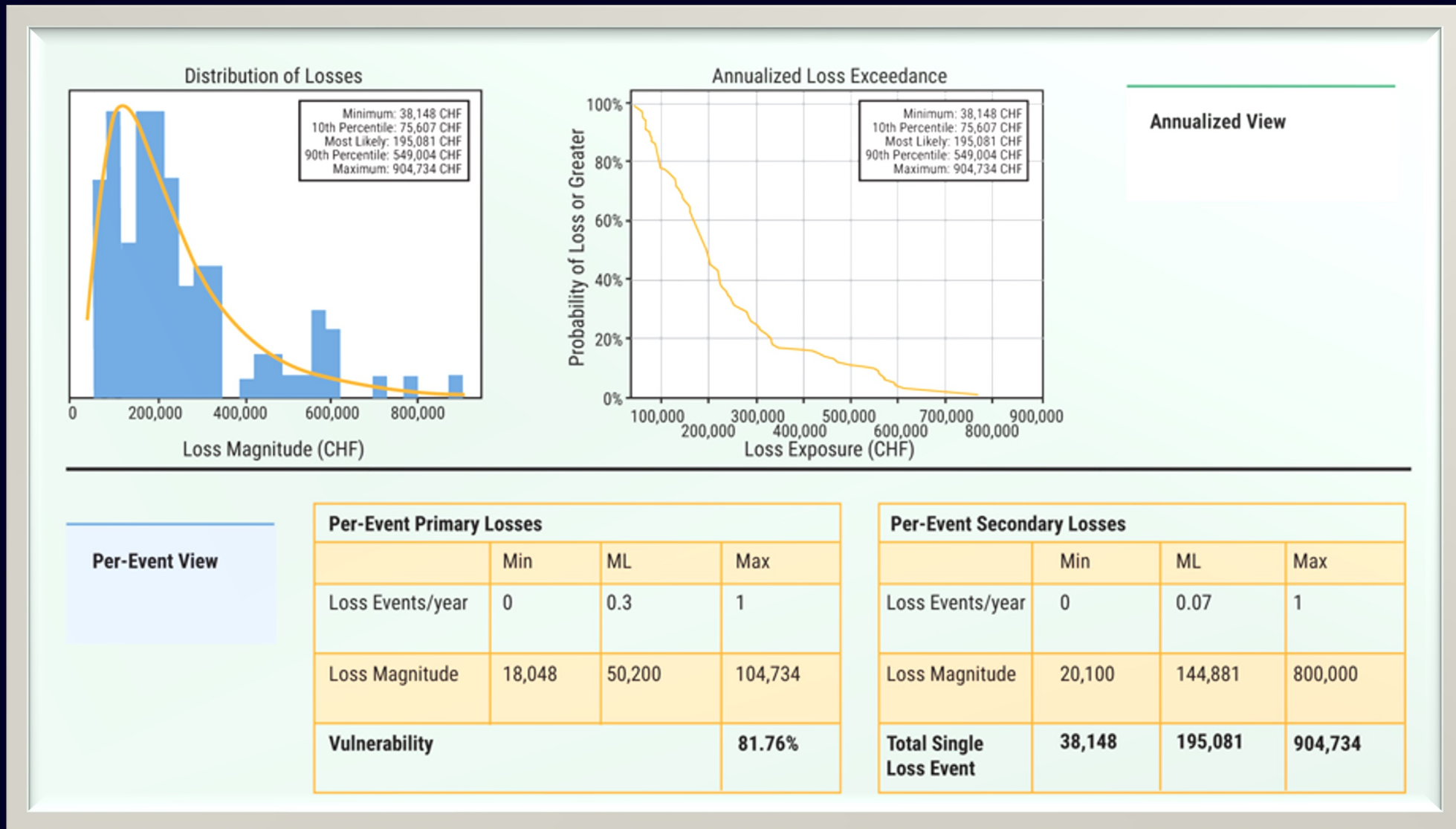


FUTURE TRENDS INCREASING CYBER LOSS EVENT LIKELIHOOD

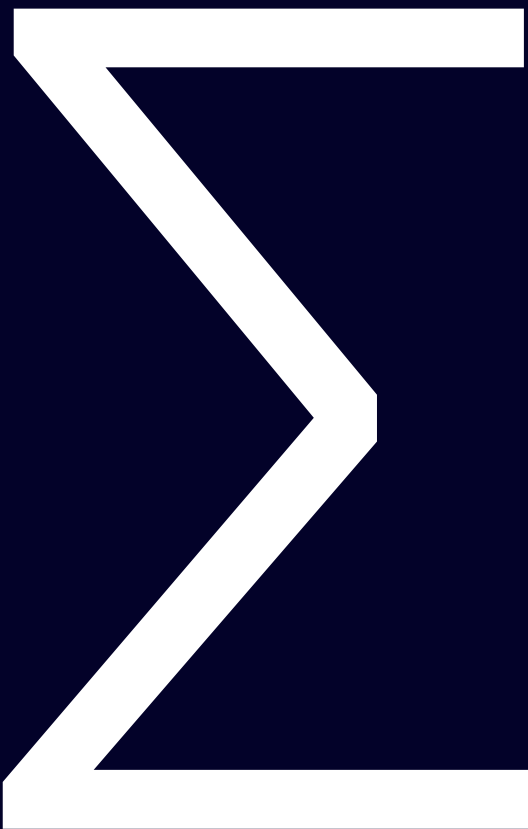
- 3rd party, cloud, supply chain & **critical infrastructure concentrations**
- Adoption of increasingly sophisticated cyber tools & methods
- AI/ML automating attacks and circumventing intrusion detection
- **Increased interconnectedness**, accelerated by APIs
- New risk exposures from adopting 5G, IoT, FinTechs, & **mutli-cloud**
- Quantum computing obsolescing current encryption investments
- Shorter clearing and settlement windows as well as change windows

+

**The global security environment
continues to be less benign**



FAIR observed used for CCAR stress testing (idiosyncratic scenarios), capital planning, and loss-adjusted forecasting.



- Duration?
- Liquidity impact?
- Capital position impact?
- Contagion/amplification?
- Monte Carlo simulation

Infosec is like rocket engineering...

- A small control failure could fail the entire system.
- A series of innocuous events could result in complete failure.
- A control that has not been tested and shown to work under worst-case scenarios should not be assumed to work under those conditions.

Example: IDS vs netflow to detect APTs



Supervisory cyber data not QUANTITATIVE...

#s and \$s

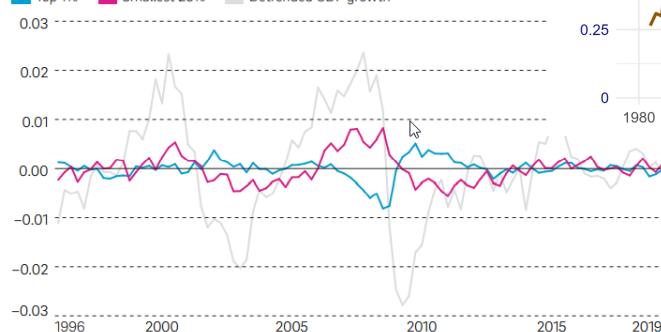
PCA Category	Total RBC Ratio	Tier 1 RBC Ratio	CET1 RBC Ratio	Tier 1 Leverage Ratio
Well Capitalized	10%	8%	6.5%	5%
Adequately Capitalized	8%	6%	4.5%	4%
Undercapitalized	< 8%	< 6%	< 4.5%	< 4%
Significantly Undercapitalized	< 6%	< 4%	< 3%	< 3%
Critically Undercapitalized	Tangible Equity/Total Assets \leq 2%			

FIGURE 2

Assets at the Largest Banks Grow with GDP, Lowering the L

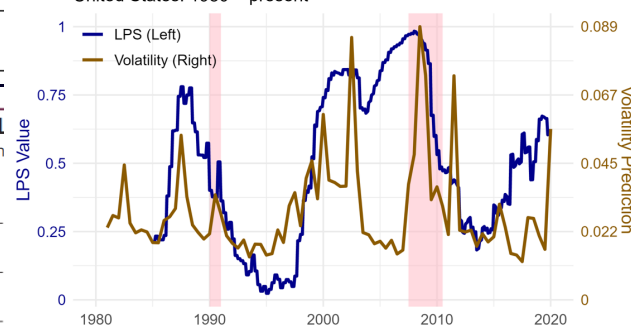
At the smallest, assets shrink and capital grows as GDP grows, raising the change in leverage ratio for largest and smallest banks, compared to change in GDP

Top 1% Smallest 25% Detrended GDP growth



Source: Call Reports aggregated and available through the National Information Center (NIC) of the Federal Reserve System

Traditional Methods: Vulnerabilities and Volatility
United States: 1980 – present



...but typically QUALITATIVE

subjective statements

- “Firm is progressing in implementing its cyber controls...”
- “Firm uses these types of cyber controls and risk management procedures...”
- “Firm has not systemically implemented this cyber control...”
- “Firm has tested the control against limited scenarios...”
- “Firm has adequate cyber controls in place...” or “Firm’s cyber controls not adequate...”

*Precision & consistency
prove challenging*

1. Systemic cyber/op risk assessment

Goal: consistently ascertain the **adequacy** of a firm's cyber & operational risk management program, practices, and controls **effectiveness**.

Cyber & Operational Risk Exposure

- **Dependencies & interconnectivity** exposure
 - "Bespoke" software and end of life technology
 - Consumer/retail services & customers/clients concentrations
 - Critical infrastructure reliance
 - FinTech, significant service provider, and 3rd / 4th party reliance
 - **Multi-cloud** reliance
 - Partners/counterparties extent and communication paths (APIs)
 - Payment processors reliance
 - Technology assets & service operations
 - Technology supply chain reliance
- **External stress state exposure**
 - Cyber and financial system shock events (amplification possible)
 - Financial system-level vulnerability extent
 - Market liquidity and counterparty stress state (contagion event)
- Firm condition
 - Merger/acquisition event
 - Technology adoption or change event
- Threat environment incident level likelihood
- Firm-level vulnerability extent
 - Control exceptions
 - Policy / standards / procedures **noncompliance**
 - **Risk acceptances**

Cyber & Operational Risk Preparedness

- Governance & risk management adequacy
 - 2LoD and 3LoD effectiveness
 - Adherence to **cyber/op-pertinent risk appetite**
 - Board and Management expertise, training, & preparedness
 - Board reporting, engagement, communications, & due care
 - Information security program, leadership, and operational personnel capabilities and consistency
 - KPIs, KRIs, & KCIs' effective selection, assessment, & reporting
 - **Risk acceptance** management effectiveness
- Inherent control effectiveness limitations
- Loss event scenarios & **control testing** adequacy
 - **Demonstrated controls effectiveness & capabilities against loss event scenarios (including compensating control validation)**
 - Regular and comprehensive tabletop as well as full BC/DR exercises against "high risk"-prioritized loss event scenarios
- Risk assessment adequacy
 - Analysis and modeling standards, methods, & consistency
 - **Communications preparedness (social media amplification)**
 - Expertise availability, credibility, and reliance
 - Idiosyncratic loss event scenarios (including "black swans")
 - Risk assessment program effectiveness, bias avoidance, and data management as well as data quality assurance practices
- Vulnerability management adequacy

Shock Resilience

- Capital planning effectiveness & capital reserves loss absorption
- **Liquidity** (call, term, funding, market)
 - Overnight liquidity coverage
 - **Short term liquidity (~1 week)**
 - Long term liquidity
 - **Artificial (asset fire sale) liquidity**
 - **Liquidity aggregation**
 - **Tradability**
- Living will effectiveness
- Public backstops
- "Safe harbors" preparations & testing
- Stress test adverse results resolution
- **Systemic financial environment & critical infrastructure preparedness and resilience**

Lessons learned for effective cyber & operational risk assessment

1. Ensure the **completeness** of data collected:

- How viable is the amount and type of data collected to substantiate effective analysis and range of practice determination?
- Extent and consistency of range of practice data.
- Determine & communicate precision.
- Openly vet and challenge results.

2. Ensure data **quality**:

- Ensure **specific** questions are asked.
- Ensure **consistent** responses required.
- Avoid “open input” for indicators; rely only on open input for substantiation.

3. Use **effective assessment results indicator terminology**:

- Problematic terminology: “**adequate**,” “**effective**,” “**satisfactory**,” “**84.3%**” (without range), “**generally/partially**,” “**meets expectations**”...results in generalization omissions, confirmation bias enablement, and range of practice inconsistency.
- Meaningful terminology: using indicator **absolutes**: “**control gap(s) identified**,” “**potential control shortcoming**,” “**no issues identified at this time**,” and “**notable practice**.”
- Decision trees for consistency.
- Magnitude of loss / material loss level often sufficient as issue indicator thresholds.

2. Understanding systemic consequences

Goal: understand extent of contagion as well as amplification of impact during shock events and adverse market conditions

$$b_t^i = \left(1 \mp \frac{2\sigma_{\text{ref}}^i}{\bar{r}_{\text{ref}}^i} \right) \bar{r}_t^i,$$

Bank “i” impaired if end of day reserve balance r drops below time-varying threshold b_t^i where \bar{r}_t^i is the past 30 day average reserve balance of bank i at time t , with numerator value 30 day standard deviation and average of bank i ’s reserve balance at reference date.

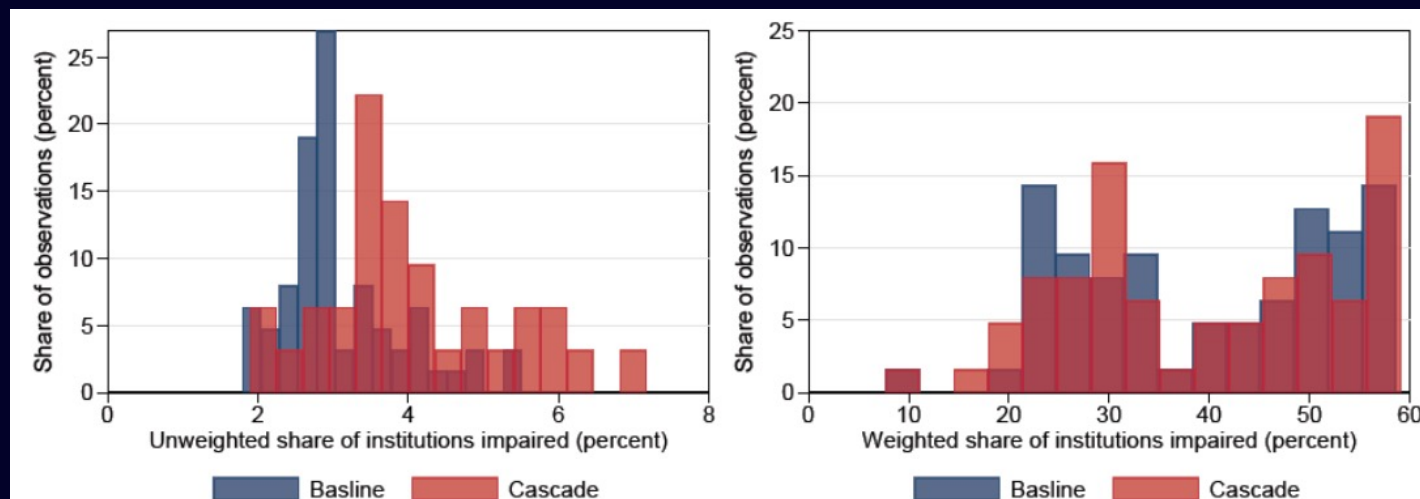
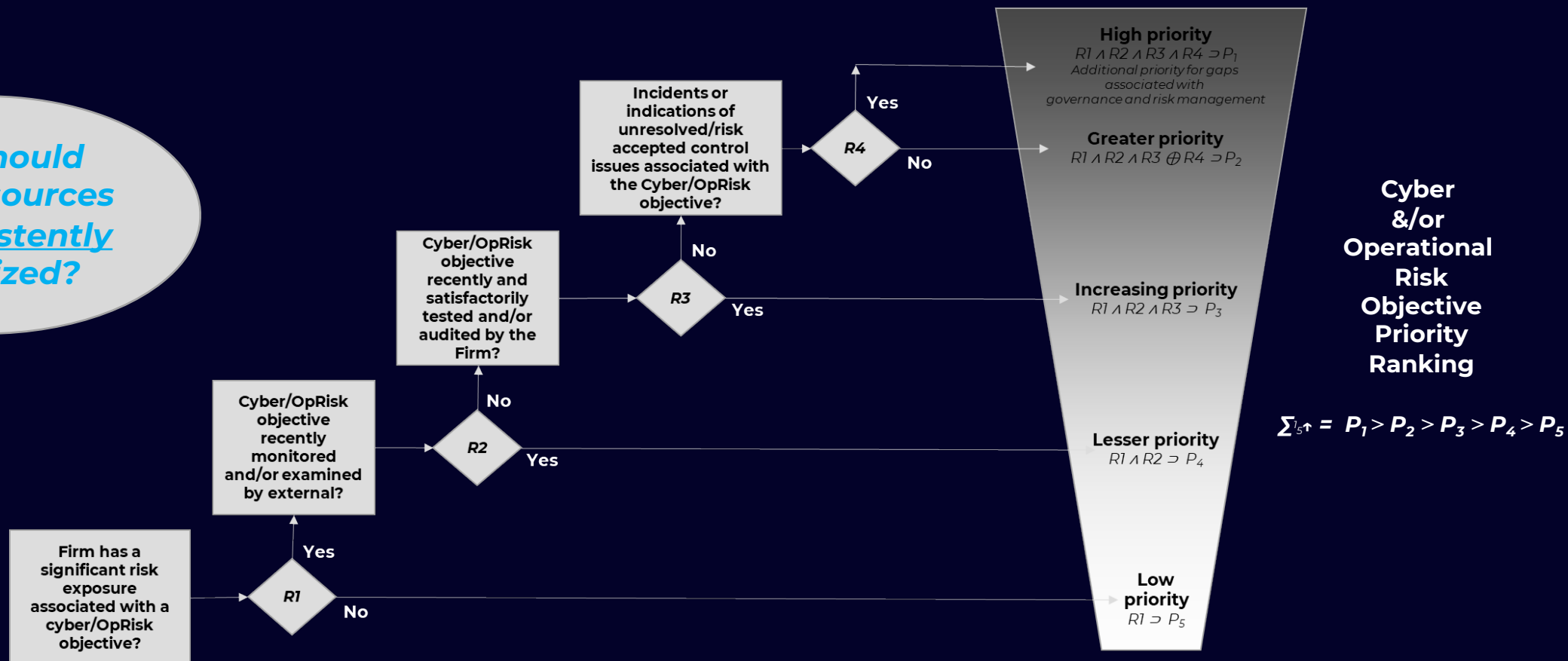


Figure 7: Comparison of simple and cascade scenario for February to April 2020. The figure shows the distribution across days of the impact for the baseline scenario and the cascade scenario for February to April 2020, averaged across the top-5 institutions. The left panel shows the unweighted share of impaired institutions. The right panel shows the share of impaired institutions weighted by payments (excluding the attacked institution).

3. Logic tautologies & decision trees

Goal: consistent control objective prioritization

How should
finite resources
be consistently
prioritized?



$$\sum_{5^{\uparrow}} = P_1 > P_2 > P_3 > P_4 > P_5$$

For next time: cyber risk appetite

1. Meaningful risk appetite statements, communications, and thresholds
2. Industry-recognized need for consistent cyber KPIs / KRIs / **KCIs** as well as thresholds
3. Category sampling:
 - Availability (KPI)
 - Incidents (KPI)
 - Losses (KPI)
 - Open/past due issues (KRI)
 - Personnel (KPI / KCI)
 - Risk acceptances & control exceptions (including legacy / EOL / bespoke system exposure) (KRI)
 - **Tested control effectiveness (KCI)**
 - Third party dependence (KPI / KRI)
 - Vulnerability management (including patching) (KPI / KRI)
4. Uniting cyber KPIs / KRIs / KCIs with other risk appetite measurements & thresholds
 - Available (liability) liquidity ratio
 - 25% 6 month total liability loss "cliff" - 2009 *Managing Liquidity in Banks*
 - Capital adequacy, including normal & stress ratios
 - Counterparty risk exposure
 - Leveraged lending ratio
 - Leverage normal & stress ratios
 - Minimum liquidity coverage ratio (daily/monthly)
 - Net stable funding ratio
 - Operational loss event exposure
 - Time to required funding
 - Value at risk and potential stress loss

Note that these KPIs / KRIs / KCIs and thresholds are not comprehensive nor regulatory required but instead representative of measurements to consider.



Matt Tolbert

CISA, CISSP, CRISC

Senior Cybersecurity Specialist
Federal Reserve Bank of Cleveland

Thank you

*The views stated herein are those of the
presenter
and not necessarily those of the Federal
Reserve Bank of Cleveland
or of the Board of Governors of the Federal
Reserve System.*

Supplemental

The Federal Reserve System


The Federal Reserve System is the central bank of the United States. It performs five key functions to promote the effective operation of the U.S. economy and, more generally, the public interest:

- conducts the nation's monetary policy to promote maximum employment and stable prices in the U.S. economy;
- promotes the stability of the financial system and seeks to minimize and contain systemic risks through active monitoring and engagement in the U.S. and abroad;
- promotes the safety and soundness of individual financial institutions and monitors their impact on the financial system as a whole;
- fosters payment and settlement system safety and efficiency through services to the banking industry and U.S. government that facilitate U.S.-dollar transactions and payments; and
- promotes consumer protection and community development through consumer-focused supervision and examination, research and analysis of emerging consumer issues and trends, community economic development activities, and administration of consumer laws and regulations.



To learn more, visit:

www.federalreserve.gov/aboutthefed.htm

A photograph of Jerome Powell, Chair of the Board of Governors of the Federal Reserve System, speaking at a podium. He is wearing a dark blue suit, a white shirt, and a blue and white striped tie. He has grey hair and is wearing glasses. A microphone is positioned in front of him. The podium features the Presidential Seal of the United States. The background is blurred, showing greenery and a building.

**“Of the risk
factors we face,
cyber risk is
certainly the
largest...”**

Jerome Powell

Chair of the Board of Governors of the
Federal Reserve System

THE WALL STREET JOURNAL.

English Edition | February 18, 2020 | Print Edition | Video

ECONOMY

New York Fed Paper Warns a Cyberattack on Banks Could Cause Major Disruption

The authors say if a cyberattack were to compromise banks' systems, there could be severe implications for the broader financial system.



The Federal Reserve Bank of New York in Manhattan released the paper Monday.

Publicly Available Supporting Sources:

- Federal Reserve: 2022 **Cyber Risk & Financial Conditions**; Thomas Eisenbach, Anna Kovner, and Michael Junho Lee
- Federal Reserve: 2022 **Implications of Cyber Risk for Financial Stability**; Danny Brando, Antonis Kotidis, Anna Kovner, Michael Lee, and Stacey Schreft
- Carnegie Endowment: 2021 **International Strategy to Better Protect the Financial System Against Cyber Threats**; Tim Maurer & Authur Nelson
- Federal Reserve: 2020 **Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis**; Thomas Eisenbach, Anna Kovner, and Michael Junho Lee
- Federal Reserve: 2019 **Coming to Terms with Operational Risk**; Gara Afonso, Filippo Curti, Atanas Mihov
- Brookings Institution: 2018 **The Future of Stability and Cyber Risk**; Jason Healey, Patricia Mosser, Katheryn Rosen, Adriana Tache
- Columbia University: 2018 **A Framework to Assess the Linkage Between Cyber Risks and Financial Stability**; Jason Healey, Patricia Mosser, Katheryn Rosen, and Alexander Wortman
- Institute of International Finance: 2017 **Cyber Security and Financial Stability**
- International Monetary Fund: 2017 **Cyber Risk, Market Failures, and Financial Stability**
- International Organization of Securities Commissions: 2016 **Guidance on Cyber Resilience for Financial Market Infrastructures**
- 2009 **Managing Liquidity in Banks**; Rudolf Duttweiler
- Federal Reserve/OCC/SEC: 2003 **Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System**

Loss Event Controls...

