



Cyber Risk Workshop

November 20, 2019



The views expressed do not necessarily reflect the views of or endorsement by the Federal Reserve Bank of Richmond, the Federal Reserve Bank of New York, or the Federal Reserve System.

To encourage frank and open exchange, the conference will be conducted under the Chatham House Rule. All attendees are welcome to use the information from the conference, but they should not attribute specific statements to individuals or institutions.

Welcome

- **Jeff Gerlach**, *Vice President, Quantitative Supervision & Research and Credit Risk Management, Federal Reserve Bank of Richmond*

Panel #1: Whitepaper Presentation, Feedback Updates and Q&A

- **Filippo Curti**, *Senior Financial Economist, Federal Reserve Bank of Richmond*
- **Sophia Kazinnik**, *Senior Quantitative Analyst, Federal Reserve Bank of Richmond*
- **Michael Lee**, *Financial Economist, Federal Reserve Bank of New York*
- **Atanas Mihov**, *Senior Financial Economist, Federal Reserve Bank of Richmond*

Cyber Risk

- Cyber incidents pose **a major threat** to the financial system
 - \$ billions lost annually to cyber breaches, fraud and business disruption
 - Potential financial stability implications
- **Top operational risk** for 2019
 - “[T]he majority of the [big banks’] CEOs cited cyberattacks as the foremost risk they faced” (Patrick McHenry, House Financial Services Committee)
- Yet, the **measurement and analysis** of cyber risk lag behind other major risk areas

Basic Questions

- How exposed is a financial institution to cyber risk?
- How effective are the institution's controls in mitigating cyber risk?
- How does the institution's cyber risk profile compare against peers?

Cyber Risk Definition and Classification: Objectives

- **Cyber risk in the financial sector:**
 - Different definitions in different contexts
 - Not consistently classified and measured across institutions
- We propose a **cyber risk definition and classification** for risk management purposes
- **Objectives:**
 - Cross-sector shared recognition and identification of relevant cyber risks
 - Assessment and monitoring of financial stability risks
 - Data collection and information sharing
 - Supervisory and regulatory guidance related to cyber risk management

Cyber Risk Definition

- **Cyber risk** is defined as the risk of loss resulting from:

digital incidents caused by internal, external or third parties, including theft, compromised integrity and/or damage to information and/or technology assets, internal and external fraud, and business disruption

➤ Form of **operational risk**

Cyber Risk Definition

- We define **cyber incident** as an observable occurrence in an information system that:
 - a) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or
 - b) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not
- A **cyber incident** is assumed to result in a financial loss and may have multiple loss impacts
- In contrast, a **cyber event** is defined as an observable occurrence in an information system that does not necessarily result in a financial loss

Cyber Risk Classification

- The proposed cyber risk classification is organized around 5 main concepts:
 1. ***Cyber incident consequence***: the outcome of a cyber incident
 2. ***Cyber incident cause***: the method through which a cyberattack is carried out
 3. ***Intent***: an indicator for whether the cyber incident was deliberate or accidental
 4. ***Origin***: an indicator for whether the cyber incident originated at the institution or at a third party/vendor
 5. ***Basel event type category***: the Basel event category assigned to the cyber incident

Proposed Data Collection

We envision a data collection with two schedules:

- 1) **Schedule at the loss incident level:** captures events that resulted in a financial loss
 - Gross loss and recovery
 - Consequence, cause, intent and origin
 - Remediation: action, time and cost
- 2) **Schedule at the aggregate level:** captures events that did not result in a financial loss along with ones that did
 - Number of cyberattacks (total and successful)
 - Total gross loss and recovery

Preliminary Feedback

- Why the Fed?
- What to share with the industry and how?

More Preliminary Feedback

- **Definition:**

- Indirect costs (possible to capture?)
- “Incident” vs. “event” terminology

- **Data Collection:**

- Add non-financial characteristics of cyber incidents (e.g., which control(s) failed)
- Define “non-successful” cyberattacks as the ones that breached at least one layer of controls (as opposed to all cyberattacks)

Classification of Intentional Incidents:

	Intentional			
Incident Consequence	Third Party	Non-Third Party	Basel Event-Type Category	Incident Cause
BDSEF	An intentional business disruption at a third party provider causes disruption to the firm.	An intentional act causes business disruption at the firm.	ET6	1-99
	Human error that led to an intentional business disruption at a third party provider.	Human error that led to an intentional business disruption at the firm.	ET7	1-99
Data Breach - PII	An employee of a third party provider uses their physical access to steal PII data from the firm.	An employee of the firm uses their physical access to steal PII data from the firm.	ET1	1-99
	An external party gains physical access under the control of a third party provider to steal PII data from the firm.	An external party gains physical access under the control of the firm to steal PII data from the firm.	ET2	1-99
Theft or Loss of Non-PII Information	An employee of a third party provider steals non PII data from the firm with remote access.	An employee of the firm steals non PII data from the firm with remote access.	ET1	1-99
	An external party steals non PII firm data from a third party provider with remote access.	An external party steals non PII firm data from the firm with remote access.	ET2	1-99
Theft of Funds	An employee of a third party provider uses their access to steal money from the firm or its customers.	An external party defrauds a third party resulting in monetary loss to the firm or the firm's customers.	ET1	1-99
	An employee of the firm uses their access to steal money from the firm or its customers.	An external party defrauds the firm resulting in a monetary loss to the firm or the firm's customers.	ET2	1-99

Incident consequence:

- **BDSEF:** Any type of internal or external incident that disrupts the business or causes a software/hardware/IT failure where there was no initial data, technology or monetary loss.
- **Data Breach – PII:** Any type of data loss or exposure involving Personally Identifiable Information (PII).
- **Theft or Loss of Non-PII Information:** Any type of theft or loss of technology, intellectual property, business proprietary information or any other information that is not PII.
- **Theft of Funds:** Any type of incident that led to an immediate and direct loss of funds, and was carried out via a digital channel.

Basel Event-Type:

1. Internal fraud (ET1)
2. External fraud (ET2)
3. Employment Practices and Workplace Safety (ET3)
4. Clients, Products & Business Practices (ET4)
5. Damage to Physical Assets (ET5)
6. Business Disruption and System Failures (ET6)
7. Execution, Delivery and Process Management (ET7)

Classification of Unintentional Incidents:

	Unintentional			
Incident Consequence	Third Party	Non-Third Party	Basel Event-Type Category	Incident cause
BDSEF	An unintentional business disruption at a third party provider causes disruption to the firm.	A software or hardware failure at the firm causes business disruption.		
			ET6	0 - Not Applicable
Data Breach – PII	A human error allows for unintentional business disruption at a third party provider, exposing PII data.	A human error allows for unintentional business disruption at the firm, exposing PII data.		
			ET7	0 - Not Applicable
Theft or Loss of Non-PII Information	A third party provider loses non PII firm data as a result of a hardware or software failure.	The firm loses non PII data as a result of a hardware or software failure.		
			ET6	0 - Not Applicable
	A third party provider loses non PII firm data as a result of a faulty process or human error.	The firm loses non PII firm data as a result of a faulty process or human error.		
			ET7	0 - Not Applicable

Incident consequence:

- **BDSEF:** Any type of internal or external incident that disrupts the business or causes a software/hardware/IT failure where there was no initial data, technology or monetary loss.
- **Data Breach – PII:** Any type of data loss or exposure involving Personally Identifiable Information (PII).
- **Theft or Loss of Non-PII Information:** Any type of theft or loss of technology, intellectual property, business proprietary information or any other information that is not PII.
- **Theft of Funds:** Any type of incident that led to an immediate and direct loss of funds, and was carried out via a digital channel.

Basel Event-Type:

1. Internal fraud (ET1)
2. External fraud (ET2)
3. Employment Practices and Workplace Safety (ET3)
4. Clients, Products & Business Practices (ET4)
5. Damage to Physical Assets (ET5)
6. Business Disruption and System Failures (ET6)
7. Execution, Delivery and Process Management (ET7)

Panel #2: Cyber Risk Definition (Introduction to Cyber Risk Management and the Need for Quantification)

- **John DeLong**, *Risk Management, Morgan Stanley*
- **Denyette DePierro**, *Vice President and Senior Counsel, Cybersecurity, Office of Advocacy and Innovation, American Bankers Association*
- **Keith Morales**, *Vice President, Office of the Chief Information Security Officer, Federal Reserve System*
- Moderator: **Michael Lee**, *Financial Economist, Federal Reserve Bank of New York*

Panel #3: Cyber Risk Classification

- **Steve Bishop**, *Head of Risk Information and Insurance, ORX Association*
- **Patrick Naim**, *CEO, Elseware*
- **Tawei (David) Wang**, *Associate Professor and Driehaus Fellow, DePaul University*
- Moderator: **Sophia Kazinnik**, *Senior Quantitative Analyst, Federal Reserve Bank of Richmond*



Cyber Risk - Incident Classification

November 2019

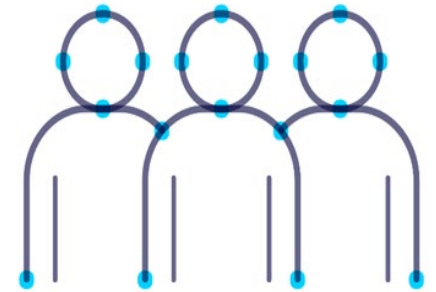
Steve Bishop, Head of Risk Information, ORX



ORX: Introduction



- Largest operational risk association in the financial services sector.
- Driving the development of operational & non-financial risk management and measurement.
- 99 members – majority of world's largest financial services firms. Owned by our members and not for profit.
- Delivering value to the industry through:



✓ Risk information:

Delivering shared learning & peer benchmarking

✓ Research & thought leadership:

Advancing operational risk management & measurement

✓ Practice

Driving risk management standards, including setting industry loss data standards

✓ Events

Facilitating member interactions across the globe

ORX: Addressing Cyber

O.R.X | Cyber

- ORX Cyber enhances the active management of cyber risk:
 - Driving improvements in the understanding of risk experience and exposure; and
 - Enhancing cyber risk management practices.
- The programme has brought together **2nd Line of Defence** cyber risk management teams from **45+ members**, collaborating through ORX to:



✓ **Share information:**

Addressing the risk data shortage and enabling peer benchmarking

✓ **Undertake research:**

Looking at risk management and reporting approaches

✓ **Develop standards:**

Enhancing practices across the industry

✓ **Improve collaboration:**

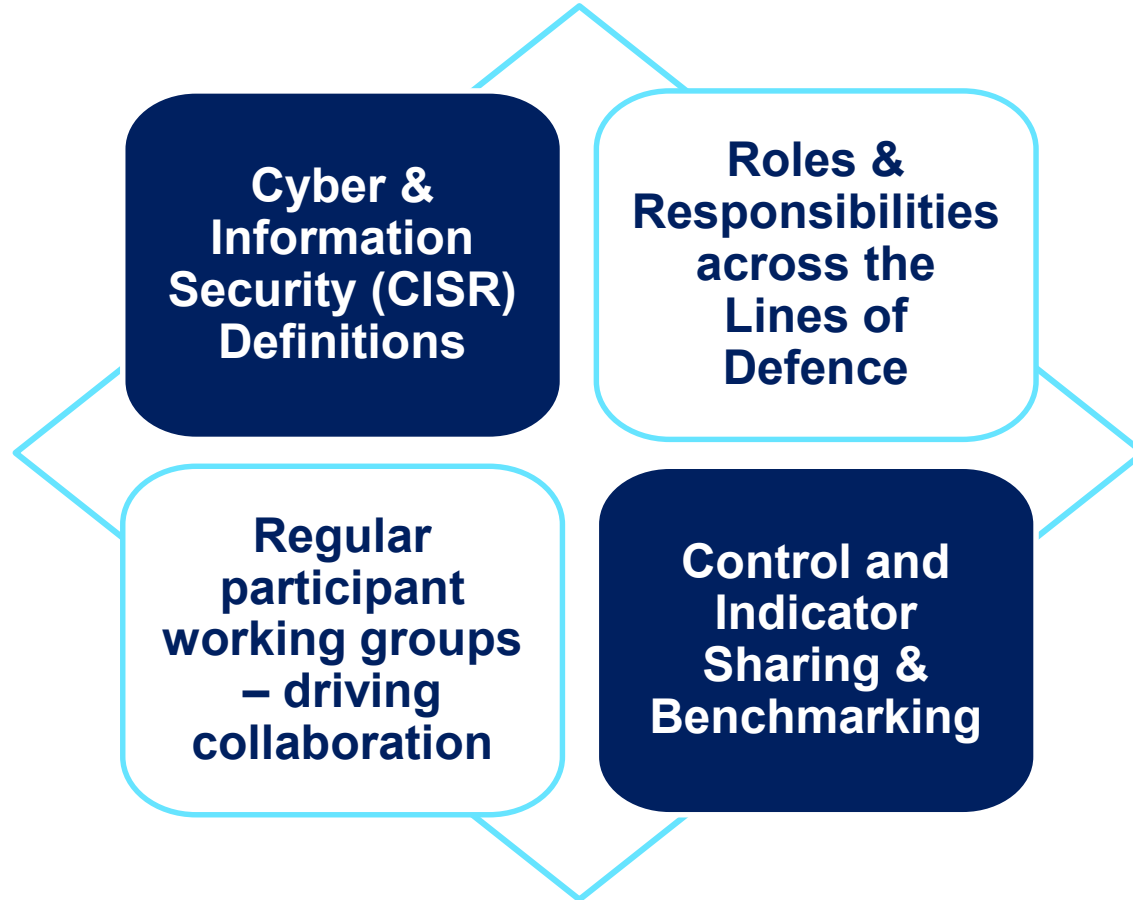
Through regular member working groups and forums, as well as with other industry bodies

ORX: Addressing Cyber

O.R.X

Cyber

Work progressed in 2019:



Upcoming activities:

- **Cyber Risk Management Reporting & Appetite Practices**
- **Anonymous sharing of Cyber Incidents**
- **Face-2-Face Forum**

See www.ORX.org for further details.

**Identifying & Sharing
Operational Risk
Loss Data
related to Cyber
is currently
challenging**

- ORX was originally set up for a unique purpose – to facilitate the anonymous sharing of operational risk loss event data.
- ORX has a database with over **700k** individual operational risk loss events, covering financial services and dating back to 2002.

BUT

Only Basel Event
Type classification
- makes it difficult
to identify cyber
losses

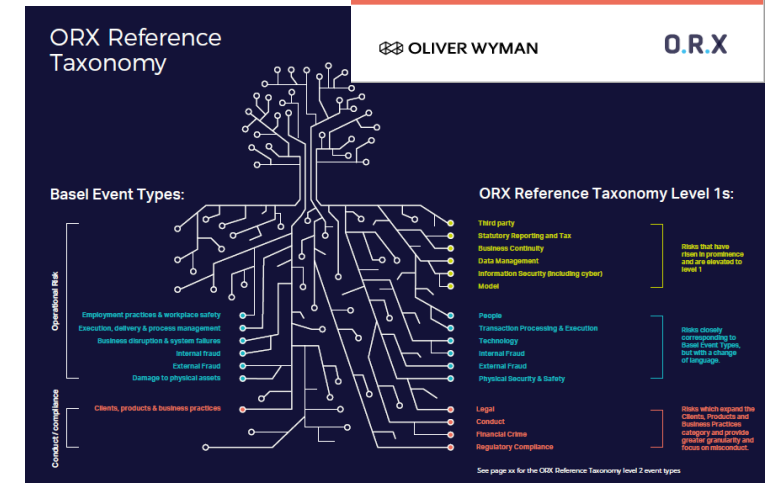
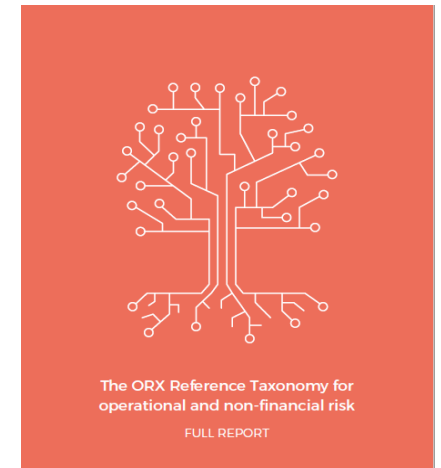
Cyber is often
treated as cause of
risk events – hiding
incident data
further

Operational risk
loss capture often
focusses on
financial loss only

ORX: Classifying & Sharing Cyber Incidents

ORX Reference Taxonomy - 2019:

- ORX has developed a level 1 and 2 **operational and non-financial risk reference taxonomy**.
- This has been designed to respond to the evolving nature of operational risks in financial services and is based on taxonomy data from **60 members**.
- Analysis highlighted **divergence** in the **classification of cyber** across the industry, exaggerated by the lack of industry risk taxonomy developments.
- However, cyber is at the forefront of institutions' minds:
 - 66% of taxonomies included standalone events referring to Cyber;
 - Many also noted it is commonly captured as a cause of events (e.g. fraud, data loss and technology failure); and
 - It has become common for institutions to use causal taxonomies and flags to gain a wider view of cyber risk.



A classification for collecting and sharing Cyber Risk Incidents

- The ORX Cyber Programme is developing a classification for the **capture** and **anonymous sharing** of cyber and information security (CISR) incident data.
- For this purpose CISR is defined as the risk of loss (financial / non-financial) arising from digital events caused by external or internal actors, or third parties.
- The objective is to overcome highlighted challenges and to deliver data and analysis so members can understand industry risk exposure and benchmark experience.

- ✓ Malicious events only
- ✓ Financial & non-financial thresholds
- ✓ Quarterly data collection

- ✓ Link to operational risk taxonomy
- ✓ Peer benchmark reporting
- ✓ ORX Analysis & Reporting

- ✓ Data attributes:
 - Incident Type (CIA), Data impacted
 - Actor, Attack Type
 - Cause and Impact
 - Control failure / lesson learnt

O.R.X

Thank you



An operative classification for cyber risk and resilience

Naim, Patrick, Mstar, patrick.naim@elseware.fr
Condamin, Laurent, Mstar, laurent.condamin@elseware.fr
Yao, Jane, ABA, JYao@aba.com

PILOT PROJECT ON CYBER RISK

- **Challenges of Cyber Risk**

- There is a gap between perceived risks and observed losses
- As most of cyber risk is intentional, it is rapidly evolving and adapting
- Cyber risk assessment involves IT and business

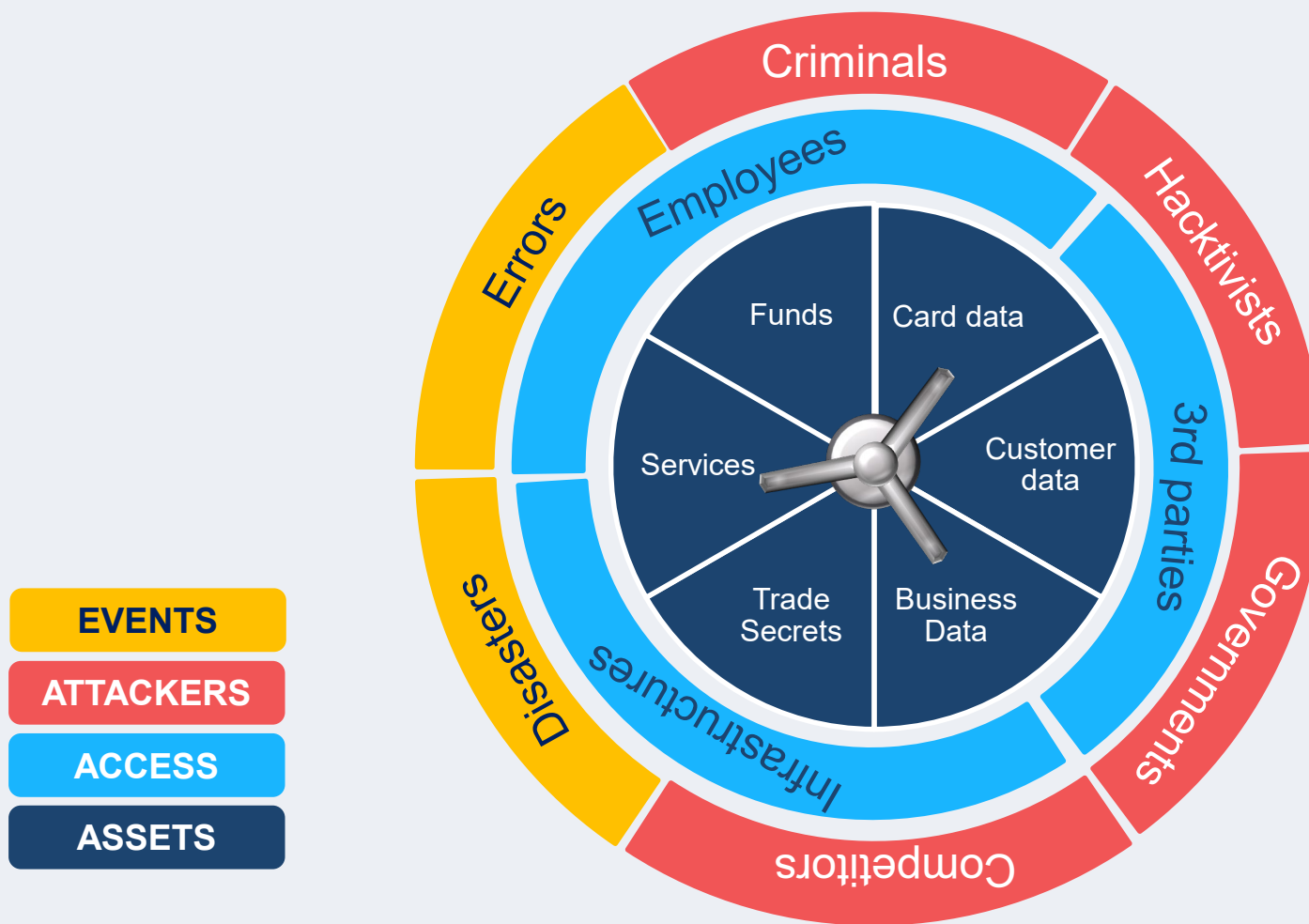
- **The ABA/MSTAR project**

- A one year (2019) project on Cyber risk modelling
- Facilitated by the ABA with the support of MSTAR modelling team
- 8 US banks

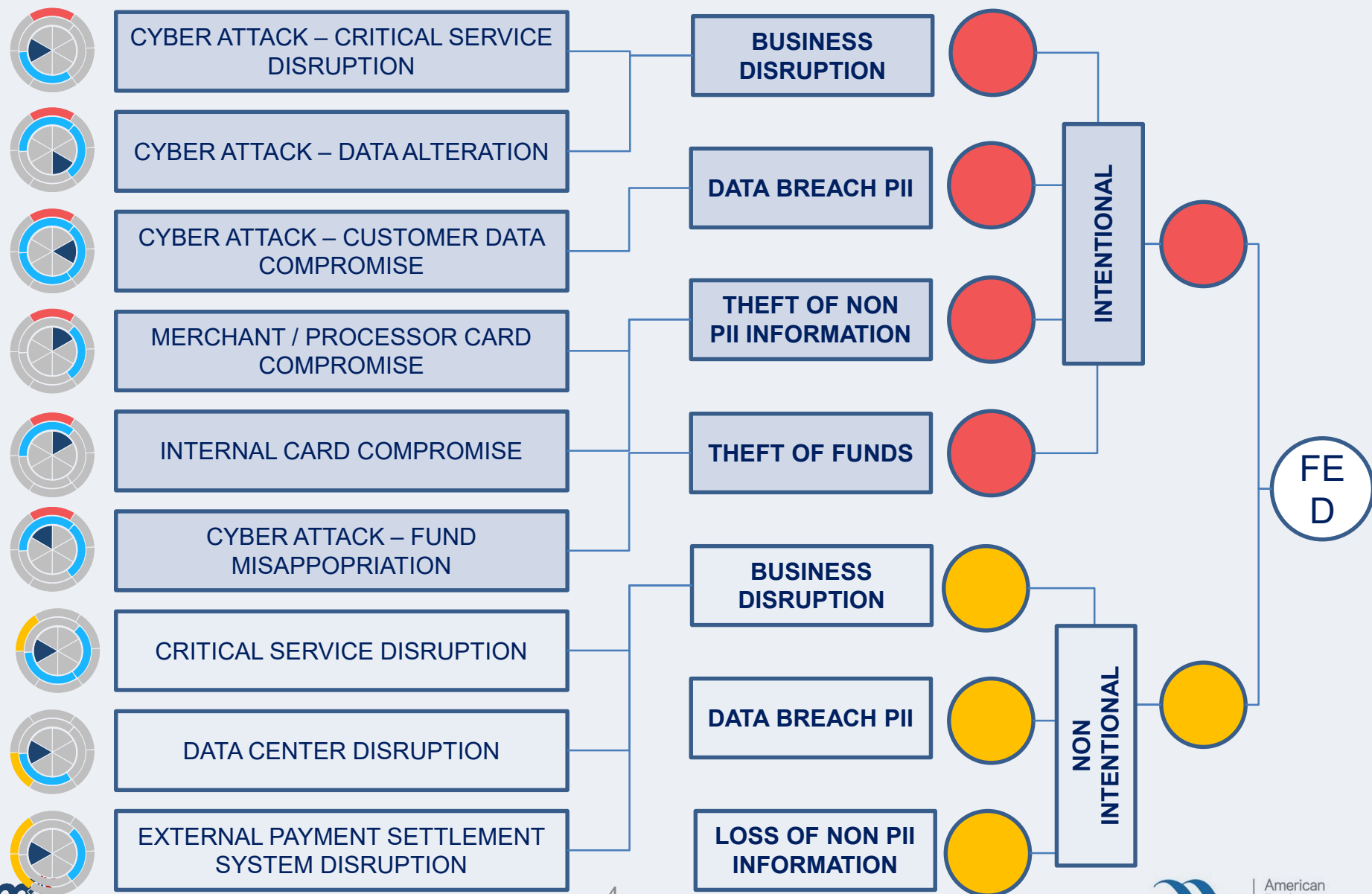
- **The objectives of the project**

- Build a shared classification of cyber risks
- Use this classification to define common cyber risk scenarios
- Assess cyber risk for participants, and benchmark assumptions and results

The cyber risk wheel

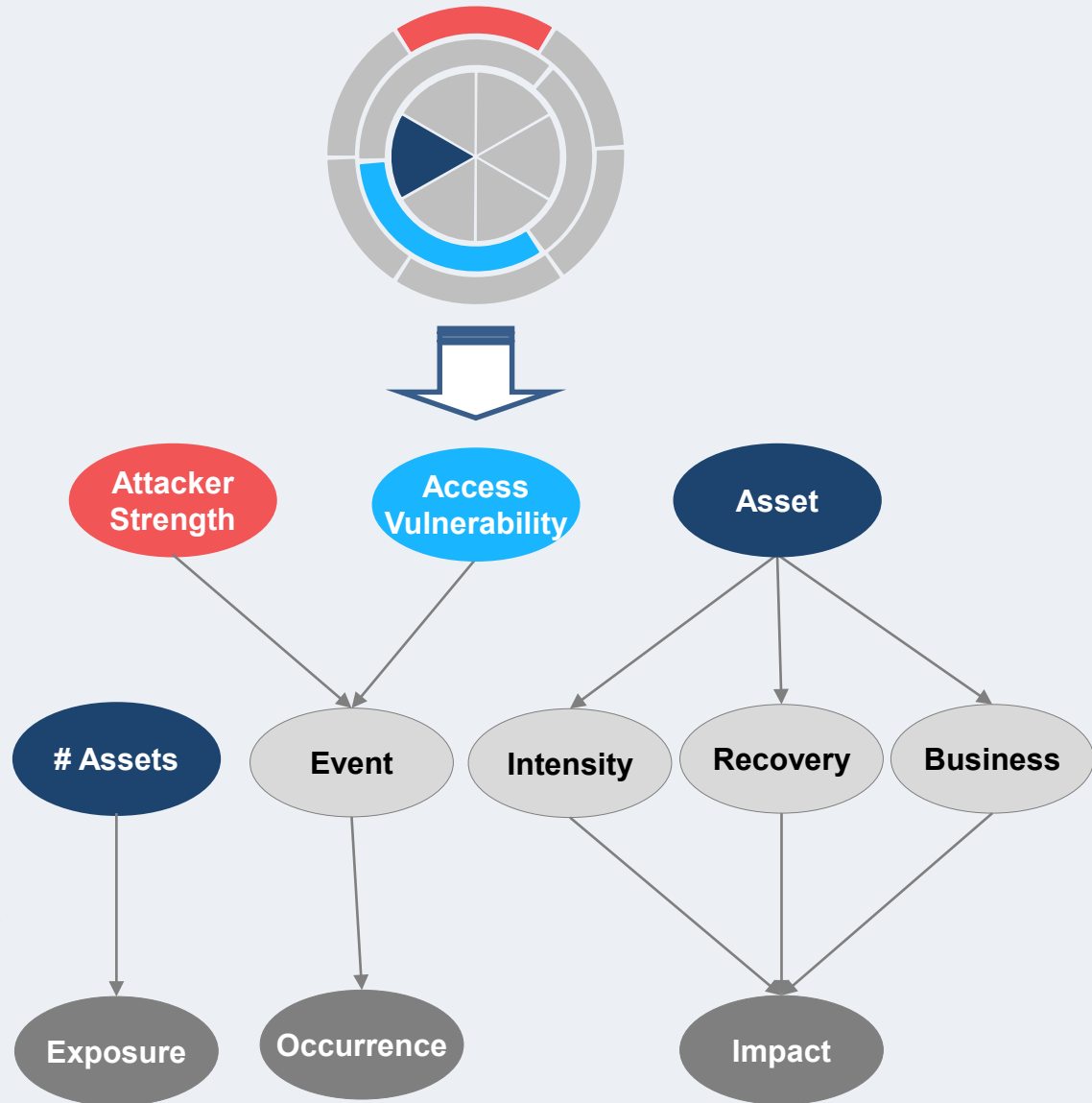


The resulting set of scenarios



Mapping to scenario assessment

- The Asset, Access, Attackers criteria are used for classification.
- They are also the foundation used to build a structured assessment of the scenario, and assess the drivers of Cyber Security and Cyber Resilience.
- The graph shown on the right is a scenario model for cyber risk assessment which can be used to assess potential losses.



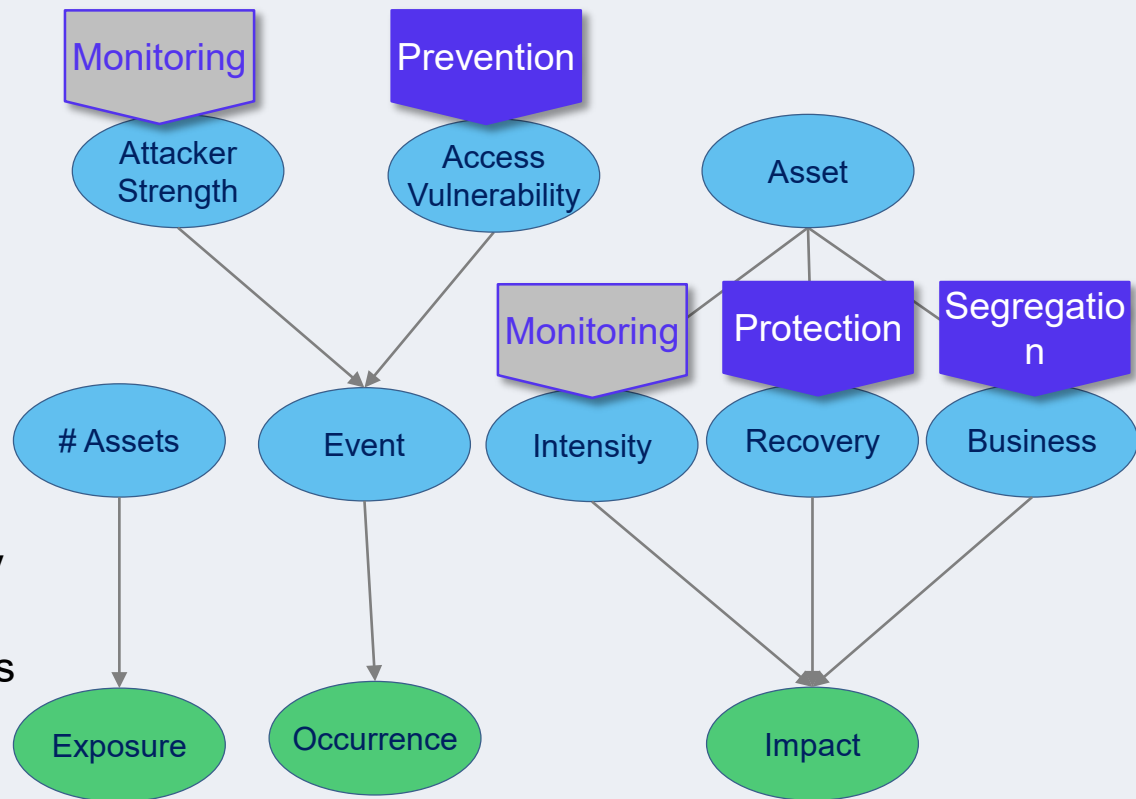
Mapping to RISK MANAGEMENT

- The drivers used in the model can be categorized for risk management purposes

- Exposure: Number of exposed units
- Threat: Level of external threat
- Vulnerability: Level of firm defense
- Intensity: Intensity of event
- Recovery : Firm resilience
- Business: Revenue, Volume

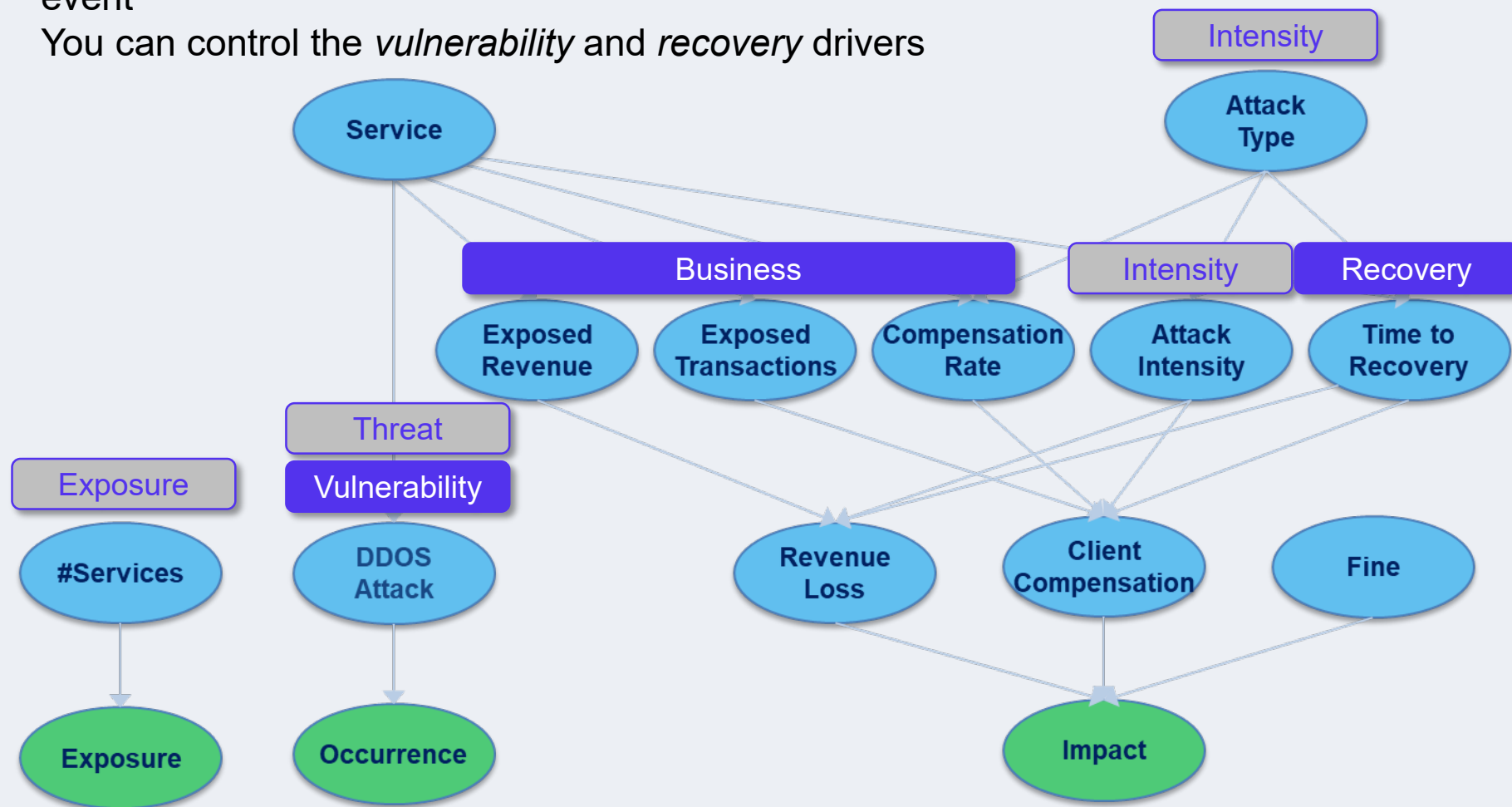
- The relevant mitigation actions follow :

- You have to *monitor* the intensity and threat drivers
- You can *segregate* your business to reduce the impact of an event
- You can *control* the vulnerability and recovery drivers



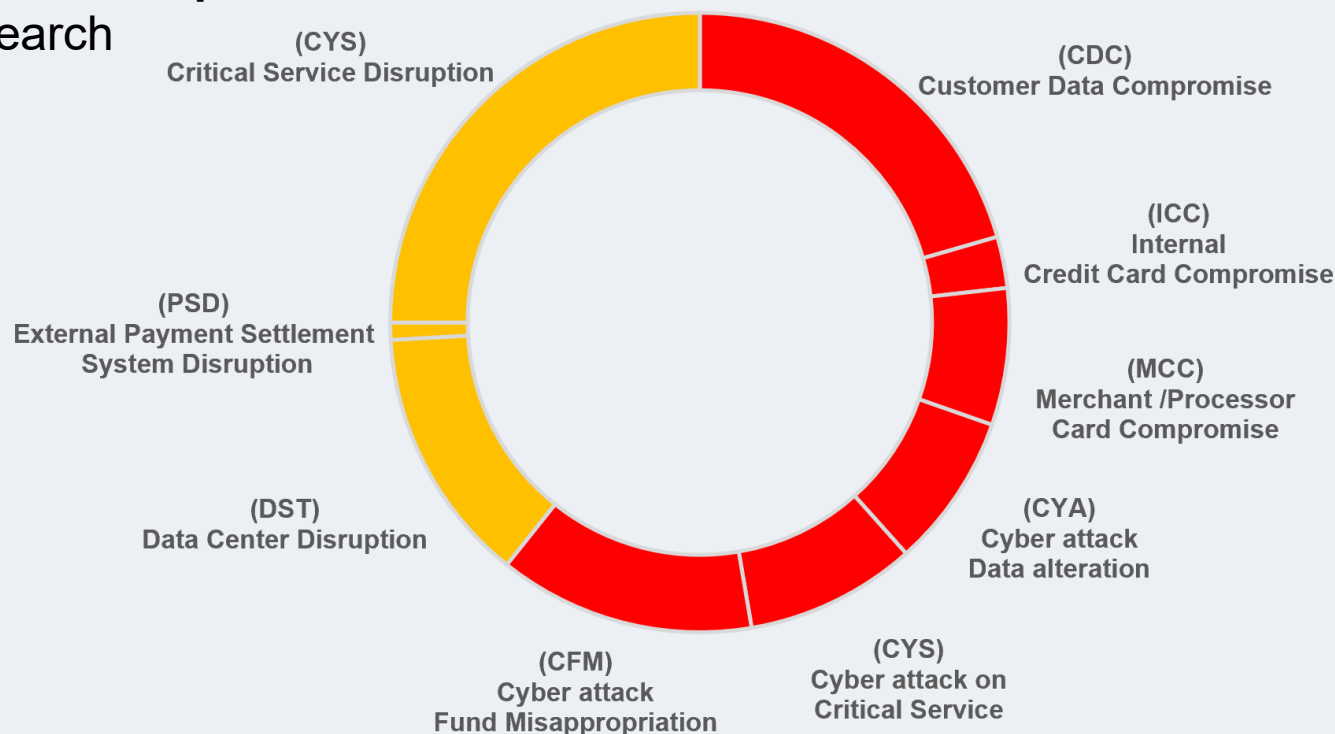
SSA DRIVERS & risk Management - example

- You have to monitor the *intensity* and *threat* drivers
- You can segregate your *business* to reduce the impact of an event
- You can control the *vulnerability* and *recovery* drivers



Illustrative cyber risk profile

- To build an illustrative quantification of the cyber risk profile, we have used :
 - **Business assumptions** for a hypothetical universal bank.
 - **Risk assumptions** based on external data and studies, and internal MSTAR research



Metrics used: VaR 99.9% of the scenario

Conclusion

- **An operative classification of cyber risk scenarios**
- **Compatible with the Richmond Fed Proposal**
- **Directly usable for building structured scenarios**
- **Directly usable for defining risk management actions**

Thank you!



Cyber Risk Classification

Tawei (David) Wang, PhD

2019 Cyber Risk Workshop
Federal Reserve Bank of Richmond, Charlotte Branch

About Me

- School of Accountancy and MIS, DePaul University
- PhD in Management Information Systems, CPA
- Research interests include information security risk management and IT management
- Teaching interests include analytics, IT auditing and IT management; involving in developing cybersecurity curriculum



“Cybersecurity is on top of everyone’s list.
What’s next?”

VP Internal Audit
Fortune 500 Company

How do companies represent cyber risk in their 10-K filings?

Research Findings 2010 – 2019

Presentation

- Generic terms
- Action-oriented terms

Content

- Business operations
- Financial performance
- Reputation
- Lawsuit and litigation
- Intellectual property

Trend

Percentage of companies disclosing a specific topic

- Business operations >90%
- Financial performance >80%
- Reputation >75%
- Lawsuit >60%
- Intellectual property <35% but increasing

Cyber Risk Classification

Source

Intentional

- Individual (insider vs outsider)
- Group
- Organization

Accidental

System Failure

Infrastructure / Disaster

Event

Confidentiality

Integrity

Availability

Vulnerabilities & Predisposition

Vulnerabilities

- Known
- Unknown

Predispositions

- Informational
- Technical
- Operational

Impact

Performance

- Operational
- Business value

Operations

Compliance

Litigation

Reputation

Equifax Breach Timeline in 2017

September

7

U.S. CERT notified the vulnerability regarding “Apache Struts”

The vulnerability info was distributed internally but was not patched

Internal scan did not identify the vulnerability

The security department noticed suspicious web traffic and took down the web application

Equifax Confirmed the loss of personally identifiable information

Announcement was made to the public; stock price dropped more than 13%; CIO, CSO, CEO retired soon afterwards

Source

Intentional

- Individual (insider vs outsider)
- Group
- Organization

Accidental

System Failure

Infrastructure / Disaster

Event

Confidentiality

Integrity

Availability

Vulnerabilities & Predisposition

Vulnerabilities

- Known
- Unknown

Predispositions

- Informational
- Technical
- Operational

Impact

Performance

- Operational
- Business value

Operations

Compliance

Litigation

Reputation

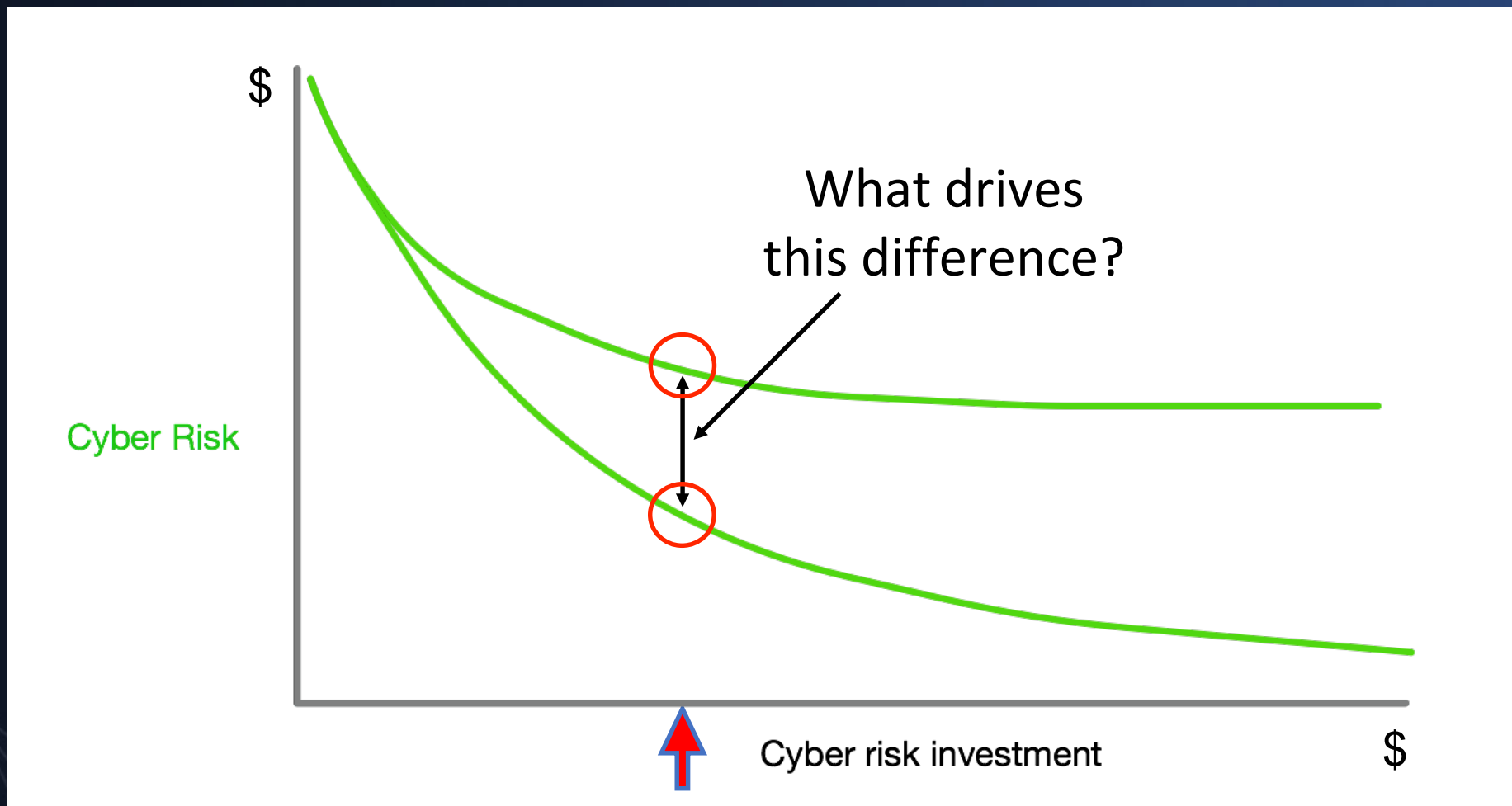
“Cybersecurity is on top of everyone’s list.
What’s next?”

VP Internal Audit
Fortune 500 Company

Panel #4: Costs and Benefits of Cyber Data Collection

- **Nedim Baruh**, *Managing Director, JPMorgan Chase*
- **Jack Jones**, *Chairman, The FAIR Institute*
- **Ni Kenney**, *Sr. Business Director, Risk Measurement and Capital Oversight, Capital One Financial*
- **Tim Pudner**, *Financial and Regulatory Reporting, Federal Reserve Bank of Richmond*
- **Evan Sekeris**, *Partner, Oliver Wyman*
- Moderator: **Filippo Curti**, *Senior Financial Economist, Federal Reserve Bank of Richmond*

Why it matters...



Decisions

How cost-effectively we apply our
risk management resources.



The risk landscape in a nutshell...

Complex



Dynamic



Limited Resources



Which
means...



Organizations must be very good at prioritizing their cyber risk problems and solutions.

70% to 90% of “high risk” issues, aren’t



A measurement example



How fast are they going?

Qualitatively

Challenges...

- Is your “fast” the same as mine?
- What’s your formula for speed? Is it the same as mine?
- Which car am I referring to?
 - One in particular? (Slowest? Fastest?)
 - An average for all of them?
- Which part of the track am I referring to?
 - Corners?
 - The straightaway?
 - Average over the entire track?
 - This lap, or an average for the entire race?

Measuring speed

- Requires three elements:
 1. The scope of what's being measured
 - Which car(s)?
 - Which part of the track?
 - Which lap(s)?
 2. An analytic model
 - What data? (time, distance)
 - How to apply the data? ($\text{speed} = \text{distance} / \text{time}$)
 3. Data

Measuring risk

- Every risk measurement involves three elements:

1. The scope of what's being measured

- ▶ What asset?
- ▶ What threat?
- ▶ Which vector?
- ▶ Which controls are relevant?
- ▶ What type of event (e.g., C, I, A)?

2. An analytic model (e.g., FAIR)

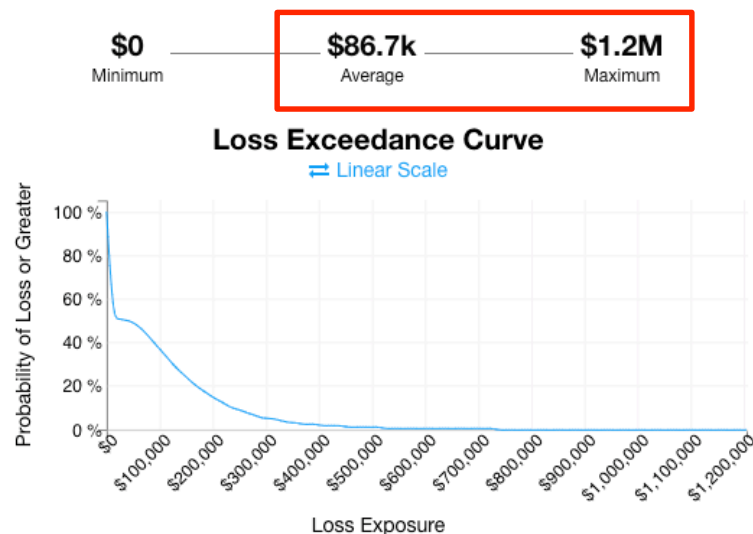
- ▶ What data?
- ▶ How to apply the data?

3. Data

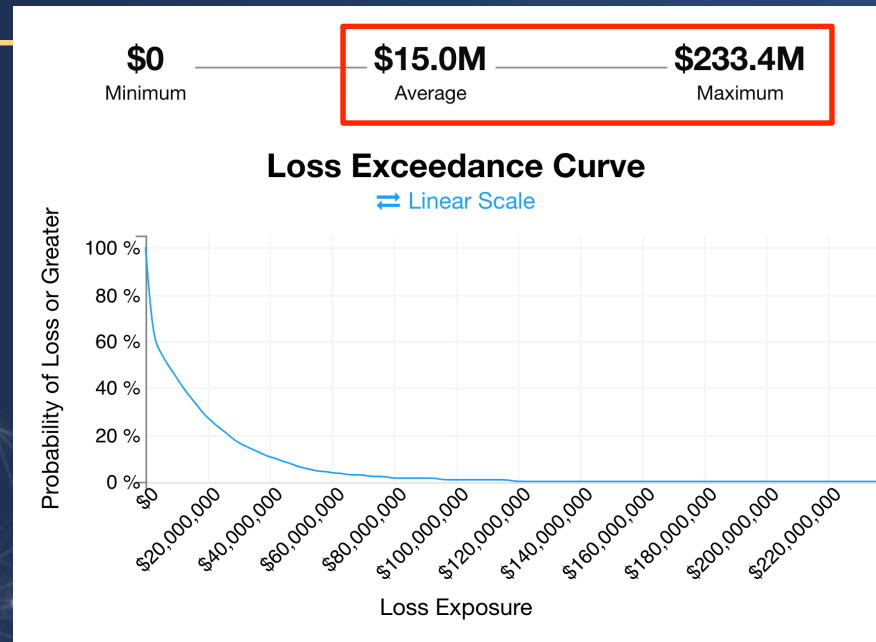
Which should we fix first?

An audit discovered that privileges are not consistently being updated for user accounts with access to a customer service application containing credit card numbers.

Analysis Results



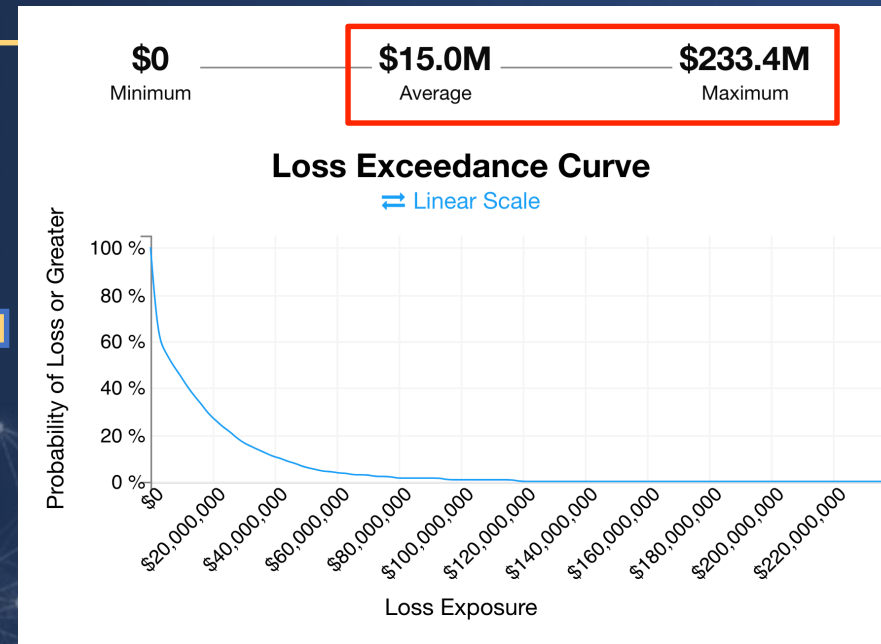
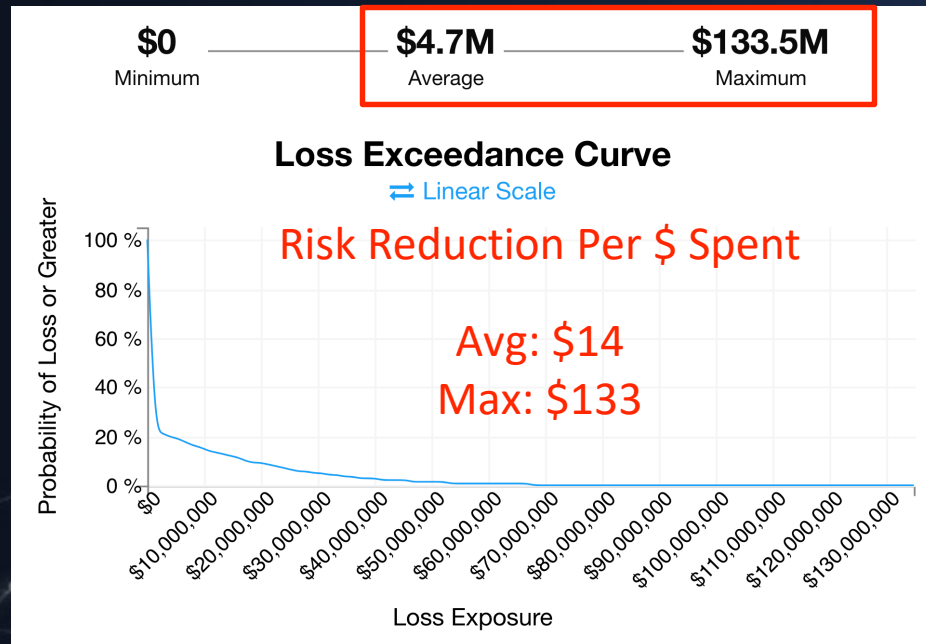
A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.



What's the ROI for "fixing" it?


A risk reduction solution was identified that was going to cost \$750k in year 1, and approx. \$300k yearly thereafter.

A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.



Summary

- Organizations must apply their cyber risk management resources cost-effectively.
- This requires the ability to prioritize accurately, and choose cost-effective solutions.
- These can only be accomplished thru reliable quantitative risk measurement.



Tim Pudner
Cyber Risk Workshop
November 20, 2019

Cyber Risk Workshop: Costs and Benefits of Cyber Data Collection



Richmond ▪ Baltimore ▪ Charlotte

Disclaimer

The views expressed are my own and do not represent those of the Federal Reserve Bank of Richmond or the Federal Reserve System.

Lessons from Implementing New Data Collections: 2009 - Present

Communication with diverse stakeholders early in the lifecycle of data collections is key to choosing the best definitions.

- Leveraging existing definitions increases benefits and reduces costs.
- Data definitions that can be leveraged for ongoing risk management increase benefits.

Trade-offs: Decisions Impacting the Costs and Benefits

- **Frequency:** How often should the data be submitted?
- **Quality Expectations:** Should the data be submitted on a “Best Efforts” basis or will there be high quality expectations from the start?
- **Confidentiality:** Should all data be Confidential Supervisory Information or should some be shared with the Public?



Questions?



Richmond ▪ Baltimore ▪ Charlotte

The background of the slide is an abstract design featuring several overlapping, wavy, translucent blue lines that create a sense of movement and depth. These lines are set against a light blue gradient background that transitions from a very pale blue at the top to a slightly darker blue at the bottom. The overall effect is clean, modern, and professional.

Thank You!