2019 Cyber Risk Workshop

FEDERAL RESERVE BANK OF RICHMOND
Richmond • Baltimore • Charlotte

Charlotte Branch
March 28, 2019

Welcome

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

Opening Remarks

- **Becky Bareford,** *First Vice President & COO, Federal Reserve Bank of Richmond*

Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, *Head of Risk Information & Insurance, ORX*
- **Deborah Bodeau**, *Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation*
- **Todd Waszkelewicz**, *Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York*
- **Trevor Watkins**, *Risk & Control Manager, PNC*
- **Albert Olagbemiro**, *Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond*

www.orx.org
+44 (0)1225 430 397

Cyber: a risk management perspective

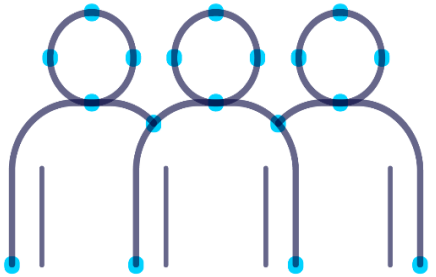
March 2019

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.
- 97 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 and measurement.
  - ✓ **Practice** – driving risk management standards, including setting industry loss data standards for many years.
  - ✓ **Events** – facilitating member interactions across the globe.

O.R.X Operational Risk Horizon 2019: Top five risks

Current risks

1. **Information security (including cyber)**
   89% of participants included an information security risk in their top ten
2. **Conduct**
   Over a quarter of conduct submissions were specifically concerned with retail mis-selling
3. **Fraud**
   The third highest risk for the last three years
4. **Transaction processing**
   Jumps from seventh last year
5. **Technology**
   79% of technology submissions expect these risks to increase in the next three years

Emerging risks

1. **Digital disruption and disintermediation**
   Remains number one emerging concern from last year
2. **Information security (including cyber)**
   95% expect their submitted risks to materialise in the next three years
3. **Geopolitical and macroeconomic**
   63% of all firms ranked it in their top ten
4. **Regulatory compliance**
   65% of larger firms ranked this in their top ten
5. **Third party**
   This risk's move into the top five is driven by the rise of cloud services

Top regional risks

Europe
Current: Information security (including cyber)
Emerging: Information security (including cyber)

Africa
Current: Information security (including cyber)
Emerging: Digital disruption and disintermediation

North America
Current: Information security (including cyber)
Emerging: Digital disruption and disintermediation

Asia/Pacific
Current: Information security (including cyber)
Emerging: Digital disruption and disintermination

managingrisktogether.orx.org

ORX: Cyber in the News

O.R.X | News

SEC EDGAR database hackers stole files and earned USD 4.1 million through insider trades

Hackers access Citrix's systems using brute force attacks and steal at least 6TB of data

Jackson Country pays USD 400,000 ransom to regain control of internal IT systems

British Airways suffers data breach compromising information on 429,000 customer cards

Banco de Chile loses USD 10 million and experiences service disruptions during malware attack

ORX: Cyber risk management challenge

- ORX members report challenges when identifying, categorising and assessing cyber.

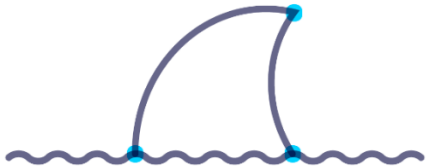
Basel event types make it difficult to identify and benchmark cyber risk

Different perspectives from firms' Risk and IT teams

Financial loss focus a factor in data shortage for assessing risk exposure

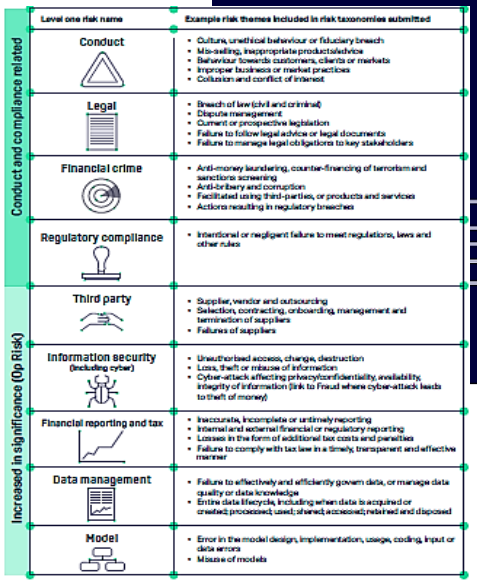
Difficult to see whether correct controls in place and actions taken

The risk has evolved rapidly and doesn't fit with traditional risk management practices & processes



ORX: Categorising cyber risk

- Members are moving away from the traditional Basel event type categorisation.
- ORX research shows many are developing risk based taxonomies, supporting risk management activity.
- A proportion include Cyber risk as a unique category. Some instead capture cyber as a flag or theme ('transversal' risk), others don't capture it.
- This inconsistency helps explain the challenge in identifying, classifying and benchmarking the risk within, as well as between firms.

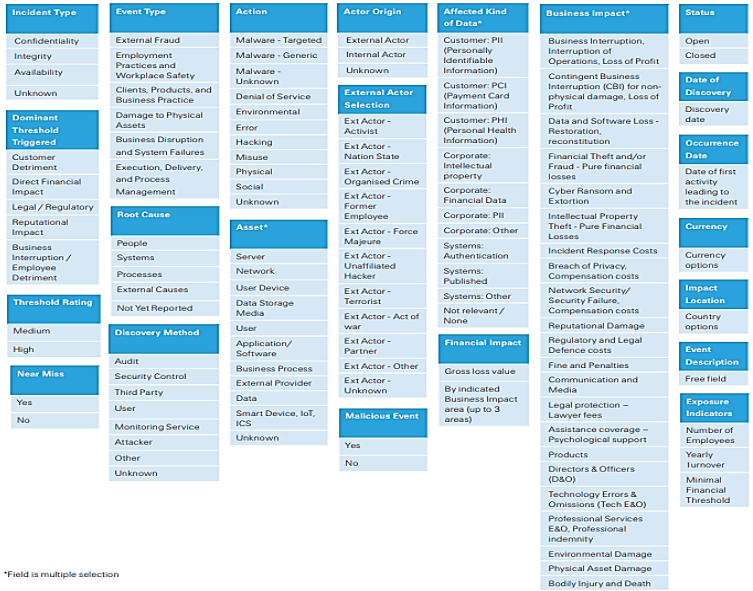


Use 'Cyber' in taxonomy?	%
Yes	48
No	43

Source: ORX 2018 Taxonomy Report

ORX: Categorising cyber risk

- From 2016, ORX was involved in a trial to identify, collect and categorise cyber & IT incidents.
- Categorisation combined IT (based on VERIS and STIX) and operational risk components.
- Principles for the trial included:
  - Easy to use by different specialists.
  - Incidents collected with a range of impacts, including loss, clean up costs, reputational and regulatory.
  - Access to data with cooperation between Risk and IT.
  - Data collected monthly.
  - Allow peer comparison and benchmarking.



Source: CROF Cyber Trial Report

An increase in Cyber Risk information began to improve risk management and measurement capability amongst participants

ORX: Addressing the issue

- Working with members, ORX has now launched O.R.X | Cyber to support the active management of cyber risk.

- This is bringing together **2nd Line of Defence** cyber risk management specialists, using the ORX 'Platform' 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.

O.R.X | Cyber

ORX: Addressing the issue

O.R.X | Cyber

Members will benefit through:

- Improved data definition, categorisation and identification.
- Improved understanding and reporting of cyber risk.
- Enhanced cyber risk management practices and peer benchmarking.
- Improved understanding between operational risk and cyber risk management teams.

> *Collaboration among many stakeholders on cybersecurity is critical to progress.*
>
> R. Quarles, Vice Chairman for Supervision, The Fed

ORX Cyber will drive improvements in the understanding of risk experience and exposure, enhancing cyber risk management in the industry.

Steve Bishop

Head of Risk Information, ORX

Steve.bishop@orx.org

Follow ORX on LinkedIn

Visit www.orx.org

Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, *Head of Risk Information & Insurance, ORX*
- **Deborah Bodeau**, *Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation*
- **Todd Waszkelewicz**, *Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York*
- **Trevor Watkins**, *Risk & Control Manager, PNC*
- **Albert Olagbemiro**, *Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond*

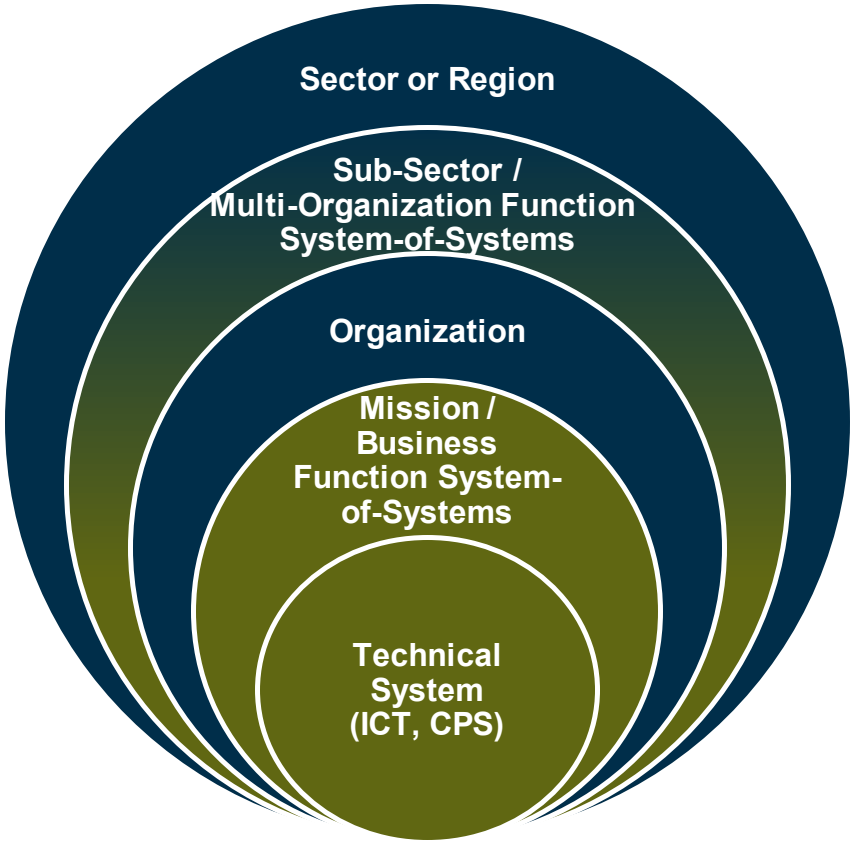
Cyber Threat Modeling in the Identification and Classification of Cyber Risks and Analysis of Cyber Resiliency

Deborah J. Bodeau
Senior Principal Security Engineer
The MITRE Corporation
dbodeau@mitre.org

MITRE

MITRE Approved For Public Release Distribution Unlimited Case Number PRS_18_2010-10

Cyber Risk and Cyber Resiliency Can Be Considered at a Range of Scopes or Scales



Cyber Risk and Cyber Resiliency Are Closely Related

Cyber Risk

The **risk of depending on cyber resources**, i.e., the risk of depending on systems or system elements which exist in or intermittently have a presence in cyberspace

Consider (may focus on) adversarial threat actors operating in cyberspace

Often evaluated as **likelihood** for a defined impact or set of consequences (e.g., data breach)

Cyber Resiliency

The ability to **anticipate**, **withstand**, **recover** from, and **adapt to adverse conditions**, stresses, attacks, or compromises **on** systems that use or are enabled by **cyber resources**

Focus on advanced cyber adversaries, who may emulate or leverage threat events from other sources

Enables definition and evaluation of strategies, practices, and technologies to reduce **consequence severity** as well as likelihood of subsequent events, assuming the success of prior threat events

For Characterization Purposes, Any of the Components of Risk Can Serve as a Starting Point

Cyber risk to a system is a function of

- **Threats**
- **The structure, characteristics, and behaviors of the system**
  - Characteristics can include vulnerabilities
- **The consequences of threats materializing or acting on the system**
  - Can be identified with asset loss
- **In an (assumed or observed) operational environment**

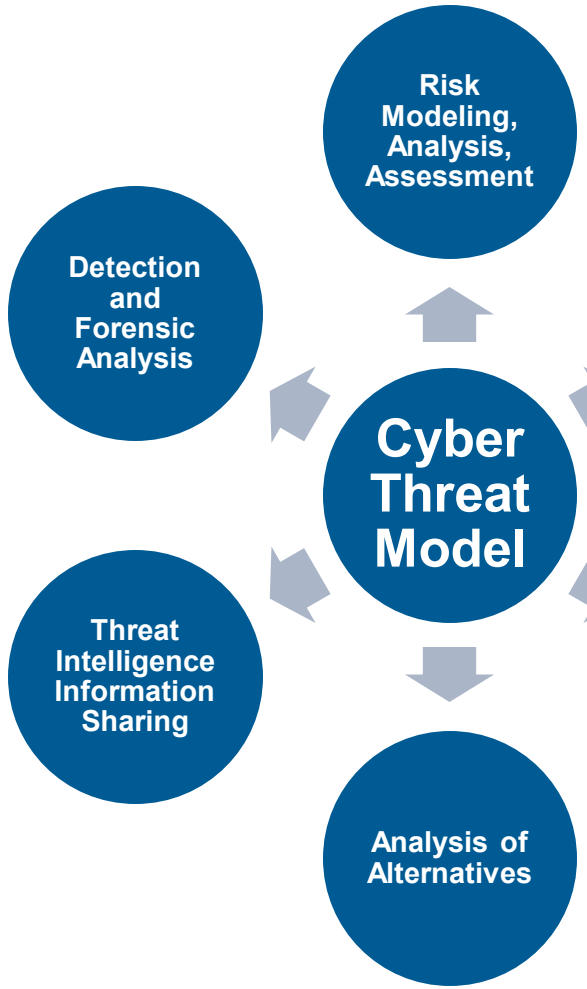
Decrease in cyber risk to a system is one measure of the effectiveness of a cyber resiliency solution

Starting with Threats Can Simplify Discussions and Facilitate Characterization and Identification

- **Avoid the need to share sensitive information about**
  - System structure, behavior, or vulnerabilities
  - Potential or past consequences
- **Avoid arguments about how best to describe systems and vulnerabilities**
- **But starting with "threat" requires qualification**
  - Threat source ≠ threat event ≠ threat scenario

MITRE Approved For Public Release Distribution Unlimited Case Number PRS_18_2010-10

The Cyber Threat Component of Cyber Risk Can Be Used in Multiple Ways



Assess likelihood of **threat scenarios** or **threat events** that produce identified consequences

Determine characteristics of observed **threat events, threat scenarios**

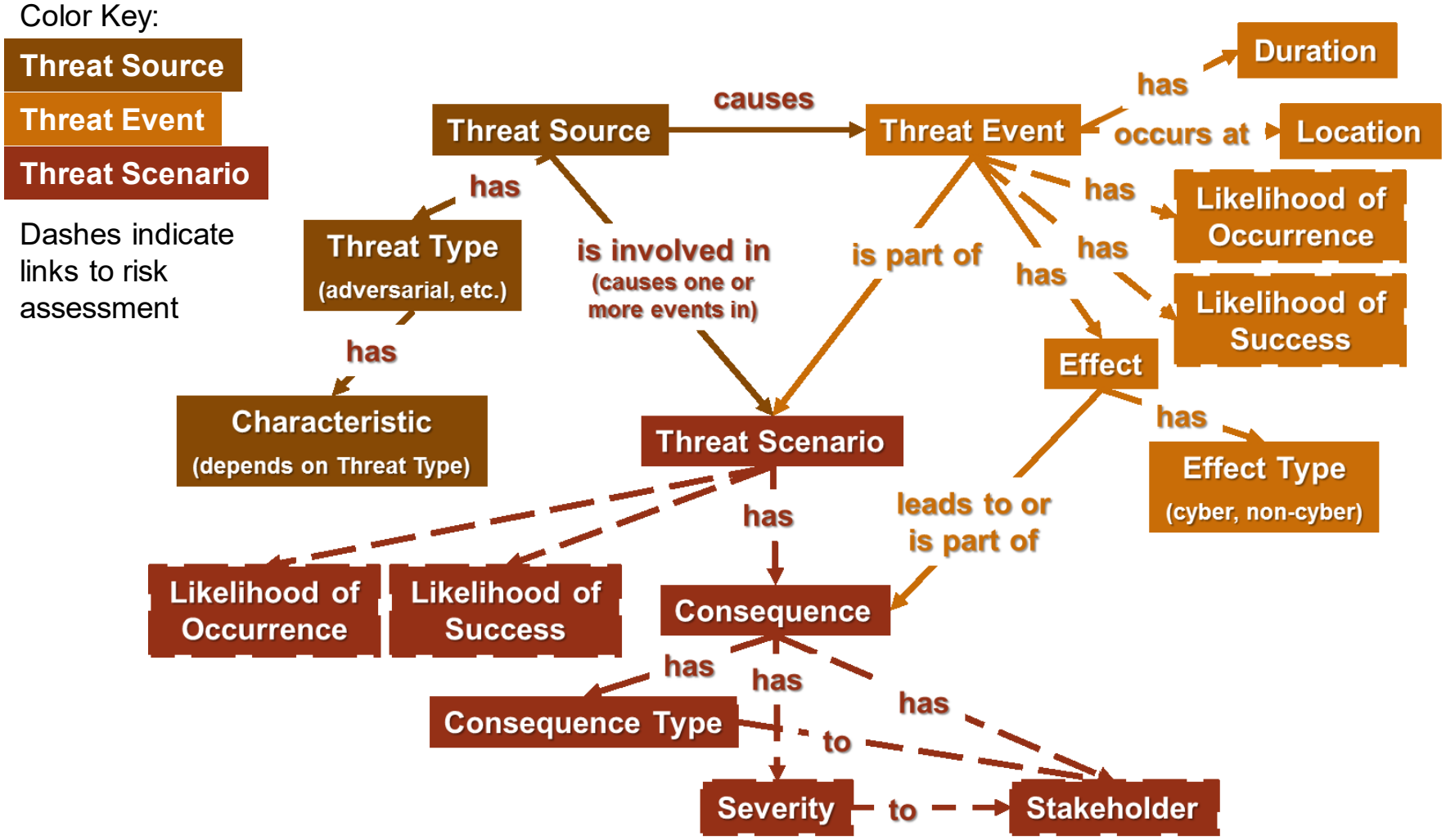
Determine operational resilience, cyber resiliency in context of representative **threat scenarios**, stresses, and operations

Share information about **threat characteristics**, observed **threat events**, observed or posited **threat scenarios** in the form of cyber campaigns

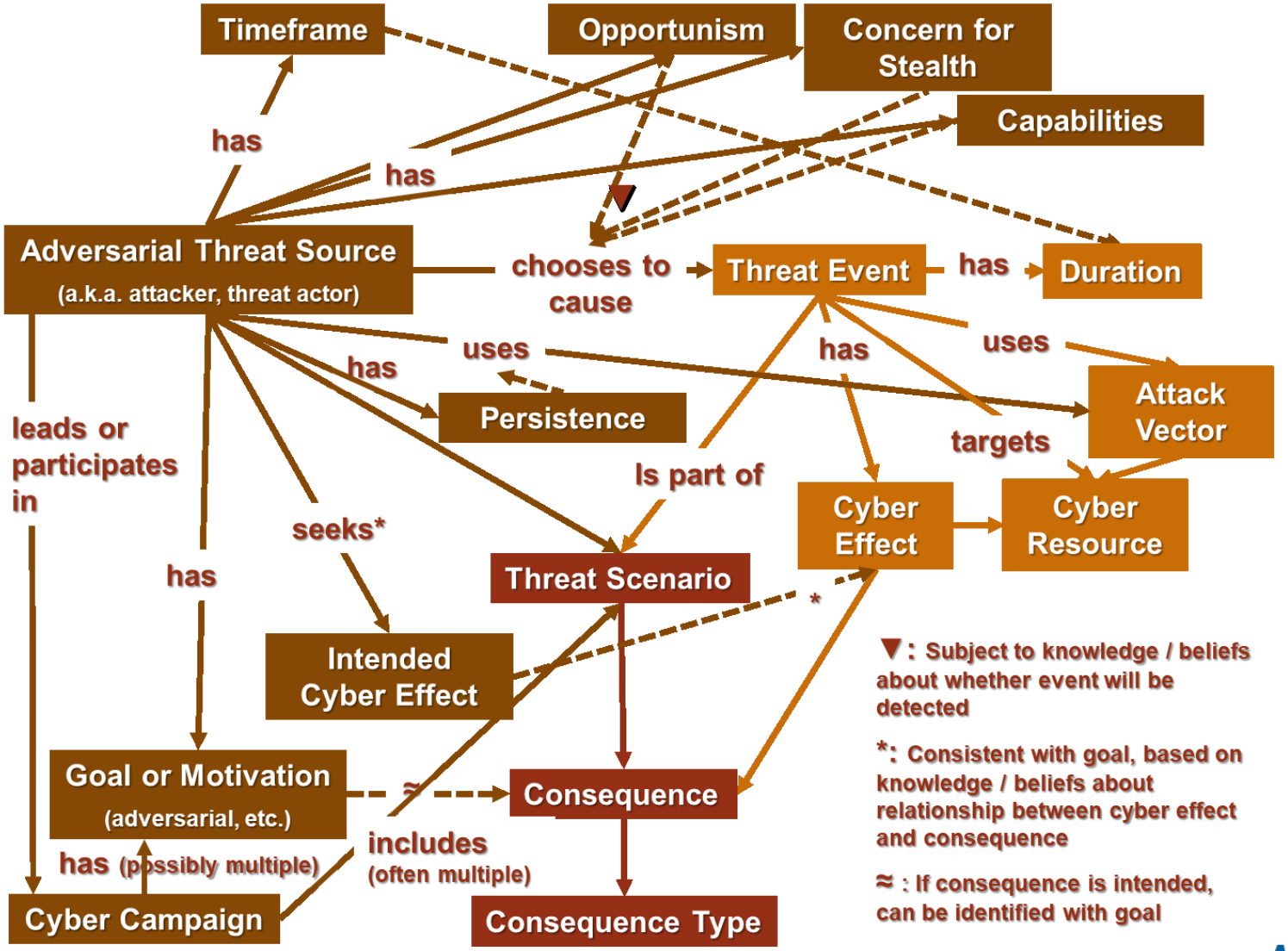
Determine which effects on **threat events** are possible; identify (and possibly assess) effects of requirements, controls, cyber resiliency solutions on adversary objectives or actions

Analyze the potential decrease in risk, ability to achieve cyber resiliency objectives, in the context of assumed **threat characteristics**

Threat Models Can Include Many Factors …

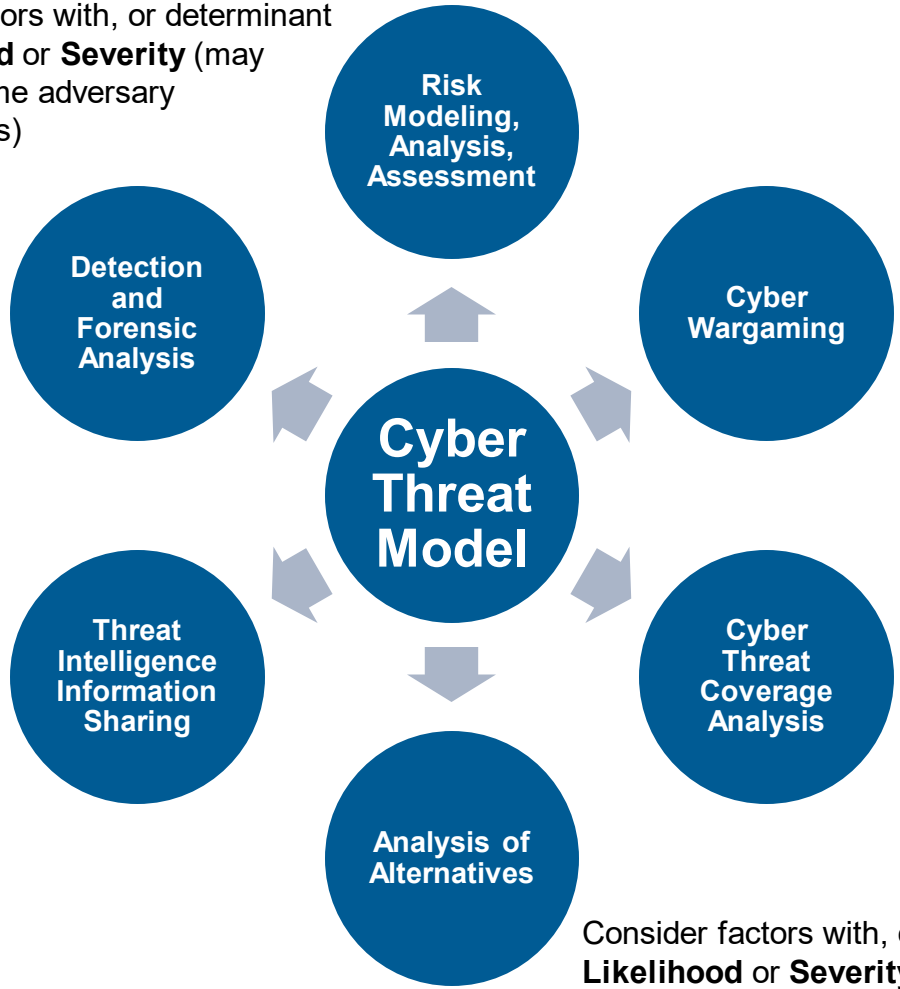


… Even When Restricted to Adversarial Threats Against Cyber Resources



But Factors Irrelevant to an Intended Use Can Be Disregarded, Enabling Focus to Be Driven by Use

Focus on factors with, or determinant of, **Likelihood** or **Severity** (may downplay some adversary characteristics)



Consider **Cyber Effects** of **Threat Events**, to look for artifacts and indicators

Define representative **Threat Scenarios**, considering **Threat Events** and their characteristics; only consider adversary characteristics to motivate Scenarios

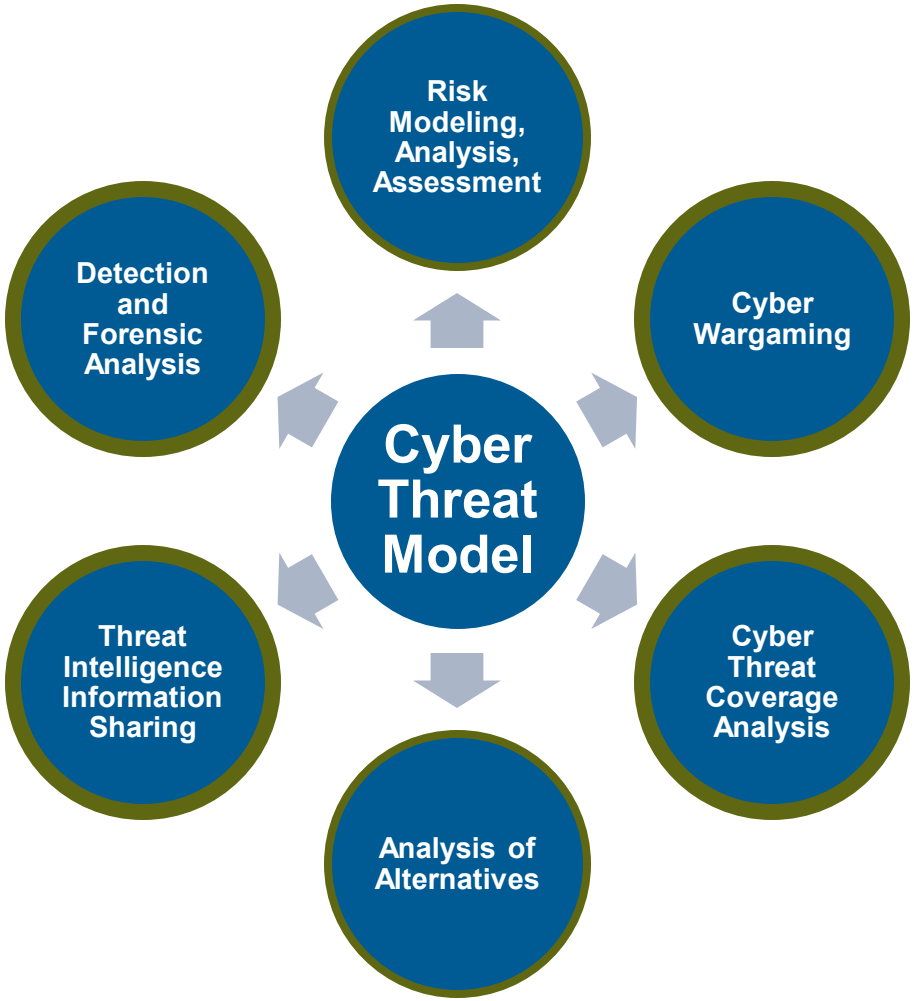
Consider **Cyber Effects** of **Threat Events**, to share information about artifacts and indicators

Consider adversary characteristics related to **intent** and **targeting**, to share information about **campaigns**

Consider potential effects on and coverage of **Threat Events**

Consider factors with, or determinant of, **Likelihood** or **Severity**

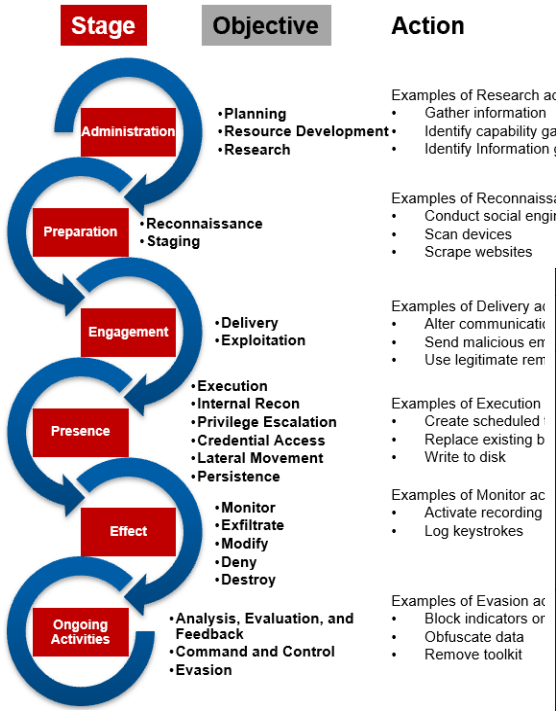
One Common Theme … Identify Threat Events Using a Framework Following the Structure of a Threat Scenario or Cyber Campaign



A variety of frameworks are available, including

- **Cyber Kill Chain™ framework**
- **NIST SP 800-30R1: cyber attack lifecycle (CAL) stages, representative events**
- **ATT&CK™**
- **ODNI Cyber Threat Framework**
- **NSA Technical Cyber Threat Framework V2**

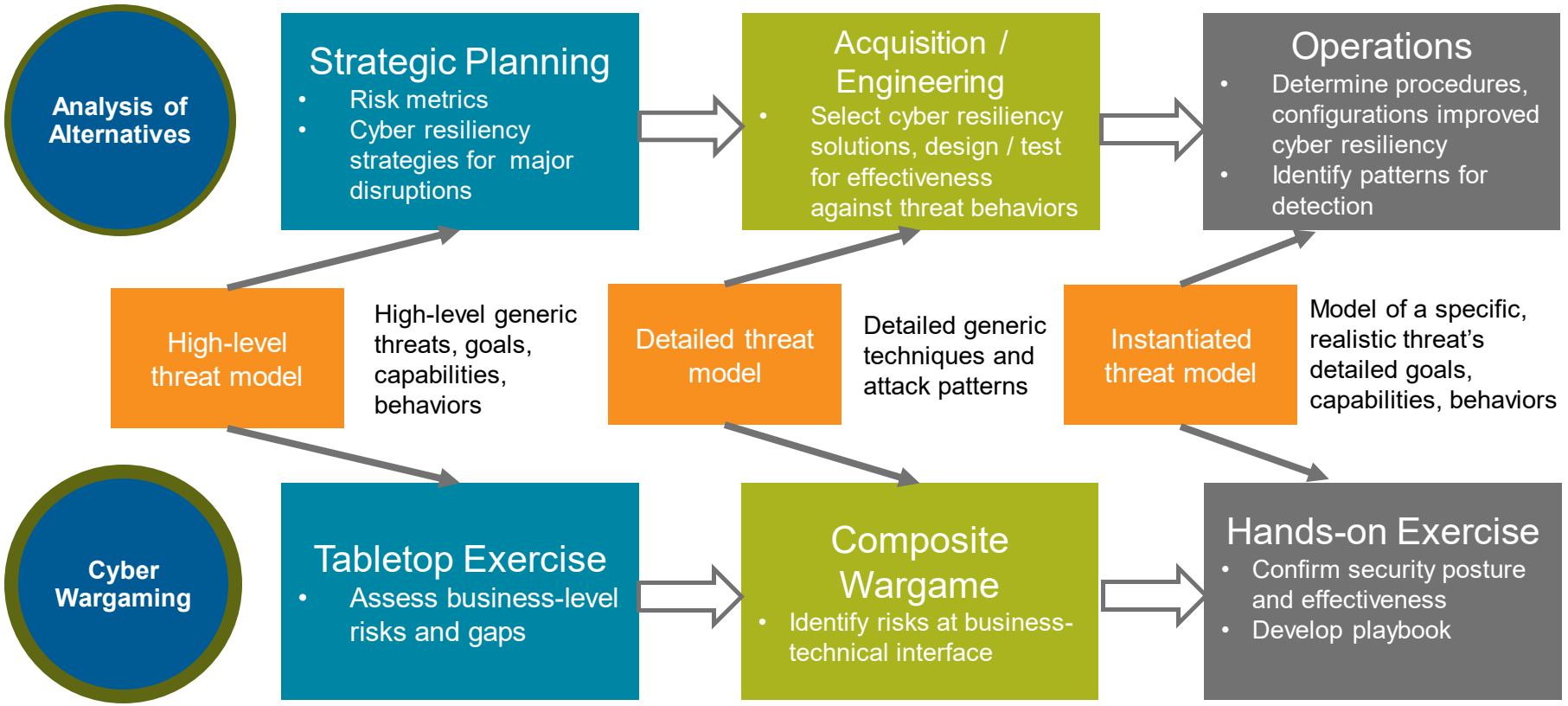
A Common Framework for Identifying Threat Events Supports Cyber Threat Coverage Analysis at Different Levels of Description



Example: Potential effects of cyber resiliency techniques and implementation approaches on adversary objectives, using the NSA Technical Cyber Threat Framework

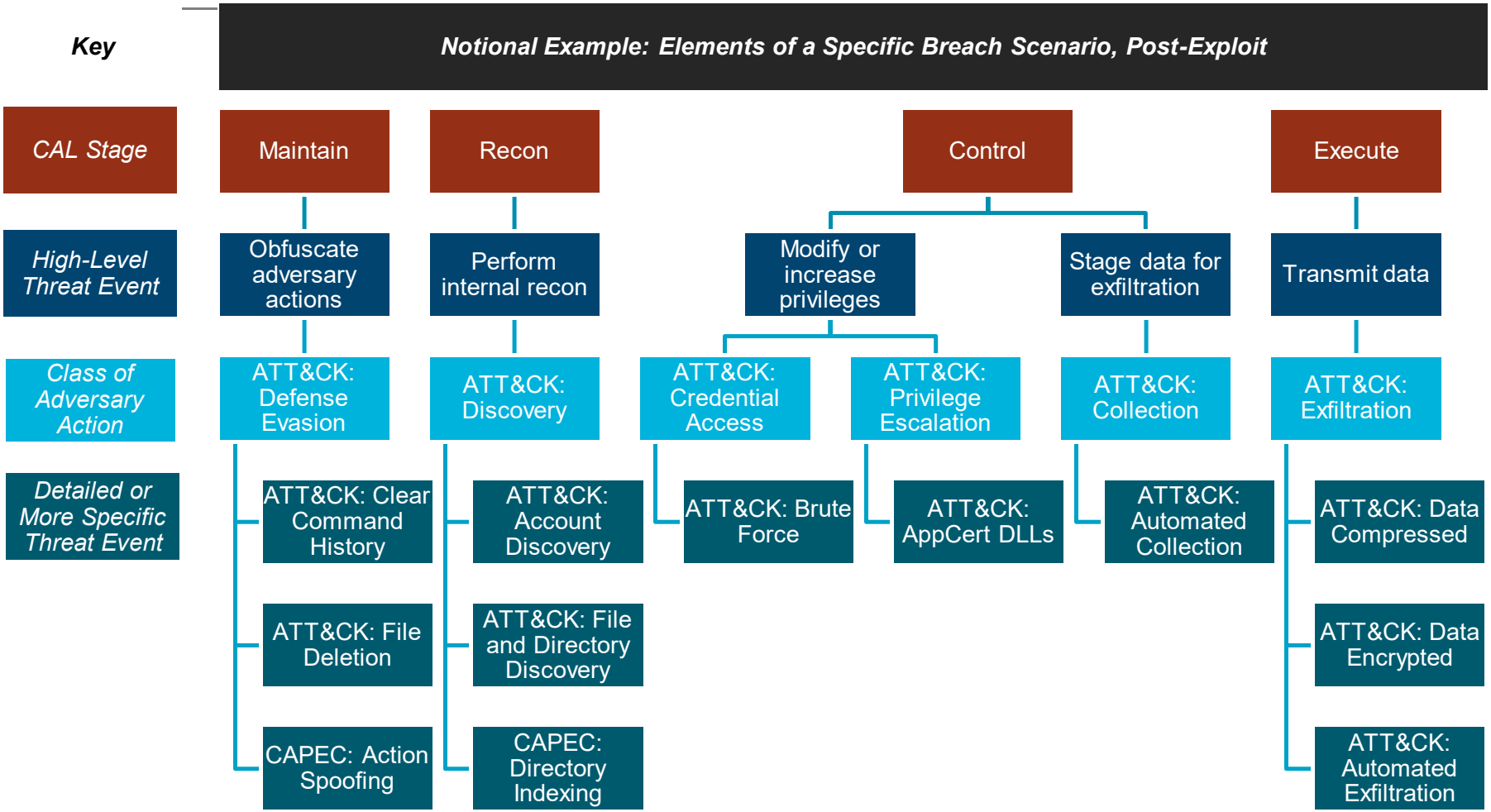
		PRESENCE Stage					
Cyber Resiliency Technique	**Objective → Implementation Approach**	**Execution**	**Internal Reconnaissance**	**Privilege Escalation**	**Credential Access**	**Lateral Movement**	**Persistence**
Adaptive Response	Dynamic Reconfiguration	Negate, Delay, Exert	Exert, Shorten	No effect	No effect	Contain	No effect
	Dynamic Resource Allocation	No effect	Delay, Exert, Shorten	No effect	No effect	No effect	No effect
	Adaptive Management	Delay, Preempt, Shorten, Reduce	No effect	Shorten, Reduce	No effect	No effect	Preempt, Negate
Analytic Monitoring	Monitoring & Damage Assessment	Detect	Detect	Detect	Detect	Detect	Detect
	Sensor Fusion & Analysis	Detect	Detect	Detect	Detect	Detect	Detect
	Forensic & Behavioral Analysis	Detect, Scrutinize, *Reveal*	Detect, Scrutinize, *Reveal*	Detect, Scrutinize, *Reveal*	Detect, Scrutinize, *Reveal*	Detect, Scrutinize, *Reveal*	Detect, Scrutinize, *Reveal*
Contextual Awareness	Dynamic Resource Awareness	No effect	No effect	No effect	No effect	No effect	No effect
	Dynamic Threat Awareness	*Detect*	*Detect*	No effect	No effect	*Detect*	*Detect*
	Mission Dependency & Status Visualization	No effect	No effect	No effect	No effect	No effect	No effect
Coordinated Protection	Calibrated Defense in Depth	Delay, Exert	No effect	Delay, Exert	Delay, Exert	Delay, Exert, Contain	No effect
	Consistency Analysis	No effect	No effect	Degrade, Exert	Degrade, Exert	No effect	Detect
	Orchestration	No effect	No effect	No effect	No effect	No effect	No effect
	Self-Challenge	Detect	Detect	Detect	Detect	Detect	No effect

A Common Framework for Identifying Cyber Threat Events Can Align Different Uses and Different Scales …



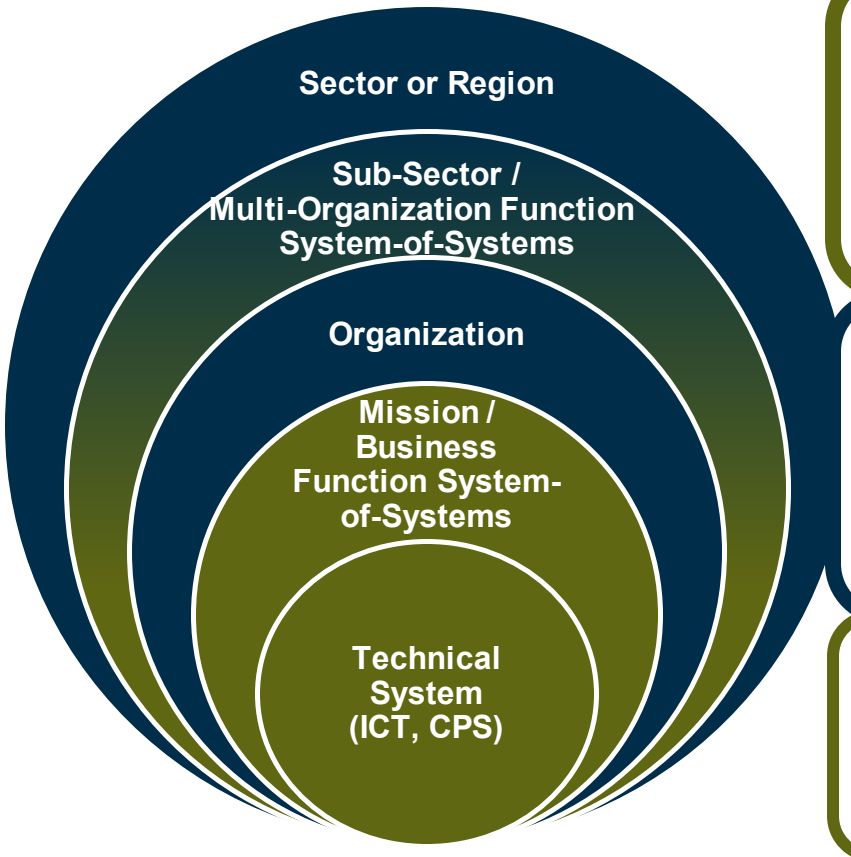
Example: Aligning Analysis of Alternatives and Cyber Wargaming within an organization

… As Long as the Threat Modeling Framework Supports Refinement and Decomposition …



Example: Refining a notional threat scenario

… As Well as Extension to Systems-of-Systems Beyond a Single Organization



- Identify systemic cyber risks, cyber resiliency gaps, and risk governance issues
- Identify gaps in
  - Widely-deployed / sector-standard technologies and practices
  - Threat and incident information sharing
- Develop cyber wargames to promote cross-organizational efforts

- Identify enterprise cyber risks, cyber resiliency gaps, and risk governance issues
- Identify gaps in
  - Cybersecurity and resilience technologies and practices
  - Cyber playbooks and Security Operations Center capabilities
- Develop cyber wargames involving threats to the enterprise

- Identify gaps in
  - Cybersecurity and resilience technologies and practices
  - COOP and contingency planning
- Develop cyber wargames involving threats to accomplishing the mission or business function

Example of uses of threat scenarios involving systems-of-systems

Conclusion

- **Any discussion of risk overlaps with or impinges on discussions of other topics … particularly resilience**
- **Analysis of cyber risk – and of cyber resiliency – informs and can be informed by a variety of other activities, including**
  - Threat intelligence information sharing
  - Cyber wargaming
  - Analysis of alternatives for strategies, system design, operations
- **Use of a common threat modeling framework can bring consistency to these activities, both within an enterprise and beyond**

For More Information …

- https://www.mitre.org/publications/technical-papers/next-generation-cyber-infrastructure-apex-program-publications
- **Publications in this collection include:**
  - Cyber Threat Modeling: Survey, Assessment, and Representative Framework
  - Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context
  - Advanced Cyber Risk Management: Threat Modeling & Cyber Wargaming Briefing
  - Enhanced Cyber Threat Model for Financial Services Sector Institutions
  - Enterprise Threat Model Technical Report-Cyber Threat Model for a Notional Financial Services Sector Institution
  - System-of-Systems Threat Model
  - Cyber Risk Metrics Survey, Assessment and Implementation Plan Report
  - Cyber Risk Metrics Survey, Assessment and Implementation Plan Briefing
  - Financial System Mapping
  - Dynamic Data Map Technical Report
- https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf

MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org

MITRE Approved For Public Release Distribution Unlimited Case Number PRS_18_2010-10

Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, *Head of Risk Information & Insurance, ORX*
- **Deborah Bodeau**, *Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation*
- **Todd Waszkelewicz**, *Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York*
- **Trevor Watkins**, *Risk & Control Manager, PNC*
- **Albert Olagbemiro**, *Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond*

Cyber Risk Workshop: Risk Identification

Federal Reserve Bank of Richmond – Charlotte Branch

Todd Waszkelewicz
Federal Reserve Bank of New York; Supervision Group – Cybersecurity Policy

March 28, 2019

Disclaimer

- The views that I express are my own and do not necessarily represent those of the Federal Reserve Bank of New York or the Federal Reserve System.

Strengthening Risk Identification

Ongoing priorities

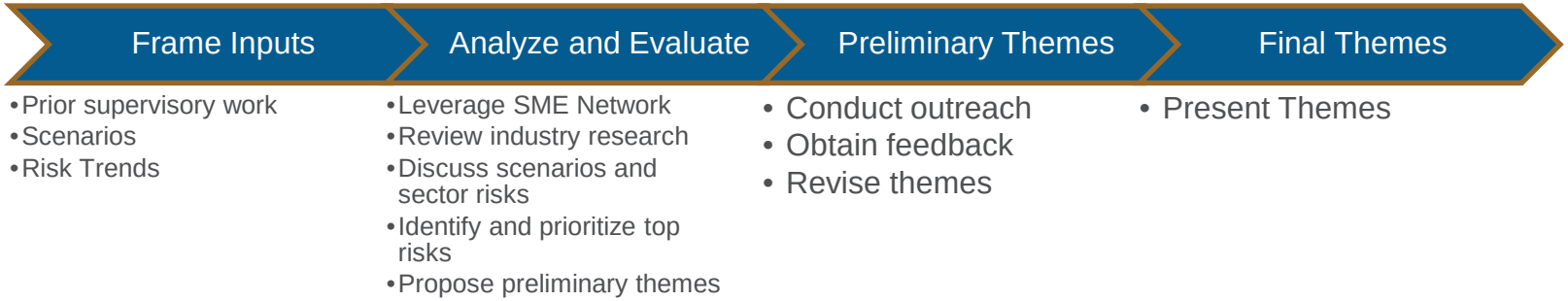
- Enhancing abilities to assess the impact of current and future cybersecurity events in the financial sector
  - Support supervisory staff in identifying, assessing and monitoring cyber risks
  - Support supervisory leaders in making data-driven decisions to better allocate policy priorities, examination focus and resources to the top risks affecting the financial sector
  - Strengthen context and understanding in response to cyber events

Examples of key initiatives to strengthen cyber risk identification

- Scenarios analysis to better contextualize cyber risks
- Mapping of financial sector interconnectedness

Scenario Analysis

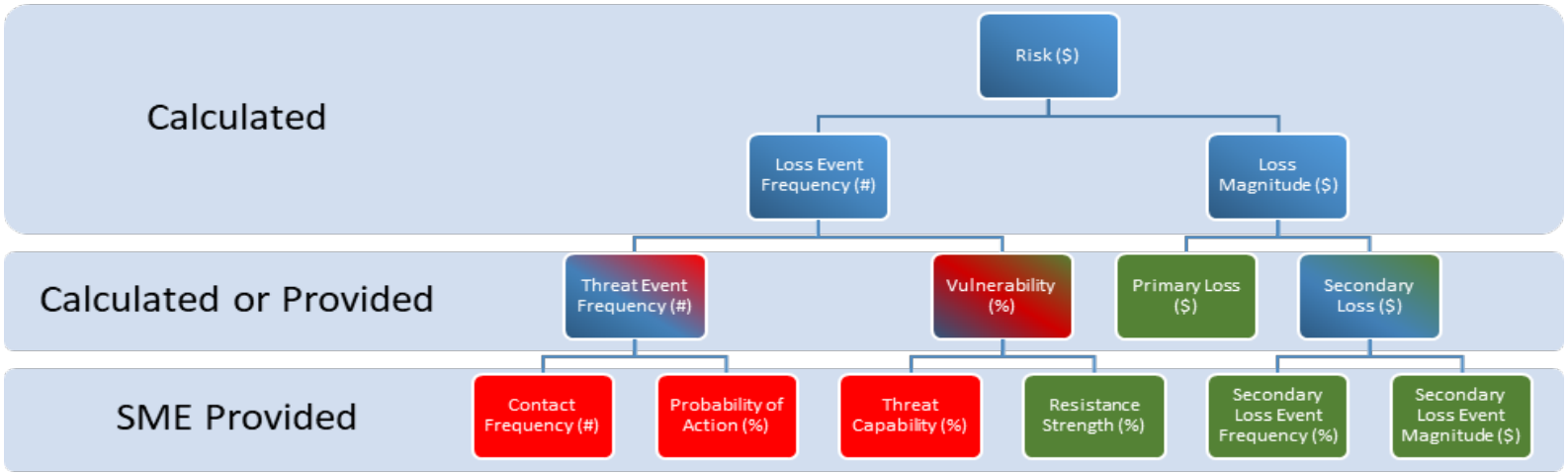
- Risk analysis process to identify top risks and develop cybersecurity supervisory themes for the next supervisory cycle



- One component of the process is to conduct scenario analysis to identify and prioritize top risks
- Utilize industry framework to estimate risks (e.g., Factor Analysis of Information Risk (FAIR))
- Enumerate plausible and concerning cybersecurity-related risk scenarios for the U.S. financial sector
- Leverage SMEs to estimate the likelihood and impact for each risk scenario using the FAIR framework
- Associate control categories related to preventing and mitigating the highest ranking scenarios
- Develop supervisory themes that incorporate the related control areas adjusting for other inputs

Why use an Industry framework such as FAIR

Factor Analysis of Information Risk (FAIR)



- Helps achieve a central objective of identifying, evaluating and comparing cybersecurity risk events
- Provides a common framework and language for SMEs to use in estimates
- No need for additional tools/software to use the methodology
- Gaining traction in industry

Mapping Financial Sector Interconnectedness

- Financial Services Sector is highly interconnected and interdependent which increases its attack surface and the proliferation of cyber risks

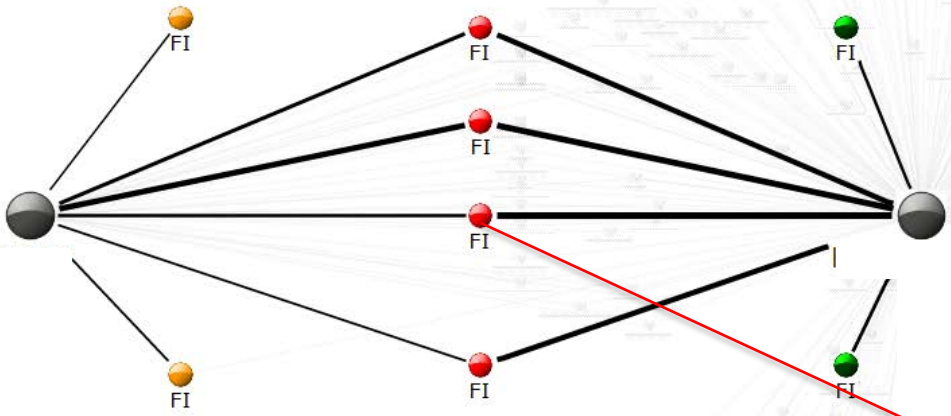
- Risk to critical functions and systems continue to build as sophistication and focus of threat actors increases

- Establishing a data-driven analytical capability to map interconnectedness and assess impact of cybersecurity risks in the financial sector
  - Map and visualize the interconnectedness of critical financial markets
  - Enhance analytical capabilities to identify and assess vulnerabilities and implications
  - Strengthen context and understanding in response to cyber events

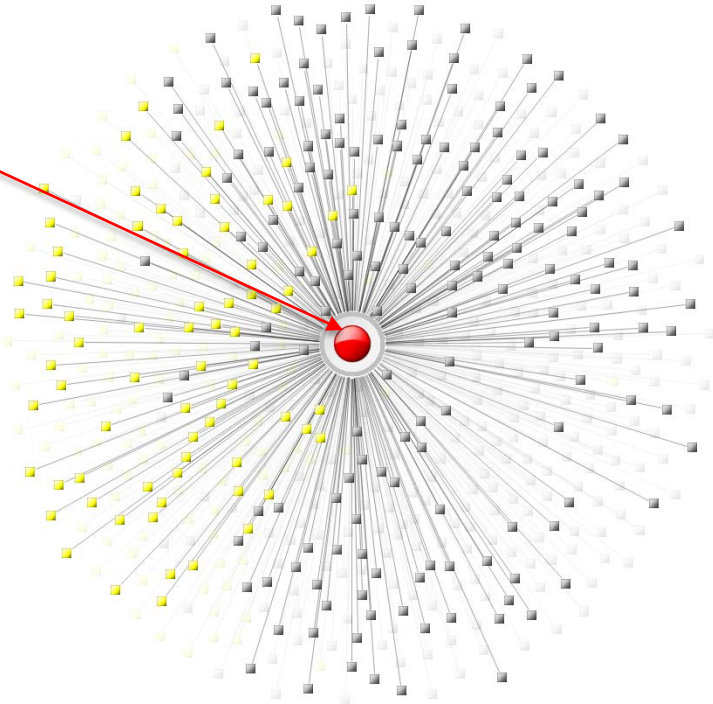
- We are aiming to answer questions such as:
  - What is the potential impact of a particular cyber event or scenario on a firm or critical financial market?
  - What are the interdependencies or concentrations that could pose risk?
  - What are the areas of greatest concern?

Analyzing the breadth, depth and complexity of Interconnectedness

Identifying key players

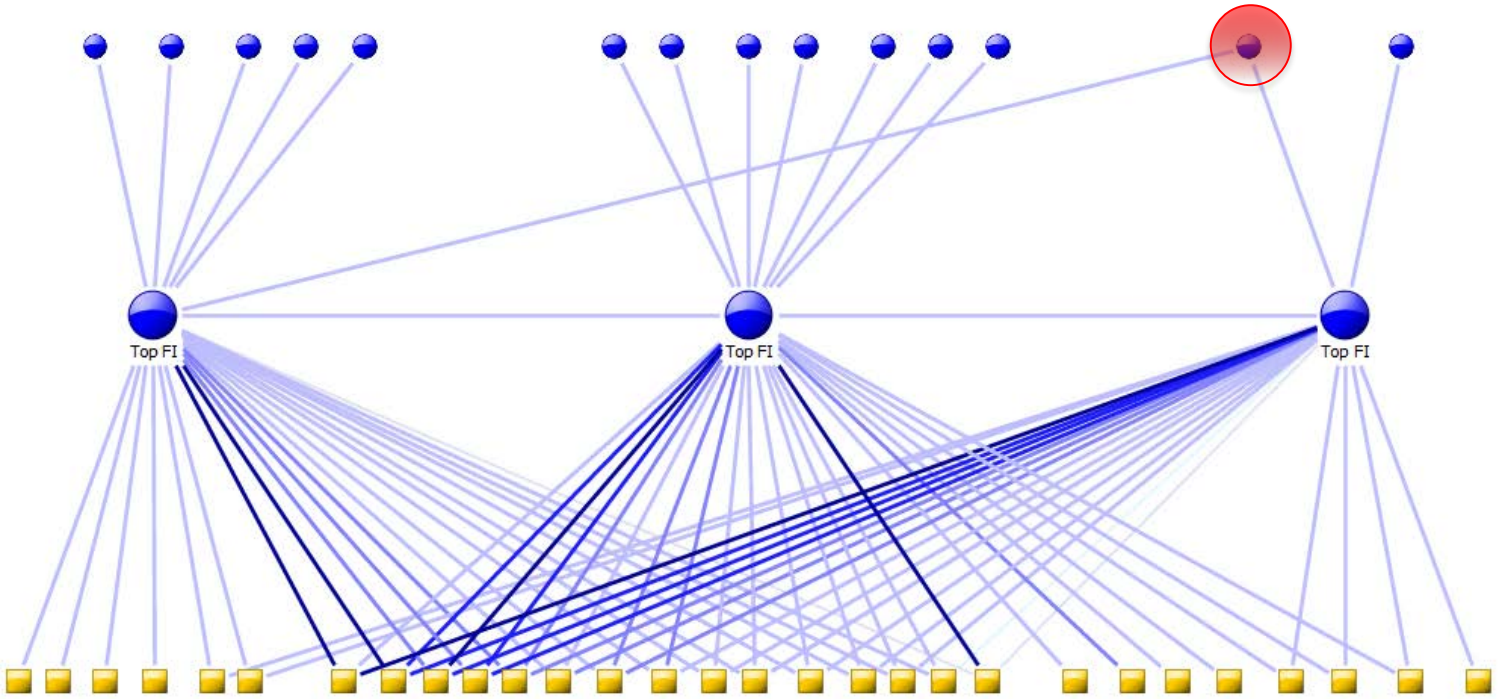


Identifying key financial market utilities and agents supporting a key player



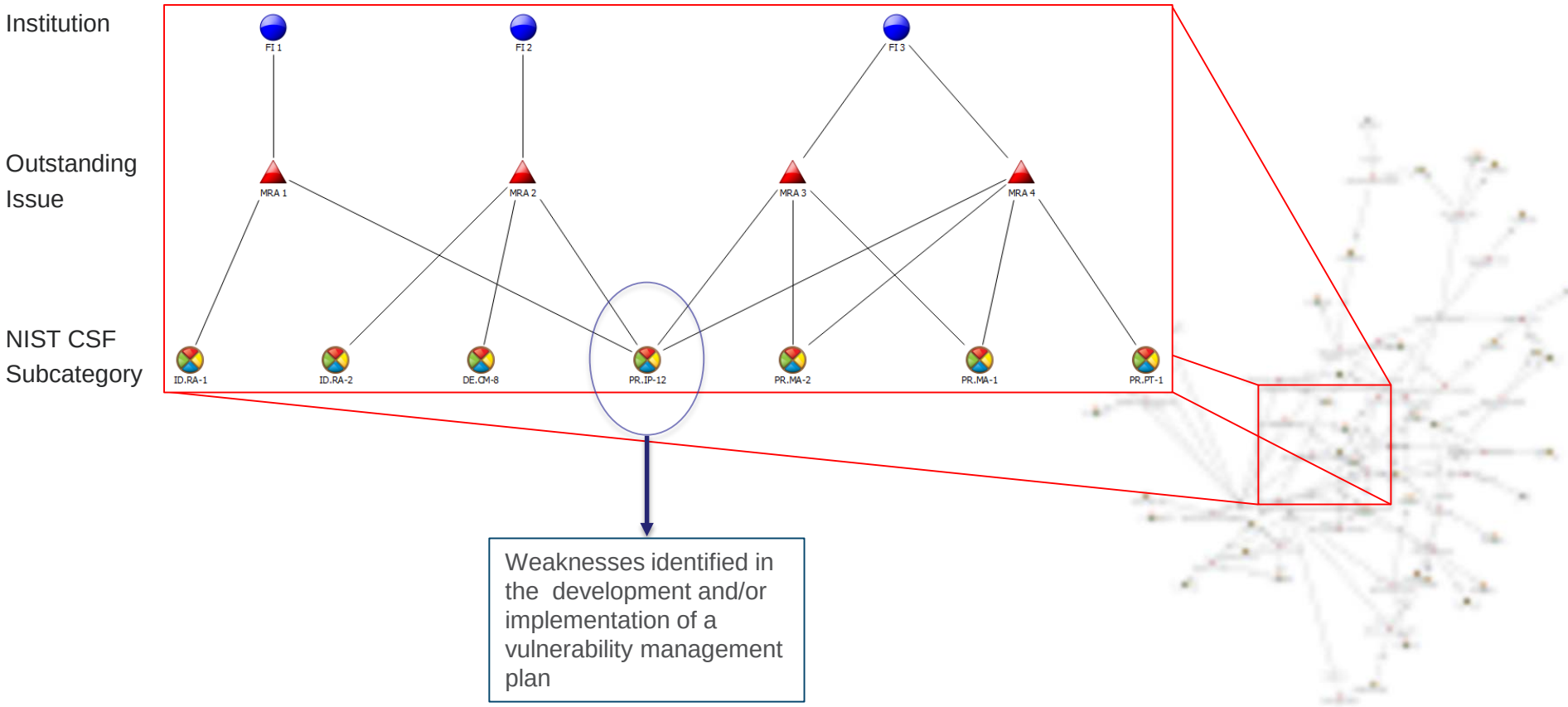
Identifying key dependencies

- Key agent dependency across two top players in a critical financial market



Identifying patterns in risk

- Relate supervisory issues to common industry frameworks (e.g., NIST Cybersecurity Framework (CSF)
- Data for three top players show an overlap in supervisory criticisms related to information protection; in particular, vulnerability management
- Collectively, these firm accounted for xx% of value of a critical financial market



Summary

- Interconnectedness mapping and analysis enables us to bring together disparate data sources (e.g., organizational, supervisory and transactional data) into one analytic platform to identify concentrations of risk and potential impact of cyber risks

- Scenario analysis helps us to drive supervisory focus to top risks in the financial sector

Panel #1: Identification and Classification of Cyber Risk

- **Steve Bishop**, *Head of Risk Information & Insurance, ORX*
- **Deborah Bodeau**, *Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation*
- **Todd Waszkelewicz**, *Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York*
- **Trevor Watkins**, *Risk & Control Manager, PNC*
- **Albert Olagbemiro**, *Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond*

Cyber Risk Workshop

Identification and Classification

Who We Are

- Overview and Background
  - PNC is one of the largest diversified financial services institutions in the United States
  - Employees in more than 40 states across the country
  - Regional presidents in 39 market
  - A retail branch network stretching across 19 states and the District of Columbia
  - Strategic international offices in Canada, China, Germany and the U.K.

The PNC Operational Risk Framework

- PNC's definition of Operational Risk closely aligns to the BASEL definition and defines risk arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.
- PNC follows an Operational Risk Framework that layers into an Enterprise Risk Management Framework ensuring the management of risk is consistent across PNC.
- PNC has classified all risks into risk categories known as risk taxonomy.

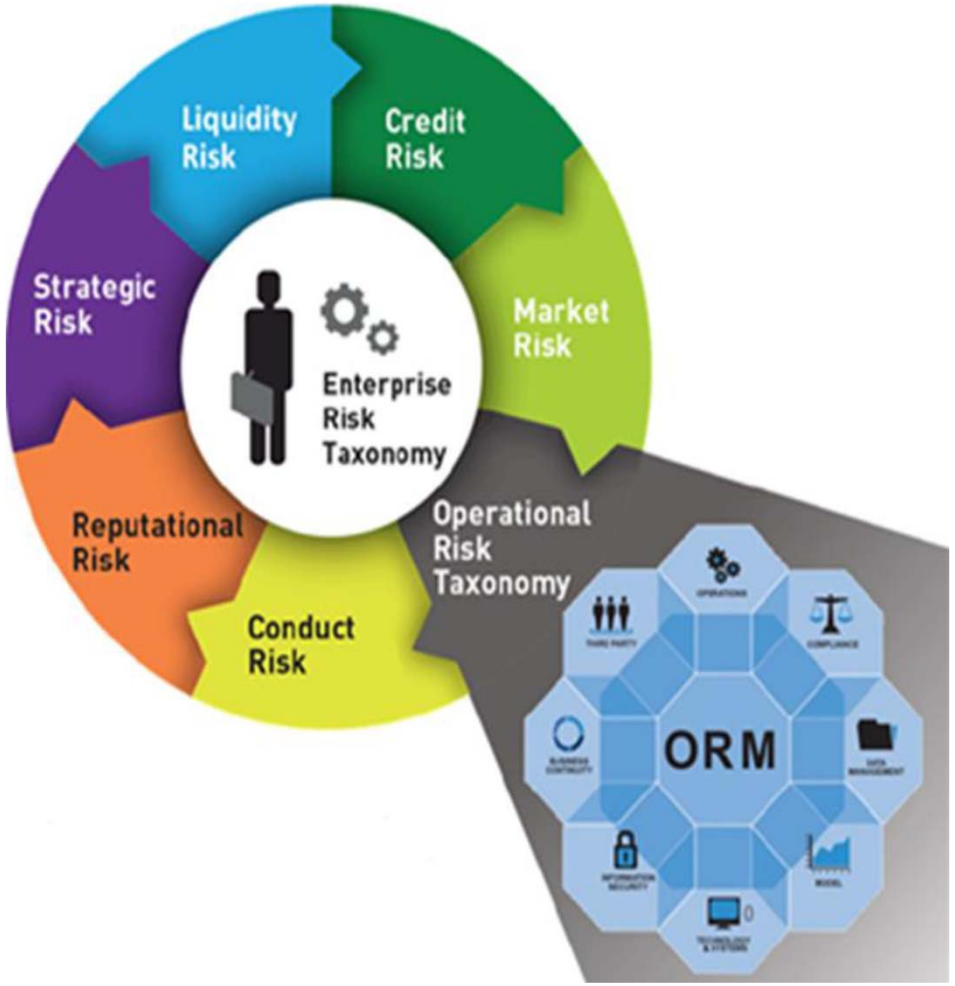


Figure 1: Risk Taxonomies

PNC Operational Risk Domains

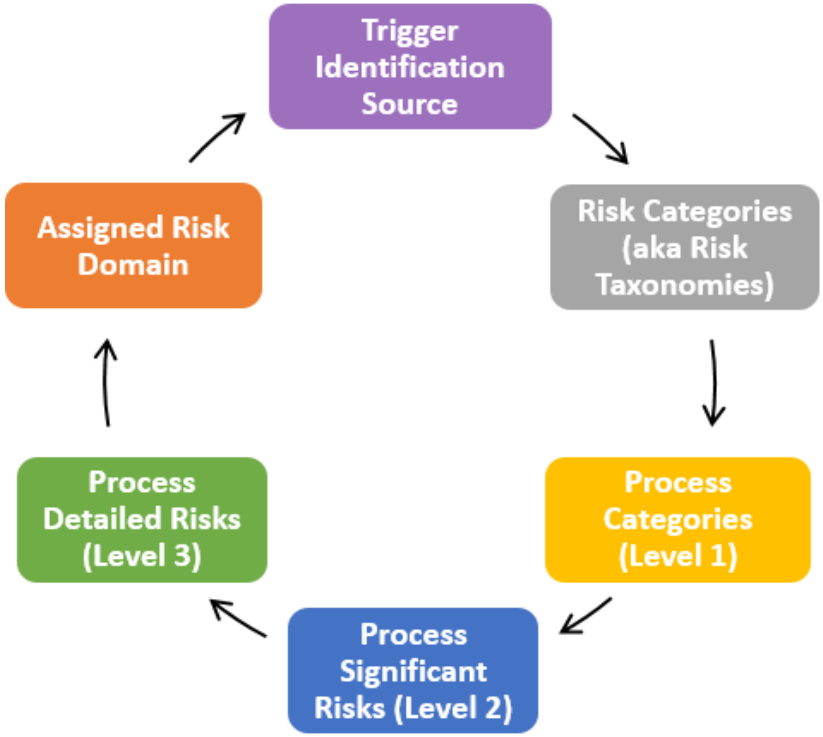
Icon	Domain	Focused on managing:
	Operations *(People/ Processes)*	Risk resulting from inadequate or failed internal processes, misconduct or errors of people and fraud
	Compliance	Risk associated with failure to comply with applicable laws and regulations or contractual obligations
	Data Management	Risk associated with incomplete or inaccurate data
	Model	Risk associated with the design, implementation, and ongoing use and management of a model
	Technology & Systems	Risk associated with use, operation and adoption of technology
	Information Security	Risk resulting from the failure to protect information and ensure appropriate access to, and use and handling of information assets
	Business Continuity	Risk of potential disruptive events to business activities
	Third Party	Risk arising from failure of third party providers to conduct activity in a safe and sound manner and in compliance with contract provisions, applicable laws and regulations

Identification and Classification of Cyber Risk

Identification through Trigger Events

- External Loss Data (ELD)
  - ✓ The review of loss events experienced by other institutions for applicability to PNC
  - ✓ Analysis of root cause and trends
  - ✓ Proactive approach to risk and control enhancement through a systematic process
- Internal Loss Data (ILD)
  - ✓ Expenses associated with an operational loss event
  - ✓ Capture and analyze ILD root causes and trends to improve ORM capabilities
- Issues
  - ✓ Failure of a control or lack of a control
  - ✓ Determine corrective action or resolution
  - ✓ Lifecycle
    - o Identification and Investigation
    - o Action Planning and Management Response
    - o Monitoring and Reporting
    - o Resolution

Classification



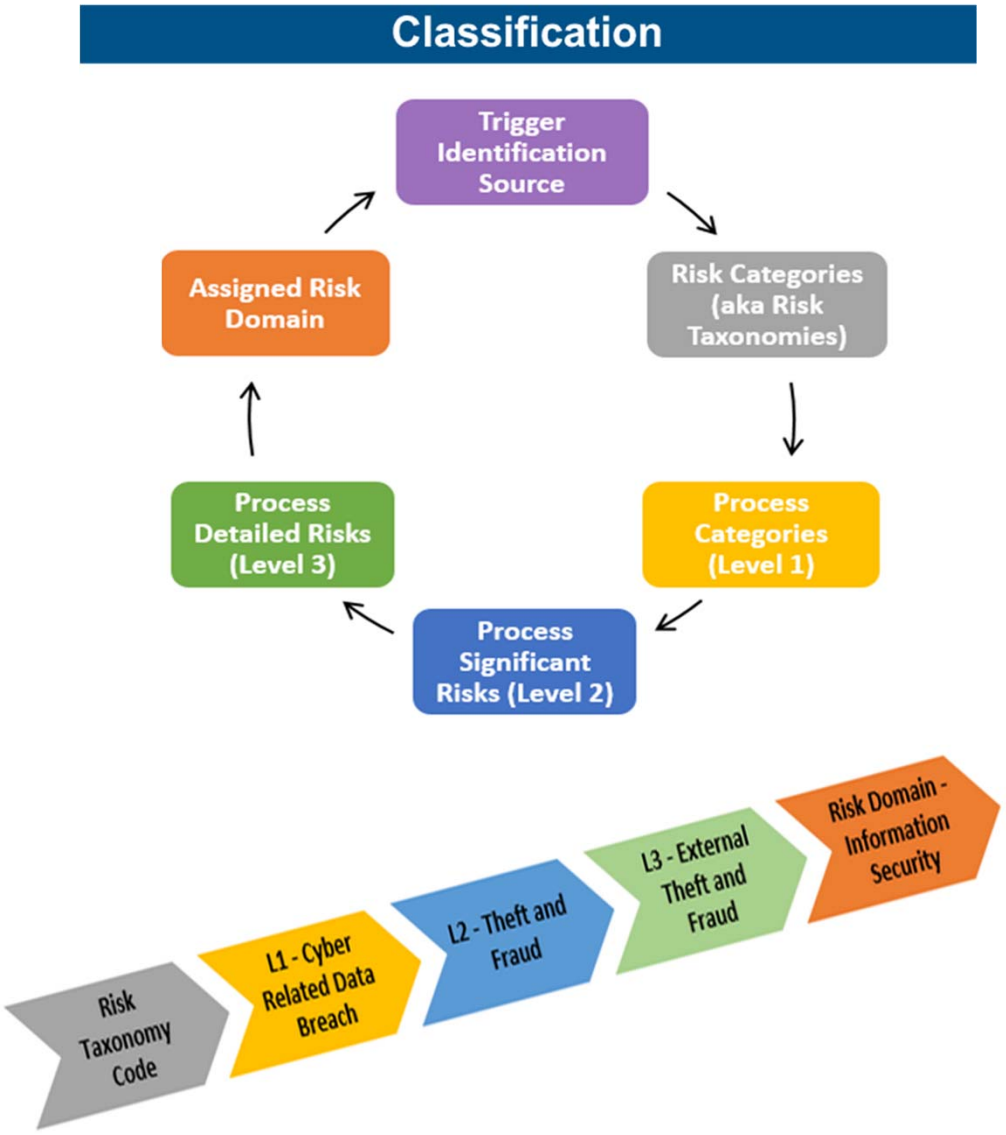
ELD Examples

BankIslami loses PKR 2.6 million after cyberattack on payment card network.

On 29 October 2018, it was reported that PKR 2.6 million (USD 19,000, EUR 17,000) had been stolen from BankIslami customer accounts after hackers compromised the bank's international payment card network and conducted debit card transactions.

According to BankIslami, the cyberattack was a coordinated attack against the payment network of its international payment scheme and the payment networks of the acquiring banks, the News International reports. One source told Profit that "there is a clear breach of information at BankIslami's part" and a digital copy of BankIslami customers' credit card information may have been leaked to hackers.

The bank has informed Pakistan's central bank of the attack, which instructed BankIslami to advise customers on precautionary measures to take, and engaged information security experts. BankIslami restored all domestic ATM cash withdrawals using biometric services on 27 October 2018, but as of 28 October 2018 was yet to restore transactions routing through its international payment scheme.



ELD Examples

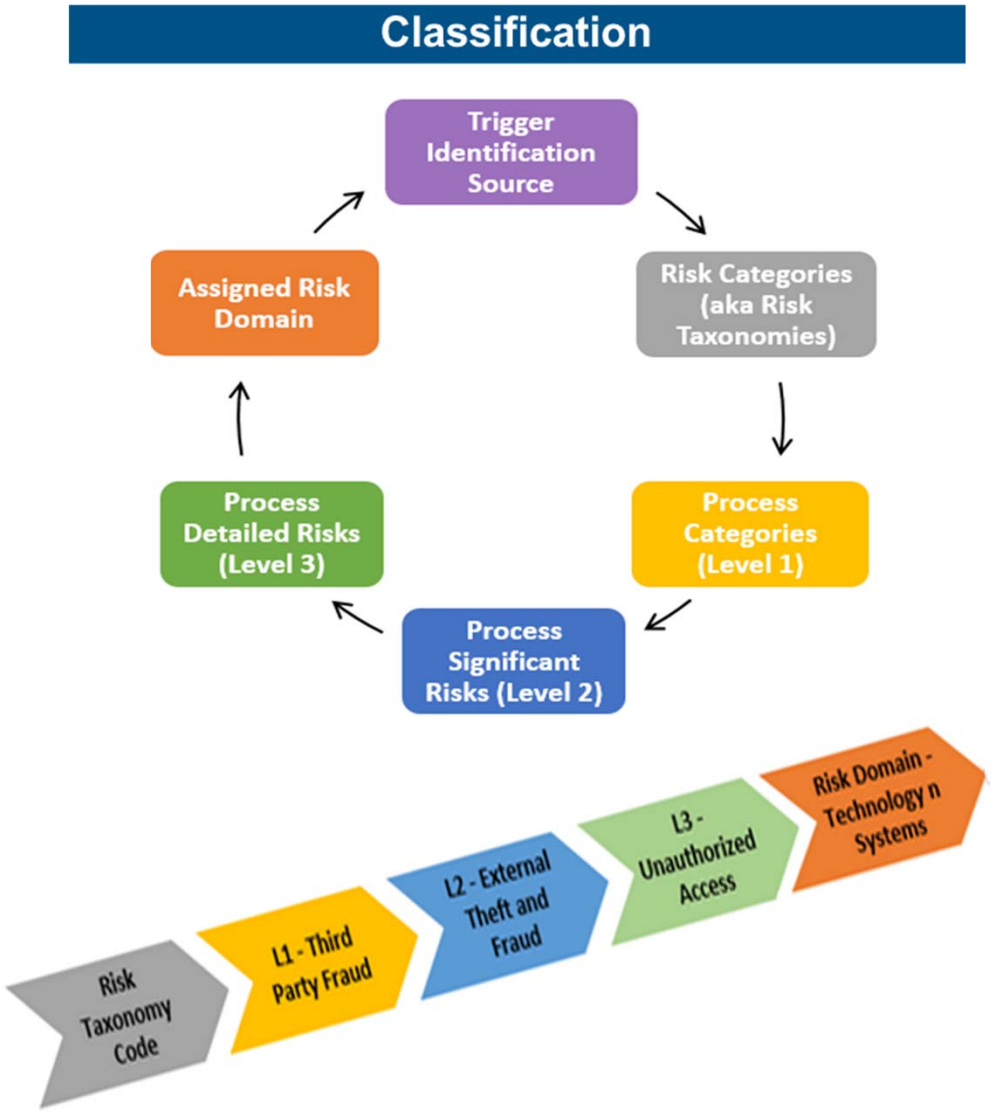
Over 77 million T-Mobile customer account PINs exposed due to Apple website security flaw

On 24 August 2018, Buzzfeed News reported that a security flaw in Apple's online store had inadvertently exposed over 77 million T-Mobile customer account PINs, which often constitute the last four digits of a customer's Social Security Number (SSN).

When purchasing an iPhone through Apple's online store, customers are prompted to select a carrier and monthly payment plan. If T-Mobile is selected, customers are redirected to an authentication page which asks for their T-Mobile phone number and account PIN or the last four digits of their SSN.

The T-Mobile authentication page did not limit the number of entry attempts. This meant that hackers could use widely-available hacking software to repeatedly enter random combinations of numbers to guess the customer's PIN, a method known as a brute-force attack.

Ceraolo stated that the vulnerability was most likely caused by an engineering mistake made when connecting T-Mobile's account validation application programming interface (API) to Apple's website. The API allows Apple access to T-Mobile's customer data in order to validate customer logins. If a hacker obtains an account PIN in combination with the correct phone number, they would then be able to pose as the genuine customer to "hijack" the SIM card by contacting the carrier and requesting that calls and texts are transferred to another phone number.



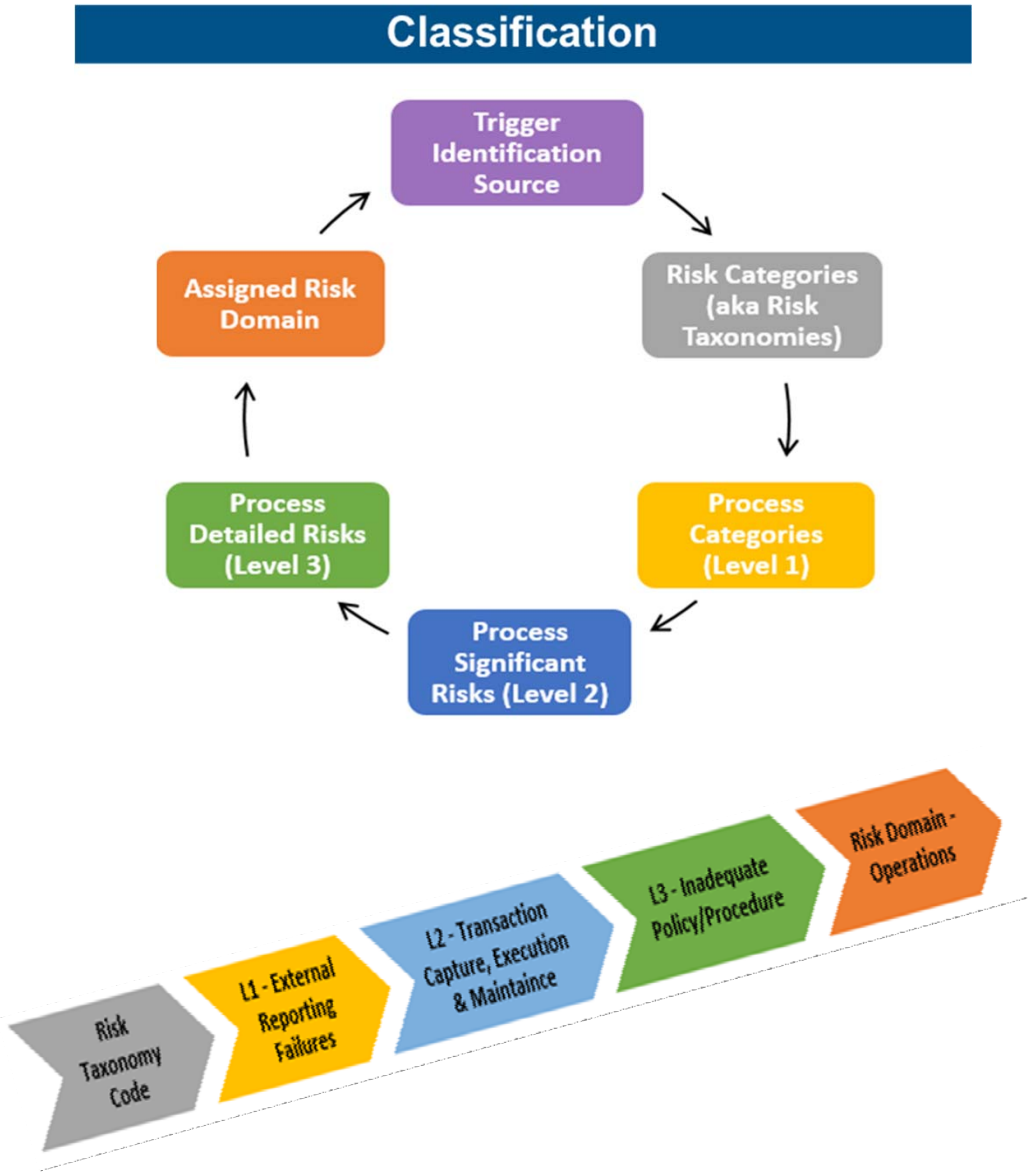
ELD Examples

CBA unable to locate 19.8 million customer records after third party fails to confirm it destroyed them

Commonwealth Bank of Australia (CBA) has been unable to locate two magnetic data tapes containing the records of 19.8 million customers after a subcontractor failed to provide documentation that it had destroyed them.

Buzzfeed names the subcontractor as Fuji Xerox, which in 2016 decommissioned the data centre where CBA customer data was stored. The tapes were due to be destroyed, but on 9 May 2016 the bank had not received documentation to confirm this had taken place.

Subsequently, on 20 May 2016, CBA informed the Office of the Australian Information Commissioner (OAIC) and the Australian Prudential Regulation Authority (APRA) that it was unable to locate the tapes. The magnetic data tapes were used to print bank statements and contained names, addresses, account numbers and transaction details from between 2000 and 2016. According to CBA, the tapes did not contain passwords, personal identification numbers (PIN) or other data that could enable fraud.



Discussion & Questions

Break

- Panel #2 starts at 11:15.
- Restrooms are located to your left as you exit the conference room.

Panel #2: Measurement and Impact of Cyber Risk

- **Gilles Hilary**, *Chaired Professor, Georgetown University*
- **Patrick Naim**, *CEO, Elseware*
- **Denyette DePierro**, *Vice President, Center for Payments and Cybersecurity, American Bankers Association*
- **Phil Collett**, *Director Cyber Risk Assessments, American Express Co.*
- **John DeLong**, *Risk Management, Morgan Stanley*
- **Filippo Curti**, *Financial Economist, Quantitative Supervision & Research, Federal Reserve Bank of Richmond*

Cyber-Incidents & Measurement

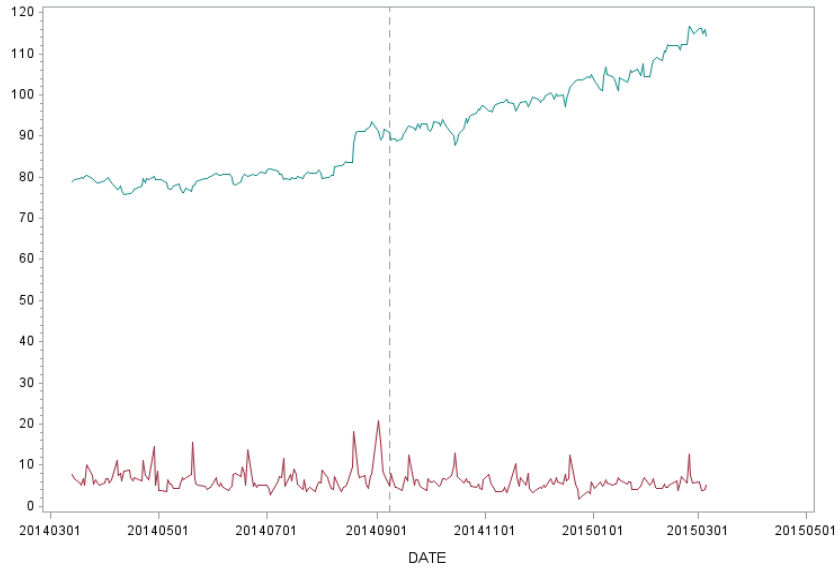
Presented by: Gilles HILARY

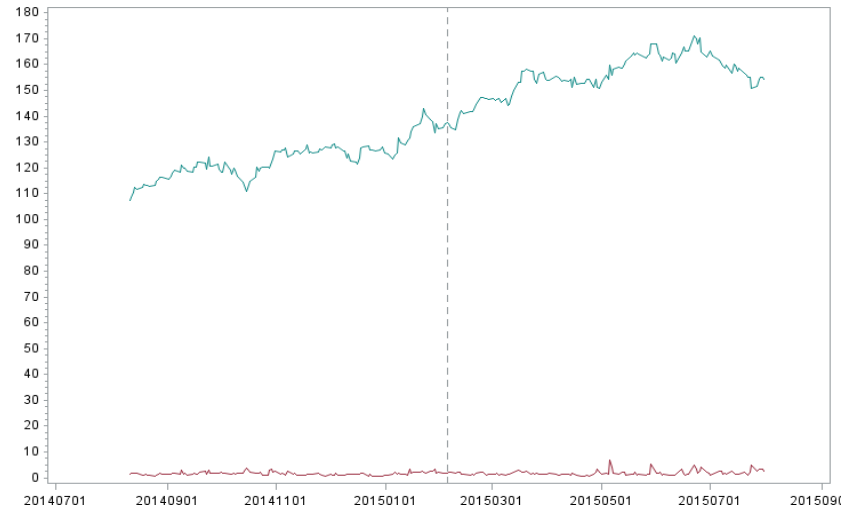
gilles.hilary@georgetown.edu

GEORGETOWN UNIVERSITY
McDonough SCHOOL of BUSINESS


PRICE($ PER SHARE), VOLUME (MM SHARES)
40
30
20
10
0
20140501
20140701
20140901
20141101
20150101
20150301
20150501
20150701
DATE
PRICE
Vol_MM


80
70
60
50
40
30
20
10
0
20130501
20130701
20130901
20131101
20140101
20140301
20140501
201407


120
110
100
90
80
70
60
50
40
30
20
10
0
20140301
20140501
20140701
20140901
20141101
20150101
20150301
20150501
DATE

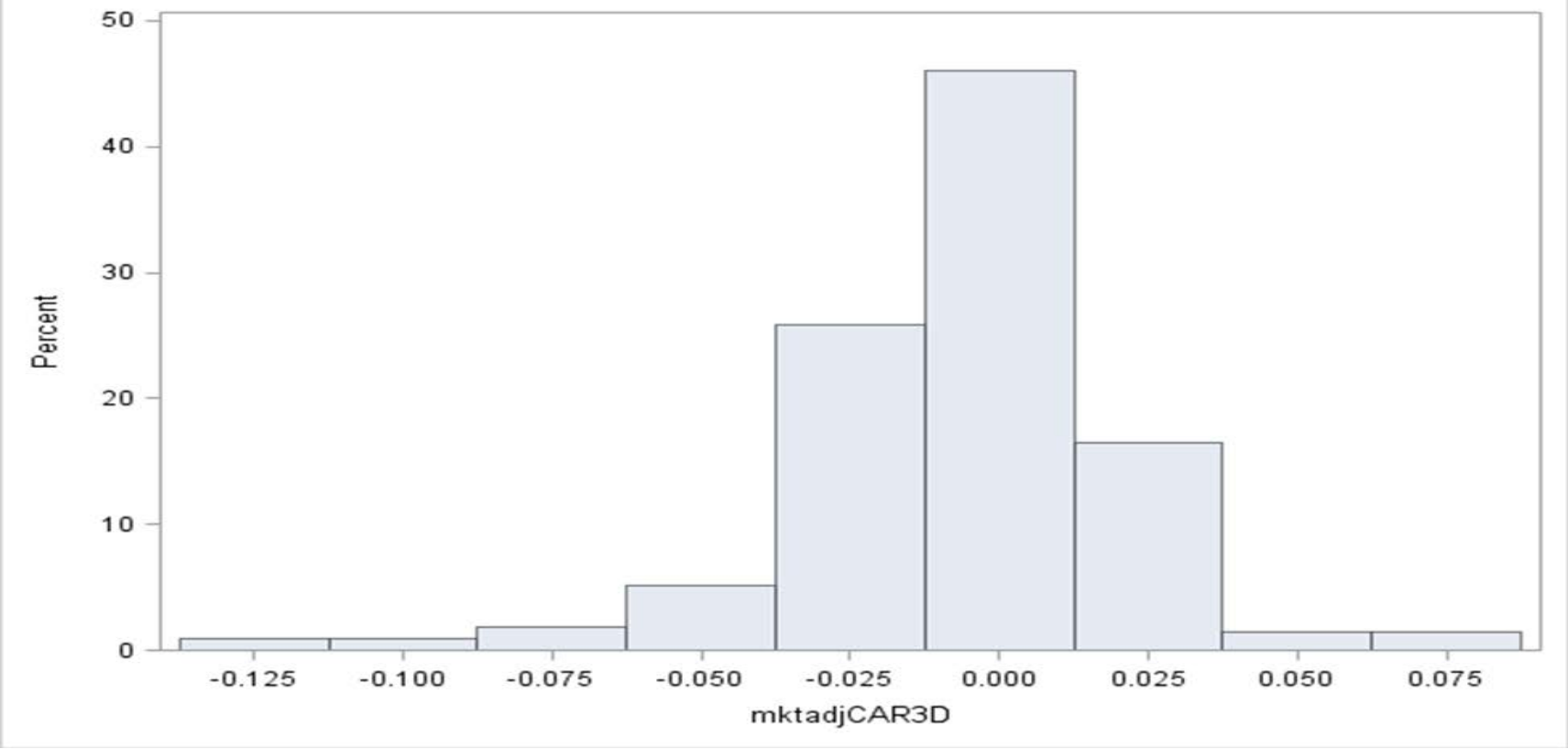

180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
20140701
20140901
20141101
20150101
20150301
20150501
20150701
201509


50
40
30
20
10
0
20160301
20160401
20160501
20160601
20160701
20160801
20160901
20161001
201611
DATE

ST Return Distribution

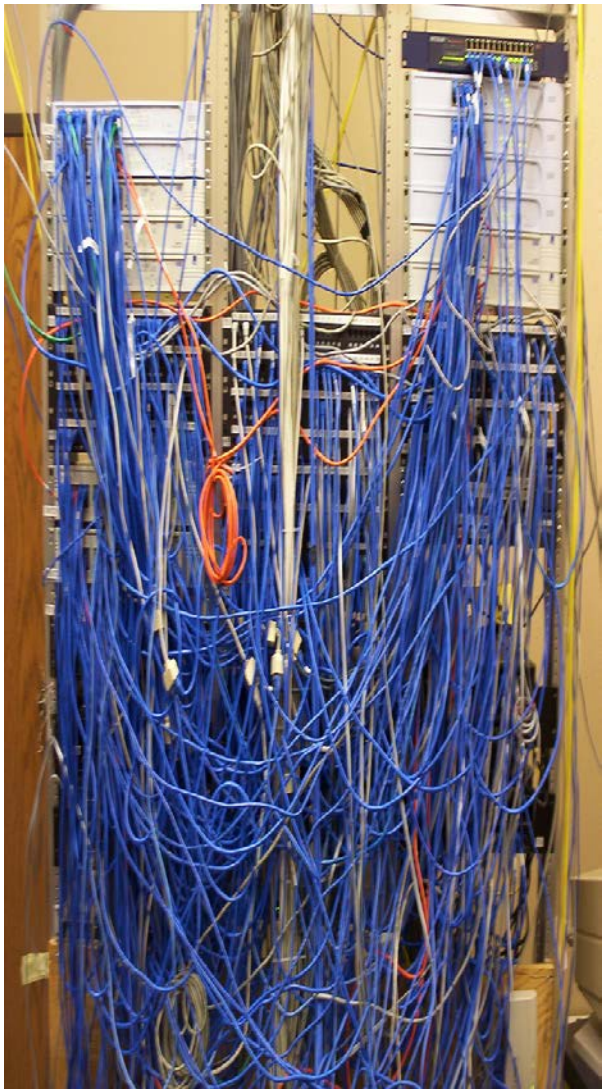
Median: -0.5%

Mean: - 0.7%

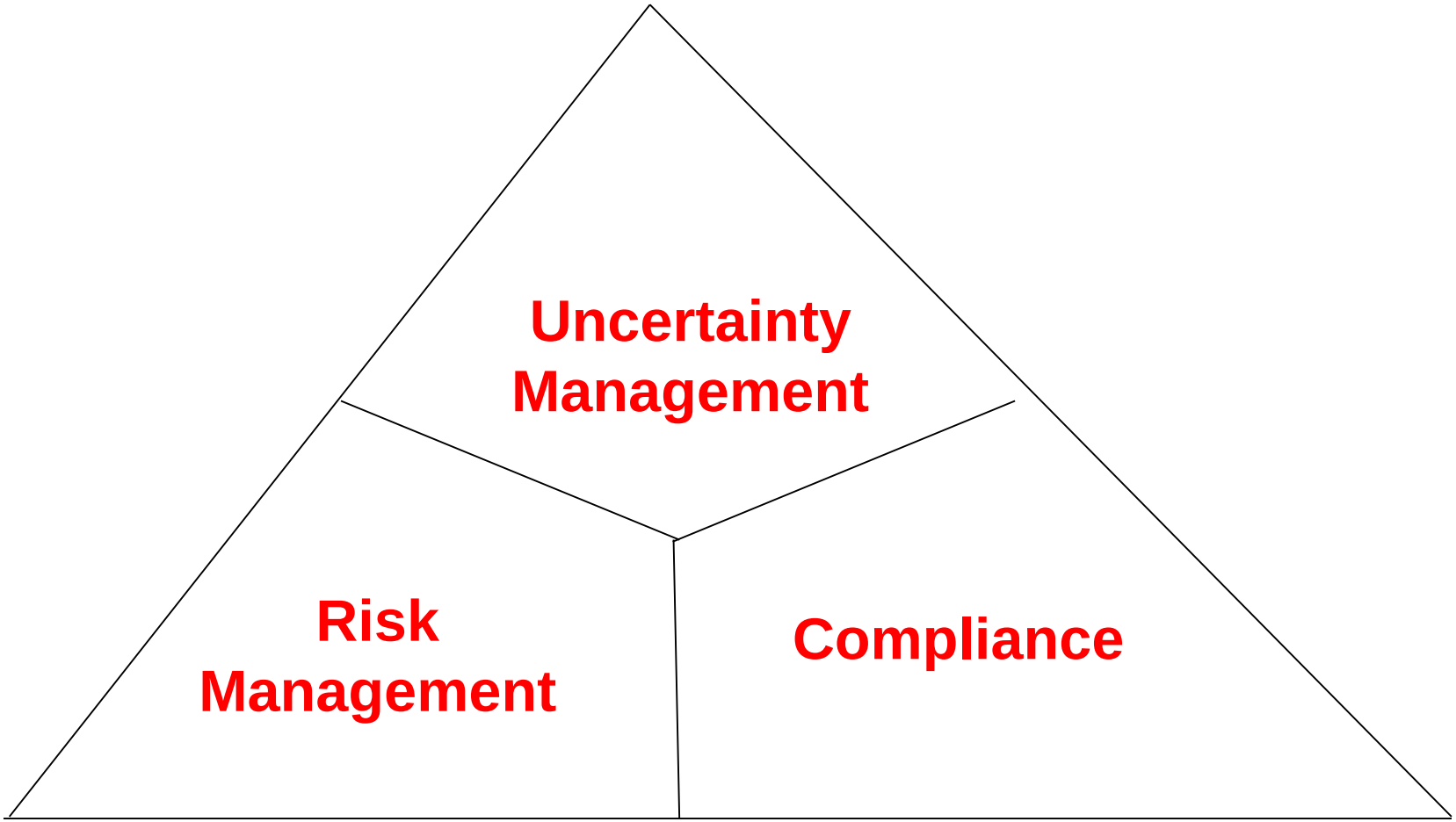



Vol (20)
10.818K
8.653K
45.500
45.000
44.500
44.000
43.500
43.000
42.500
42.000
41.460
41.000
40.500
40.000
39.500
39.000
38.500
38.000
Déc
2019
16
Févr
15
Mars
18
Avr


AMERICAN ROSE SOCIETY
MINIATURE
ROSE TEST GARDEN



FUD vs CURe



Thank You !

Gilles.Hilary@georgetown.edu

Panel #2: Measurement and Impact of Cyber Risk

- **Gilles Hilary**, *Chaired Professor, Georgetown University*
- **Patrick Naim**, *CEO, Elseware*
- **Denyette DePierro**, *Vice President, Center for Payments and Cybersecurity, American Bankers Association*
- **Phil Collett**, *Director Cyber Risk Assessments, American Express Co.*
- **John DeLong**, *Risk Management, Morgan Stanley*
- **Filippo Curti**, *Financial Economist, Quantitative Supervision & Research, Federal Reserve Bank of Richmond*

Assets, Access and Attackers

A consistent framework for identification, assessment, peer benchmarking and mitigation of cyber risk

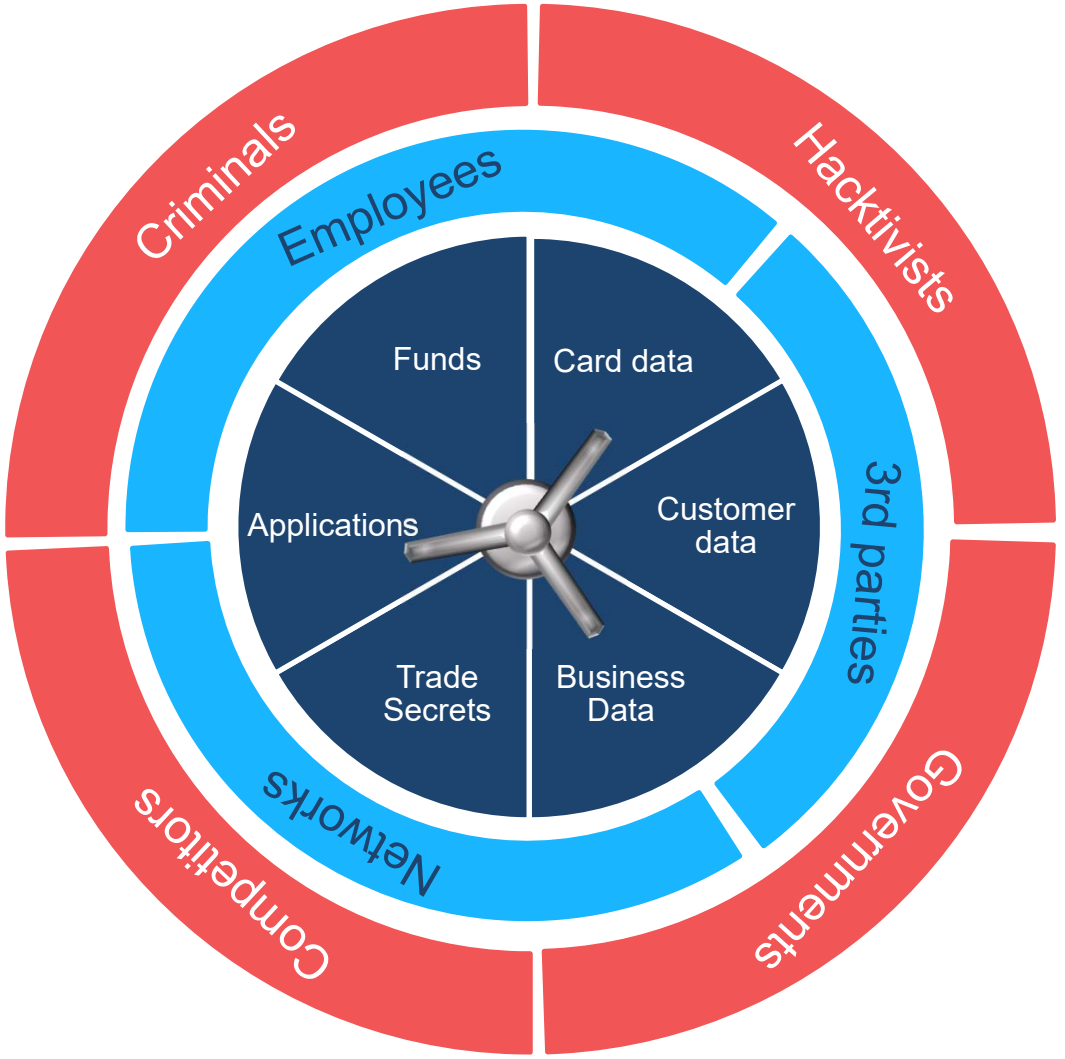
Naim, Patrick, Mstar, patrick.naim@elseware.fr
Condamin, Laurent, Mstar, laurent.condamin@elseware.fr

Version 25/03/2019

Executive SUMMARY

- We propose a consistent method for the structured identification and assessment of cyber risks:
- **The identification of risks** is based on a breakdown of critical Assets, possible Accesses to these assets, and possible Attackers.
- This decomposition by **Asset, Access, Attacker** can be directly mapped to the Exposure, Occurrence, Impact approach to **Structured Scenario modelling**.
- Structured modelling defines a **loss generation mechanism** which allows an explicit quantification of scenarios and peer benchmarking.
- Structured modelling allows the impact of **mitigation** actions to be assessed.

The cyber risk wheel

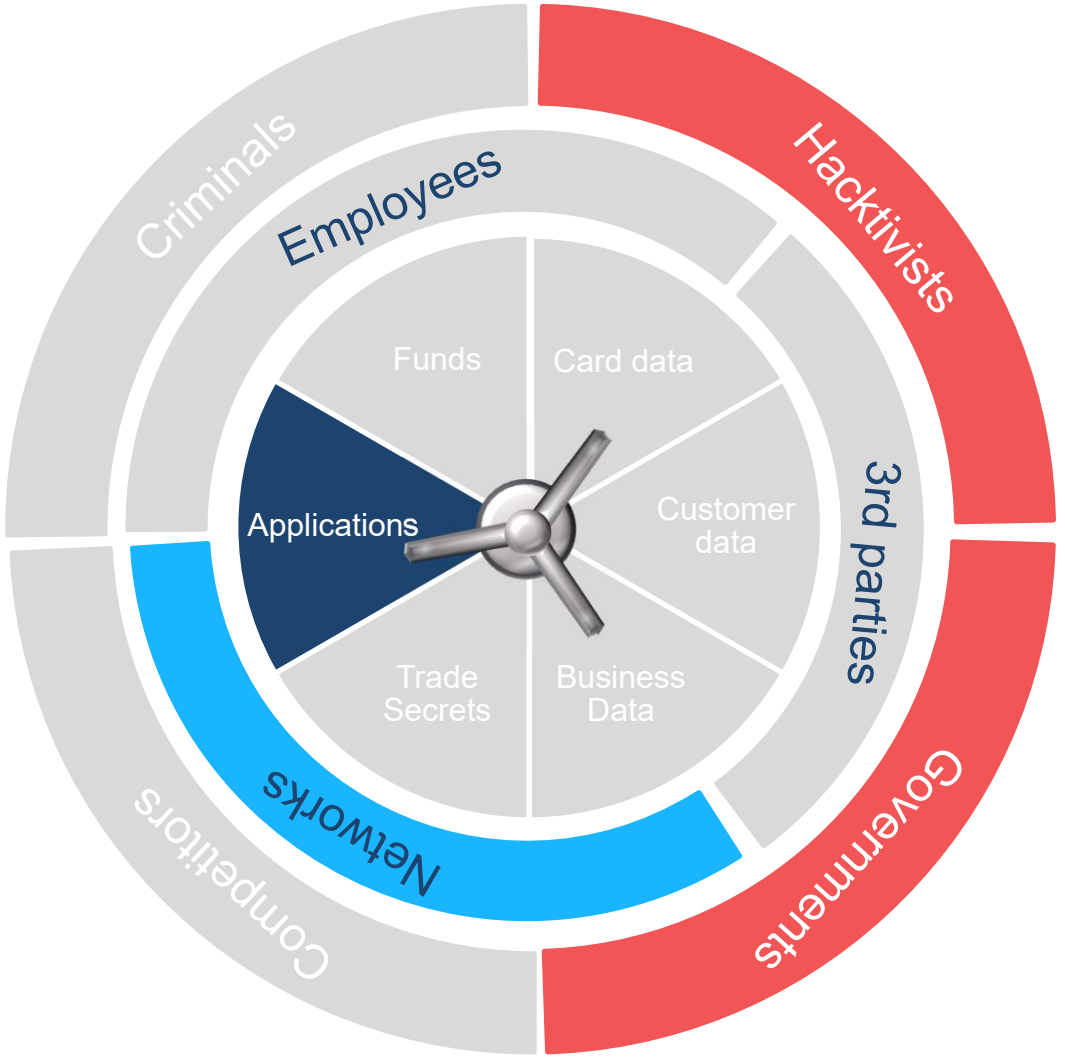


ATTACKERS

ACCESS

ASSETS

Example – CYBER Attack on critical service

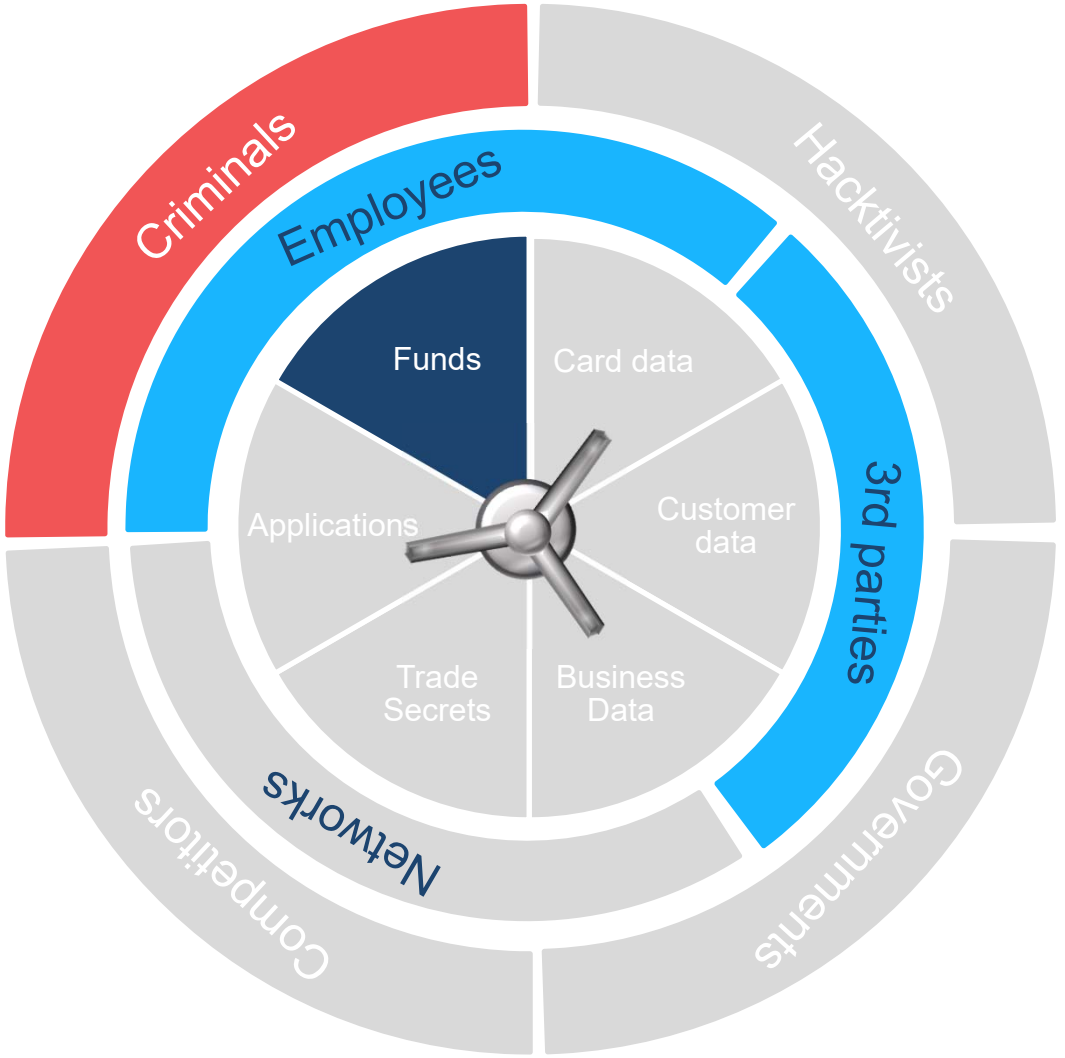


ATTACKERS

ACCESS

ASSETS

Example – CYBER FUND MISAPPROPRIATION

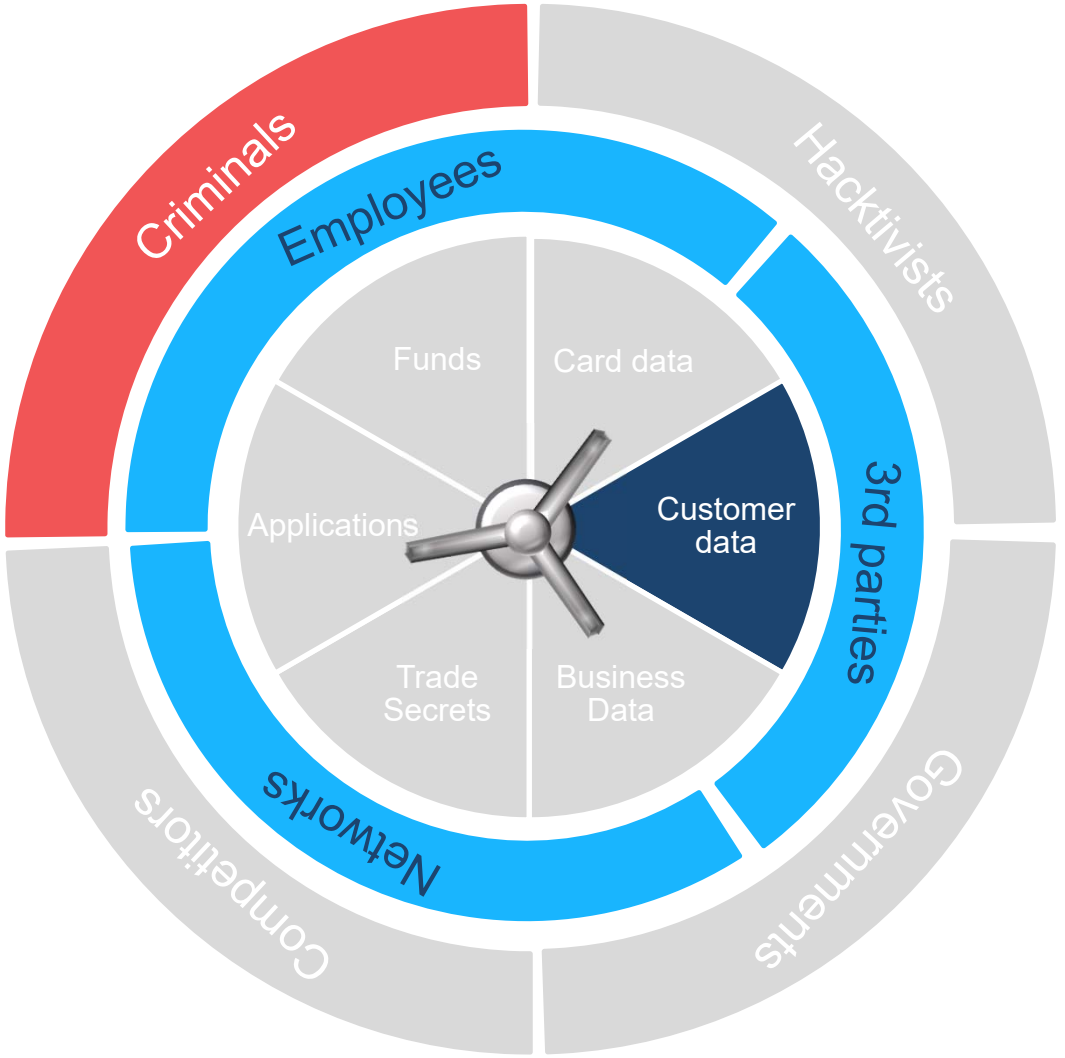


ATTACKERS

ACCESS

ASSETS

Example – customer data compromise



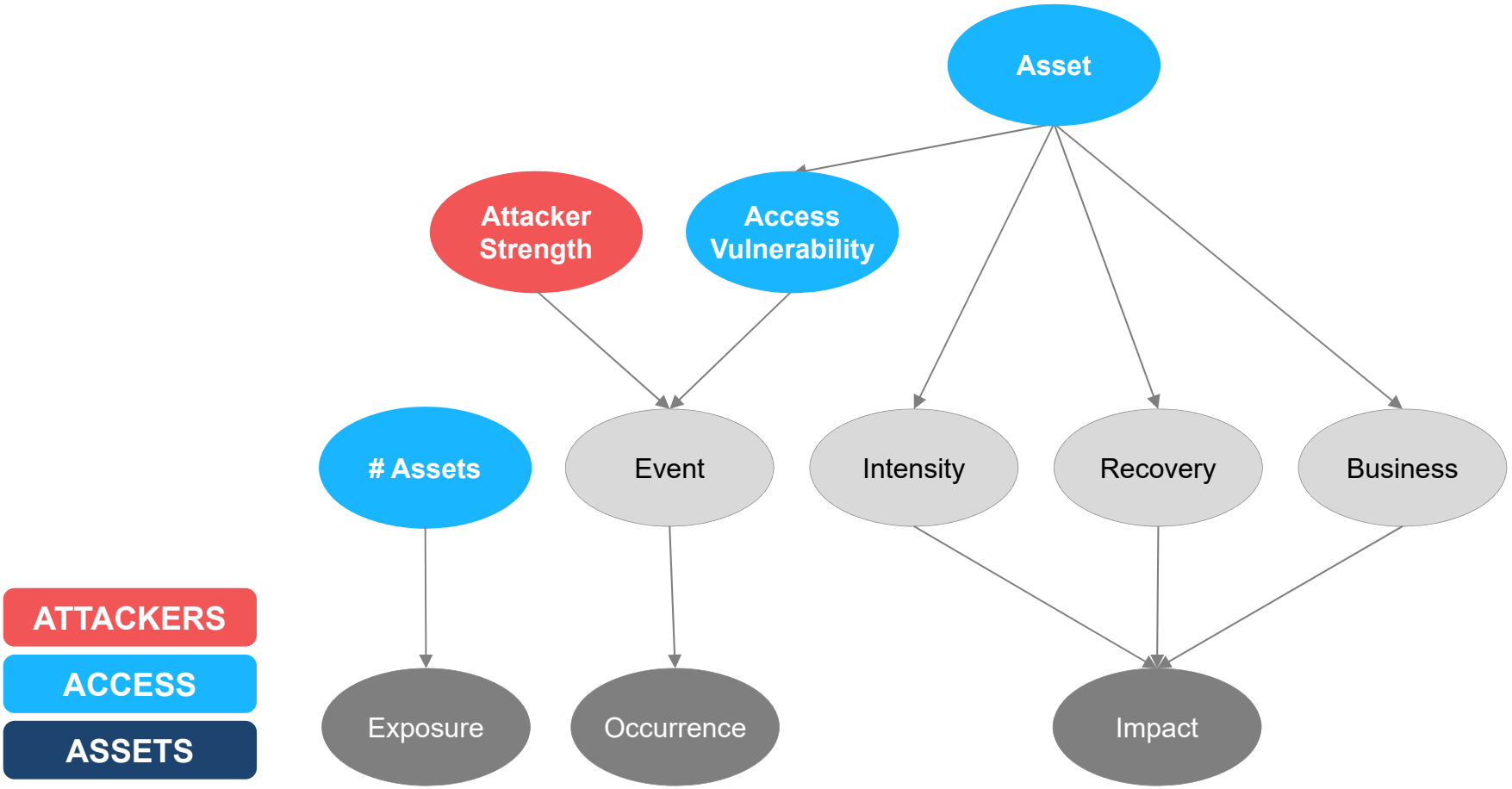
ATTACKERS

ACCESS

ASSETS

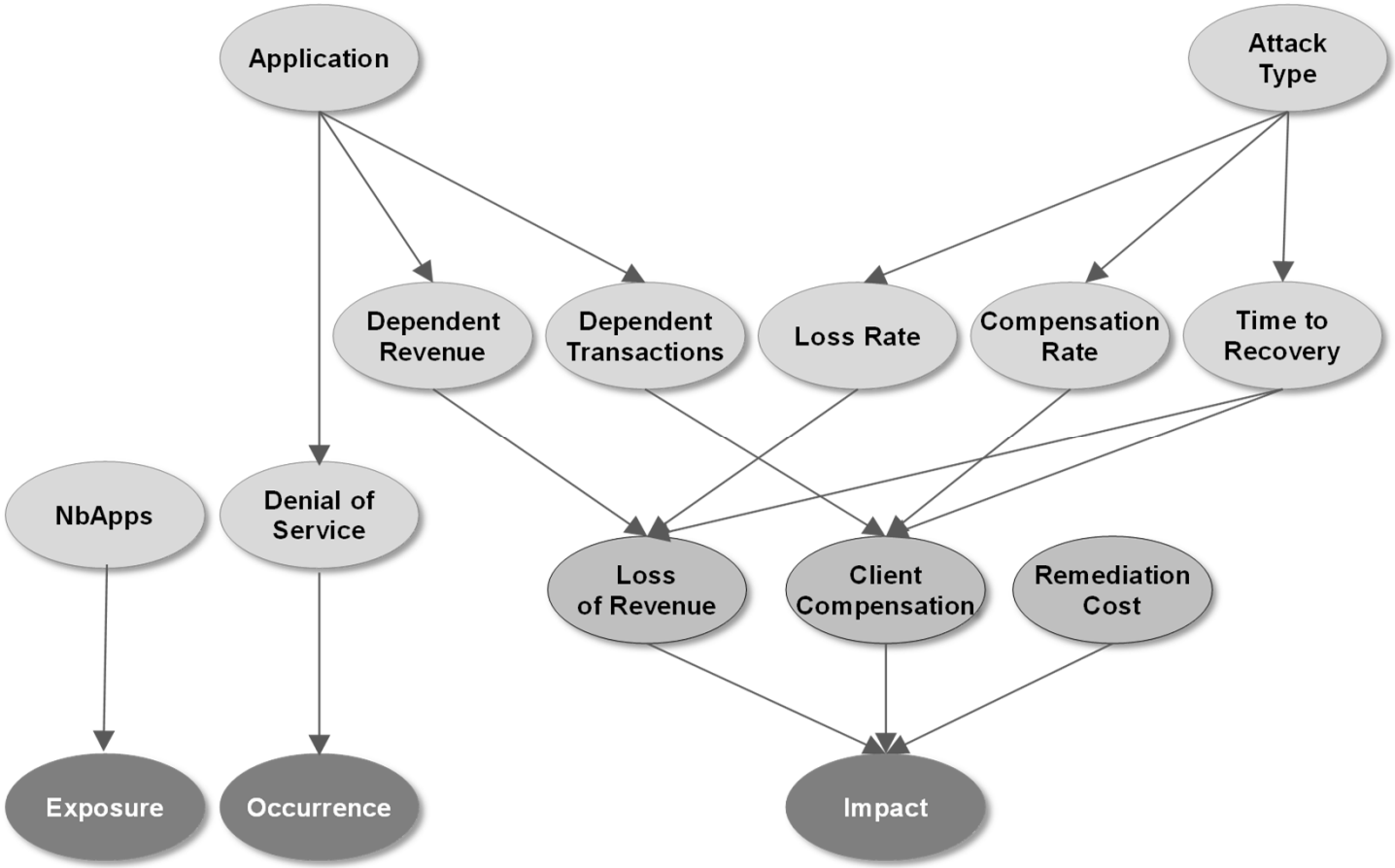
Mapping to scenario assessment

- The decomposition of a cyber risk scenario into Asset, Access and Attacker can be used to build a structured assessment of the scenario:



Example – CYBER Attack on critical service

- The decomposition of a cyber risk scenario into Asset, Access and Attacker can be used to build a structured assessment of the scenario:



Cyber Attack Critical service - Quantification

DRIVER	TYPE	ASSESSMENT	SOURCE
Number of critical services	Objective	5 services: Cards, Transfers, Trade, Loans, Internet Banking	Business Data, Resiliency Team
Type of Attack	Subjective	Duration: 80% Magnitude: 20%	SMEs, External Research, ILD & ELD
Probability of Cyber Attack	Subjective	[5%-20%] per application	SMEs, External Research, ILD & ELD
Dependent Revenue	Objective	Internet Banking: $5m-$10m Cards, Loans: $10m-$20m	Business Data, Annual Reports
Dependent Transactions	Objective	Transfers: $70bn-$80bn Trades: $4bn-$6bn	Business Data
Compensation Rate	Subjective	Transfers: 0-10$ per $1mm trans. Trades: 0-300$ per $1mm trans. for a duration attack, 0-600$ per $1mm trans. for a magnitude attack	Local model used based on Daily Penalty, Slowdown, Average TTR
Loss of Revenue Rate	Subjective	Duration Attack: 20% Magnitude Attack: 100%	SMEs
Time To Recovery	SMEs	Duration Attack: 2-12 days Magnitude Attack: 0-2 days	Resiliency Team, Business Impact Analysis, External Research

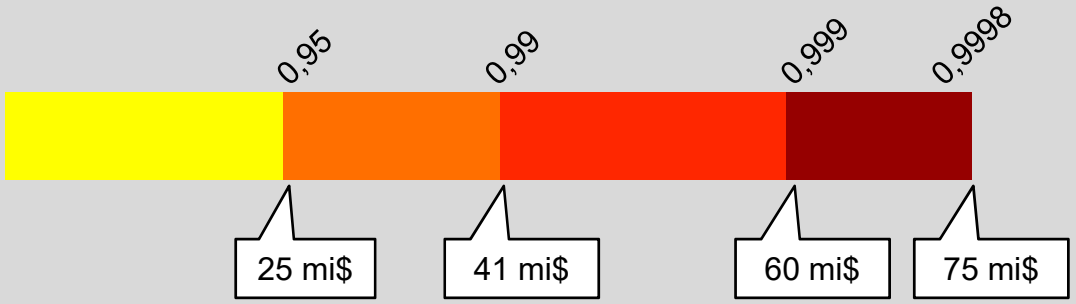
Cyber Attack – Critical Application - Simulation

The scenario structure and the driver assessments are compiled into a Bayesian Network that is sampled through Monte Carlo simulation to estimate the distribution of the potential losses.

REPEAT 1,000,000 times:

- SET the cumulated loss to 0
- SAMPLE the **exposure** from its conditional distribution
- FOR each exposed unit, sample the **occurrence** of the event from its conditional distribution
  - IF the occurrence is TRUE:
    - SAMPLE the **impact** of the event from its conditional distribution
    - ADD the impact to the cumulated loss

Number of iterations	**1 mi**
Single Loss	
Average	9.5 mi$
Max Possible	48.5 mi$
Frequency	
Average	0.5
Cumulated Loss	
Min	0$
Max	119 mi$
Mean	5.0 mi$



Benefits of the approach

- **Explicit definition of Cyber Scenarios and their boundaries**
- **Consistent reporting of events – and use of external events**
- **Direct mapping to structured asssement**
- **Identification of KRI**
- **Quantification of risk scenarios**
- **Possibility to benchmark assessment with peers**
- **Evaluation of mitigation actions**

Panel #2: Measurement and Impact of Cyber Risk

- **Gilles Hilary**, *Chaired Professor, Georgetown University*
- **Patrick Naim**, *CEO, Elseware*
- **Denyette DePierro**, *Vice President, Center for Payments and Cybersecurity, American Bankers Association*
- **Phil Collett**, *Director Cyber Risk Assessments, American Express Co.*
- **John DeLong**, *Risk Management, Morgan Stanley*
- **Filippo Curti**, *Financial Economist, Quantitative Supervision & Research, Federal Reserve Bank of Richmond*

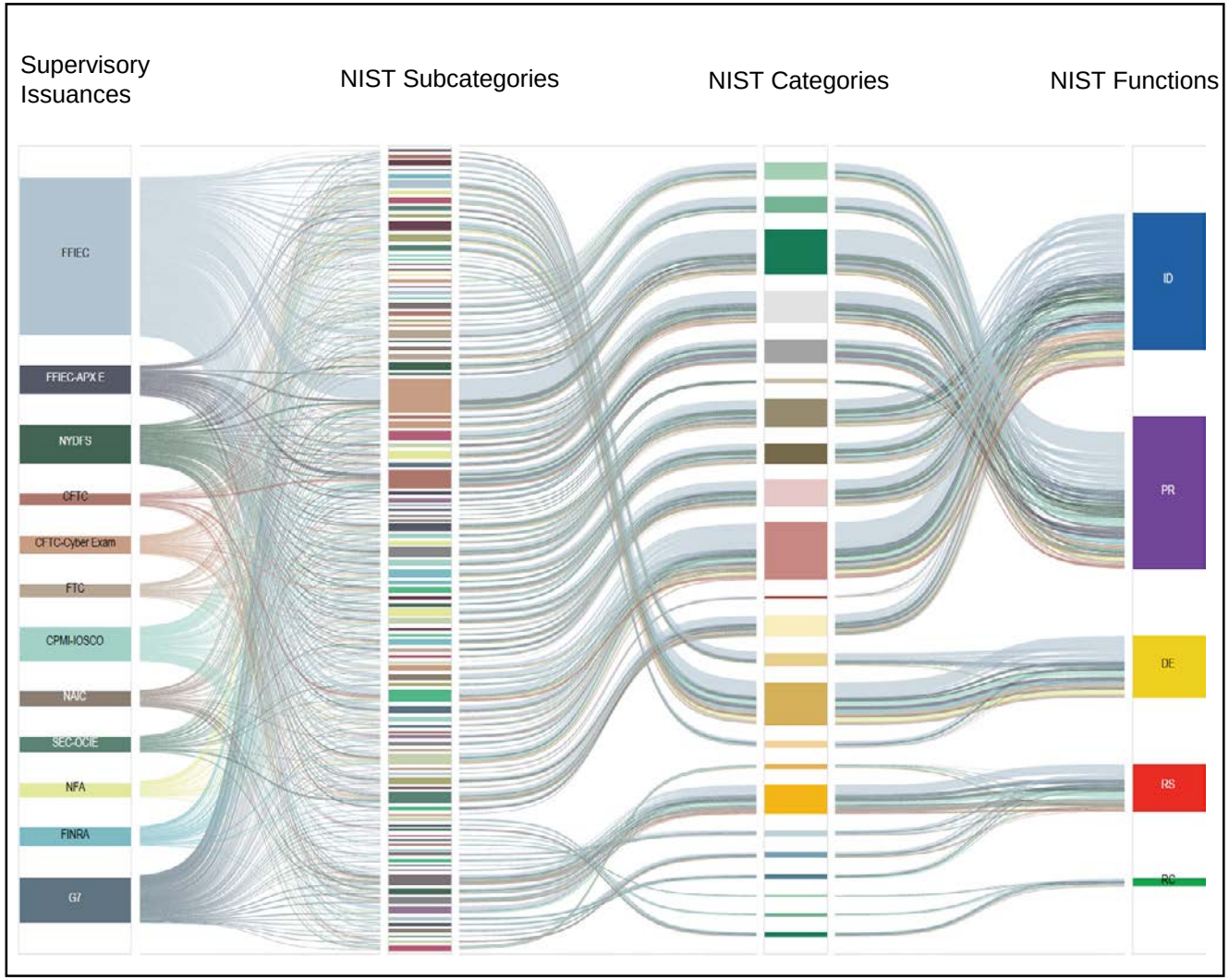
FSSCC Cybersecurity Profile

- An Overview -

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Topical Overlaps, Semantic Differences = Resources Focused on Reconciliation, Compliance

- 2016 Survey: **40%** of Information Security teams' time on avg spent on reconciliation of cyber expectations
- (ISC)2: Gap of cyber pros growing, with a **gap of 3 million projected for 2019**
- FSB (2018): **72% of jurisdictions** reported plans to issue new cyber requirements



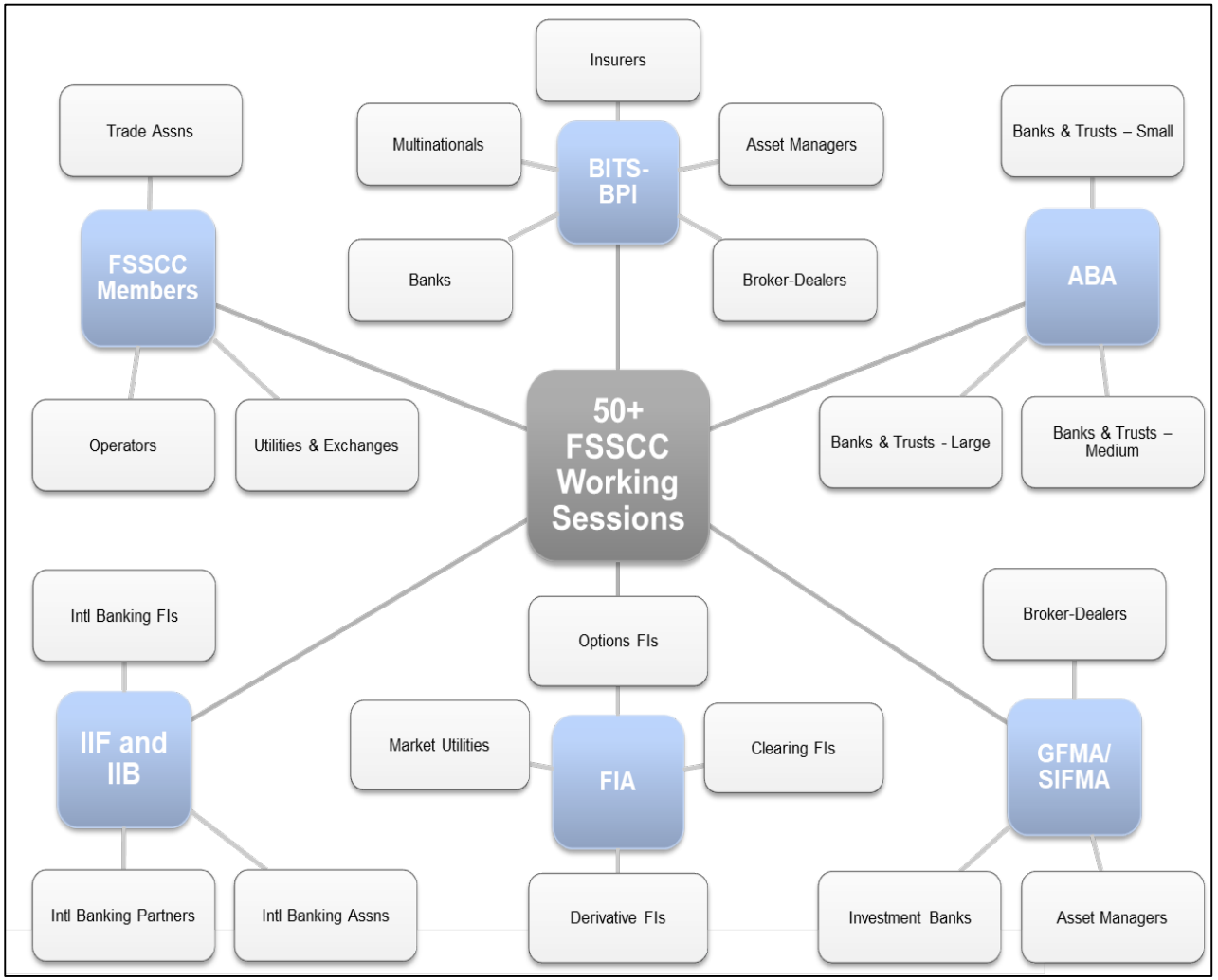
Developing the Profile: Process and Participants

Over the past 2 years –

- FSSCC Coalition;
- BITS and ABA co-lead;
- ***50+ working sessions;***
- ***300+ participants;***
- ***150+ financial institutions represented***.

Financial Services and Other Agencies –

- *Provided material for incorporation*, notably:
  - FRB;
  - OCC;
  - FDIC;
  - SEC;
  - CFTC;
  - FINRA;
- NIST workshop on risk/impact scaling.

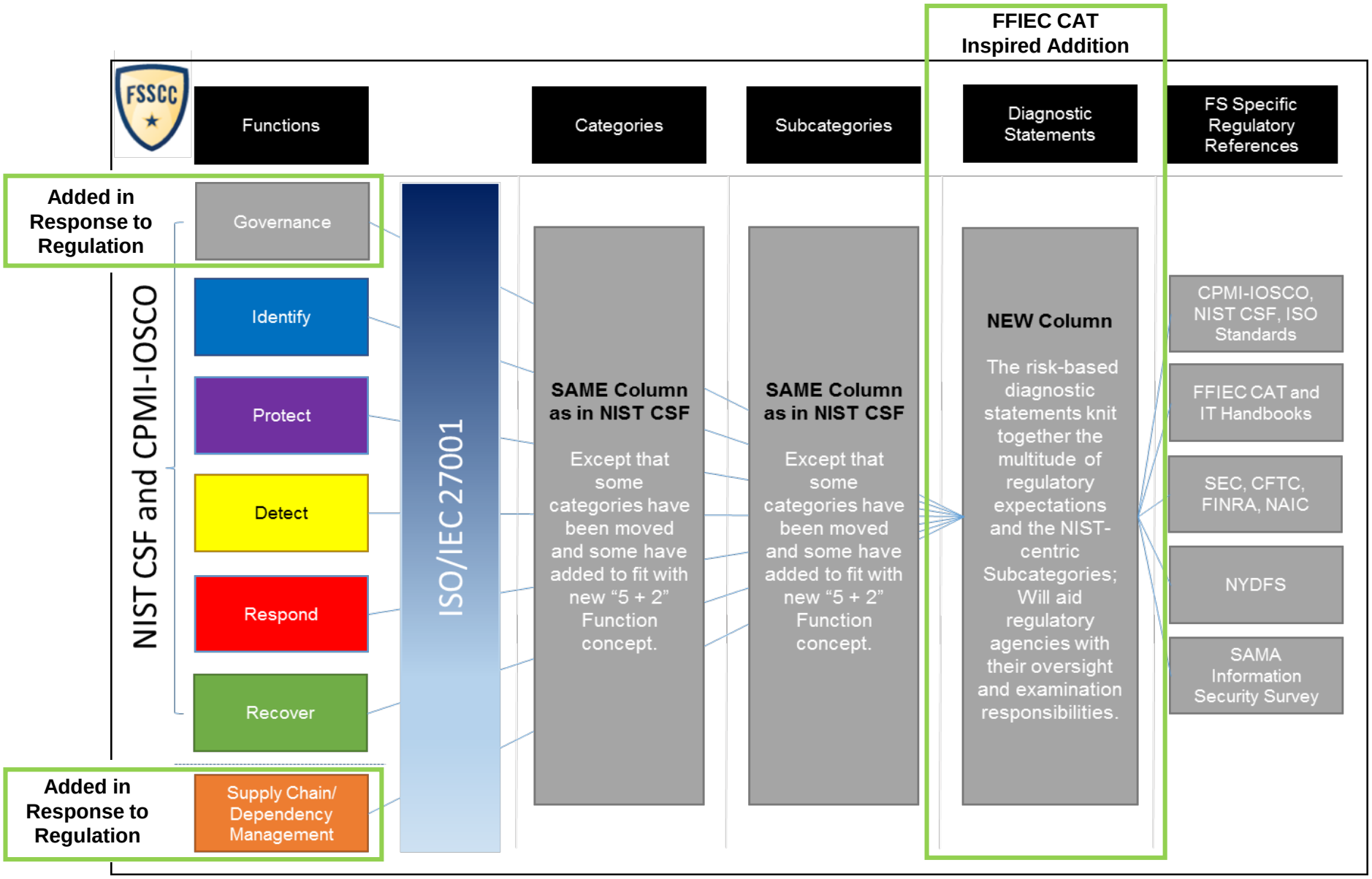


Benefits Explored - Efficiencies Gained

- ***73% Reduction for Community Institution Assessment Questions.*** For the least complex and interconnected institutions, it is expected that they would answer a total of 145 questions (9 tiering questions + 136 Diagnostic Statement questions). As compared to another widely-used assessment tool's 533 questions, this represents a ***73% reduction.***

- ***49% Reduction in Assessment Questions for the Largest Institutions.*** For the most complex and interconnected institutions, the reduction also is significant. With the Profile, it is expected that such institutions would answer 279 questions (2 tiering questions + 277 Diagnostic Statement questions) as compared to the other widely-used assessment's 533, ***a 49% reduction.***

PART I: The Profile's Underlying NIST Architecture



Part II: Sector-Wide Impact Assessment

National or Global Impact – Tier 1

- Systemically important and/or multinational firms.
- GSIBs, GSIFIs, systemically important market utilities.

Subnational (Regional) Impact – Tier 2

- Firms offering mission critical services or have over 5 million customer accounts.
- Super-regional banks, large insurance firms.

Industry-wide scaling achieved through collaboration with NIST, Federal Reserve, OCC, FDIC, SEC, FINRA.

40+ firms implementing the Profile or actively exploring implementation for 2019/2020.

- Firms with a high degree of interconnectedness, and between 1-5 million customer accounts.
- Regional banks, large credit unions.

Sector Only Impact – Tier 3

- Applies to the firms with a relatively small number of customers.
- Community banks, small broker dealers/investment advisors.

Customer/3rd Party Impact Only – Tier 4

Benefits of the Profile Approach

Financial Institutions

- ✓ ***Optimization of cyber professionals' time*** "at the keyboard," defending against next gen attacks – ***complete once per cycle, report out to many***.
- ✓ ***Improved Boardroom and Executive engagement***, understanding and prioritization.
- ✓ Enhanced, ***efficient third-party vendor management***.

Supervisory Community

- ✓ ***Examinations more tailored to institutional complexity, enabling "deeper dives"*** in those areas of greater interest to that particular agency.
- ✓ ***Enables supervisory agencies to better discern the sector's systemic risk***, with more agency time for specialization, testing and validation.
- ✓ Enhanced ***visibility of non-sector and third-party cyber risks***.

The Ecosystem

- ✓ ***Based on NIST and ISO, it allows for greater intra-sector, cross-sector and international cybersecurity collaboration and understanding***.
- ✓ Enables ***collective action to better address collective risks***.
- ✓ ***Greater innovation as technology companies, including FinTech's, are able to evidence security*** against the standardized set of compliance requirements.

The Profile: A NIST Cybersecurity Framework Extension to Align with Financial Services Requirements and Supervisory Expectations

NIST Cybersecurity Framework provides a globally accepted organizational structure and taxonomy for cybersecurity and cyber risk management

The following countries are either exploring its use or promoting it through translation –

- Bermuda
- Brazil
- Canada
- Israel
- Italy
- Japan
- Malaysia
- Mexico
- Philippines
- Saudi Arabia
- Switzerland
- United Kingdom
- Uruguay

The Profile extends the NIST Cybersecurity Framework to be more inclusive of financial services requirements and supervisory expectations

Extended NIST to highlight 2 special categories of particular (& appropriate) regulatory focus:

Governance

Supply Chain/ Dependency Management

The following international governments and organizations have expressed positive interest in the Profile –

- Argentina
- Brazil
- China (Mainland and Hong Kong)
- Chile
- Colombia
- European Union
- International Standards Organisation
- Japan
- Organization of American States
- Singapore
- United Kingdom

Websites

- https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile
- https://www.fsscc.org/The-Profile-FAQs
- https://www.fsscc.org/files/galleries/NIST_Letter_of_Support_re_FSSCC_Financial_Services_Sector_Cybersecurity_Profile.pdf

Executive Summary

The Issue: Domestic and international regulatory agencies asking the same question in many different ways, stretching already scarce cybersecurity talent.

The Profile as a Solution: The Profile, which is a common, standardized approach that can act as a baseline for examination and future cyber regulation - *fill out once per exam cycle, report out many*.

Voluntary with Many Benefits, Including:

- Provides more consistent and efficient processing of examination material by both firms and regulators.
- Allows Regulators and Firms to focus on systemic risk and risk residual to firms.
- Establishes an Industry best practice beyond regulatory use.

Supporting Associations:

FSSCC Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

American Bankers Association

bpi Business Innovation Technology Security BITS

FIA

gfma

iib Institute of International Bankers Advancing the interests of the International Banking Community in the United States www.iib.org

IIF Institute of International Finance

Panel #2: Measurement and Impact of Cyber Risk

- **Gilles Hilary**, *Chaired Professor, Georgetown University*
- **Patrick Naim**, *CEO, Elseware*
- **Denyette DePierro**, *Vice President, Center for Payments and Cybersecurity, American Bankers Association*
- **Phil Collett**, *Director Cyber Risk Assessments, American Express Co.*
- **John DeLong**, *Risk Management, Morgan Stanley*
- **Filippo Curti**, *Financial Economist, Quantitative Supervision & Research, Federal Reserve Bank of Richmond*

Cyber Risk Quantification

March 2019 | Phil Collett

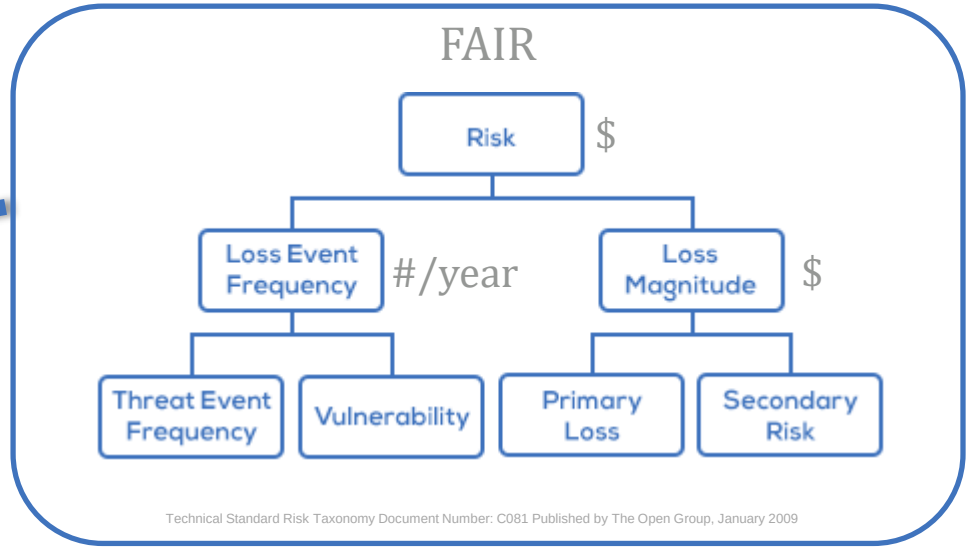
Risk Quantification

Problem Statement:

*An increasing number of control frameworks and regulations trend toward using less prescriptive language in favor of an emphasis on taking a **'risk-based approach'.** However, many firms struggle to design and implement operationally feasible, repeatable, and accurate risk quantification methodology and tooling.*

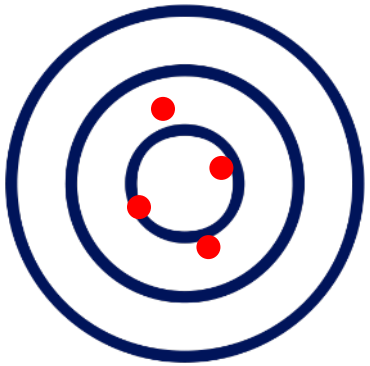
Analysis of Risk Quantification Methods:

Cyber Risk Methodology	Precision	Quantification	Agility	Ease of Use	Overall (0 – 100)
Factor Analysis Information Risk (FAIR)	↑	⇈	=	=	70
CORA	=	↑	↑	↑	70
ISRAM	=	↑	=	=	65
Facilitated Risk Analysis Process	↑	↓	=	=	60
COBRA	=	↓	=	↑	55
OACTIVE ALLEGRO	↑	↓	=	=	55
NIST 800-30	↑	↓	=	=	50
ISO 30101:2009	=	↓	=	=	45
COBIT	⇊	↓	=	=	40

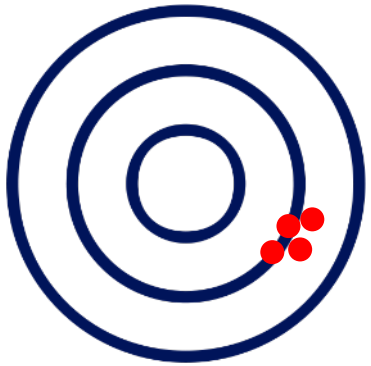


Quantification Accuracy

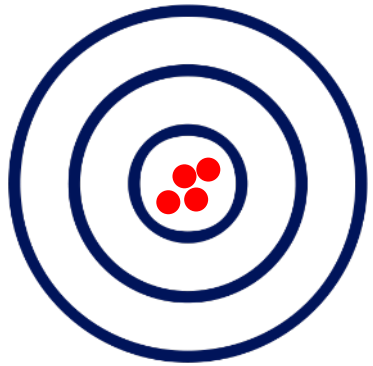
*It is better to be consistent (precise) by using a **single source of truth for** inputs such as **asset value**, **control strength**, and **threat frequency**. Once precision is achieved, focus on calibrating the inputs to achieve accuracy.*



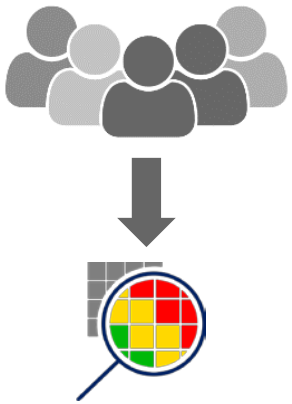
TRUE, BUT LACKING PRECISION



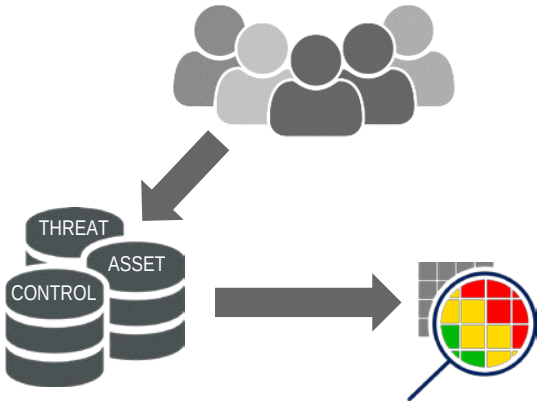
PRECISE, BUT LACKING TRUENESS



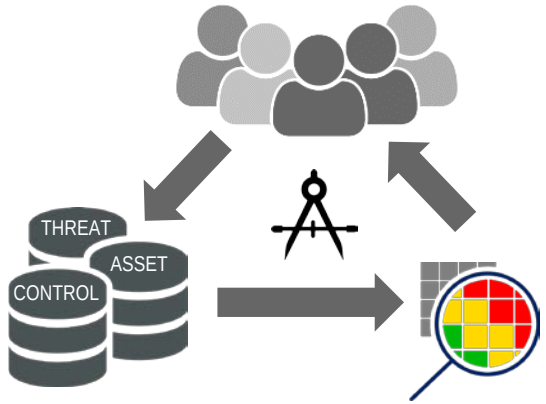
ACCURATE



Assessor relies upon their own experience and training while interacting with the model



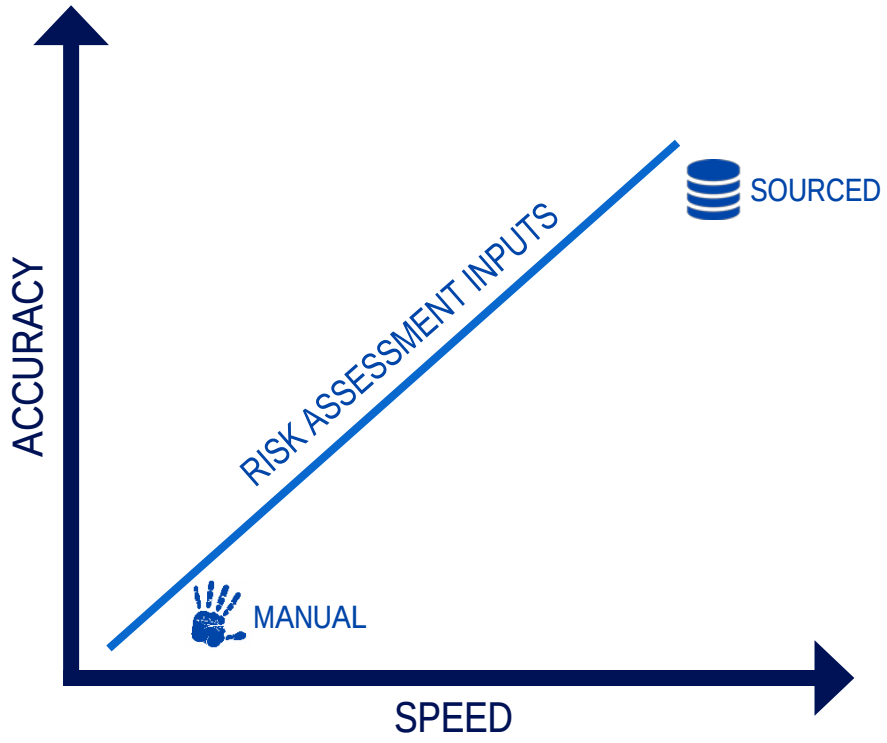
Assessor uses pre-defined values for asset value, control effectiveness, and threat inputs



Over time, the systems of record for asset, control, and threat data are calibrated for accuracy

Quantification Adoption

Improve risk assessment speed and accuracy by sourcing as many risk assessment inputs as possible from either metrics or pre-aligned values.

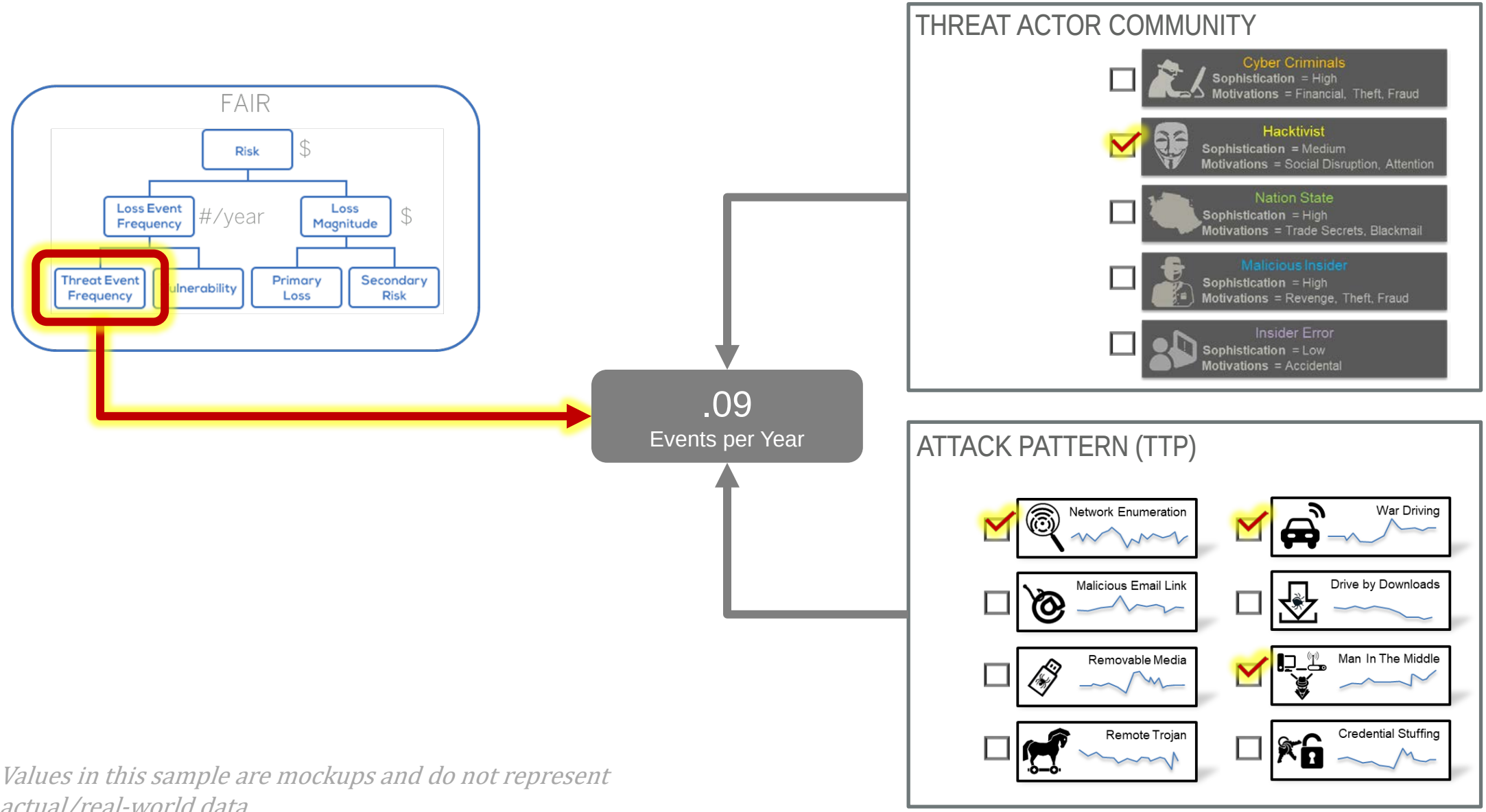


Sample Risk Assessment Inputs:

Assessment scope
Identify relevant threats
Identify relevant assets
Identify applicable controls
Threat actor capability
Threat frequency
Effectiveness of applicable controls
Controls ability to reduce likelihood
Controls ability to reduce impact
Primary losses based on asset
Reputation costs based on asset
Response costs based on asset
Potential fines and legal fees

Example: Threat Input Quantification

*This sample shows how a single source of truth for **attack types** and **threat actor communities** can save an assessor from having to speculate on the threat event frequency in a risk assessment using FAIR.*



Values in this sample are mockups and do not represent actual/real-world data

Thank You

Panel #2: Measurement and Impact of Cyber Risk

- **Gilles Hilary**, *Chaired Professor, Georgetown University*
- **Patrick Naim**, *CEO, Elseware*
- **Denyette DePierro**, *Vice President, Center for Payments and Cybersecurity, American Bankers Association*
- **Phil Collett**, *Director Cyber Risk Assessments, American Express Co.*
- **John DeLong**, *Risk Management, Morgan Stanley*
- **Filippo Curti**, *Financial Economist, Quantitative Supervision & Research, Federal Reserve Bank of Richmond*

Morgan Stanley

2019 Cyber Risk Workshop

John DeLong

Operational Risk

Discussion & Questions

Lunch

- Lunch is available outside the conference area.
- Please go through the buffet line and then be seated in the pre-function area.
- Please be back in your seats for the keynote at 1:30.

Keynote Address

- **Patricia Mosser,** *Director, MPA Program in Economic Policy Management; Senior Research Scholar of International and Public Affairs, Columbia University*

Cyber Risks to Financial Stability

Cyber Risk Workshop

Quantitative Supervision and Research
Federal Reserve Bank of Richmond, Charlotte Branch

Patricia C. Mosser
Columbia SIPA
March 28, 2019

Cyber Risks to Financial Stability

General Framework

Cyber Risks

1. **Internal IT Enterprise**
2. **External Dependencies**
   a. Counterparties and Partners
   b. Outsourced and Contract
   c. Supply Chain
   d. Upstream Infrastructure
3. **External Shocks**

Can Trigger

Transmission from Cyber to Financial

Transmission Channels

How Can Cyber Events Threaten Financial Stability?

1. Lack of Financial Substitutability
2. Lack of IT Substitutability
3. Loss of Confidence
4. Data Integrity
5. Interconnectedness

Can Trigger

Financial Stability

1. **Fragility**
   a. Leverage
   b. Maturity Transformation
   c. Procyclicality of Risk
2. **Complexity**
3. **Adaptability**
   a. Innovation
   b. Regulatory Arbitrage

Feedback to Cyber and Larger System

Amplifiers and Dampeners

Can Exacerbate or Alleviate Risks Over Time

Within Environment of

Geopolitical Fragility – Financial Fragility – Technological Fragility – Societal Fragility

Analysis can begin with cyber risks (flowing left to right, like the incident itself); with financial stability and working backwards (right to left), or from the amplifiers and dampeners (bottom up)

Break

- Panel #3 starts at 2:30.
- Restrooms are located to your left as you exit the conference room.
- Refreshments will available in the pre-function area from 4-5 pm for the networking session.
- Transportation
  - Address is 530 East Trade Street; pickup is directly in front of the building
  - Taxi number is 704-444-4444

Panel #3: The Role of the Federal Reserve System

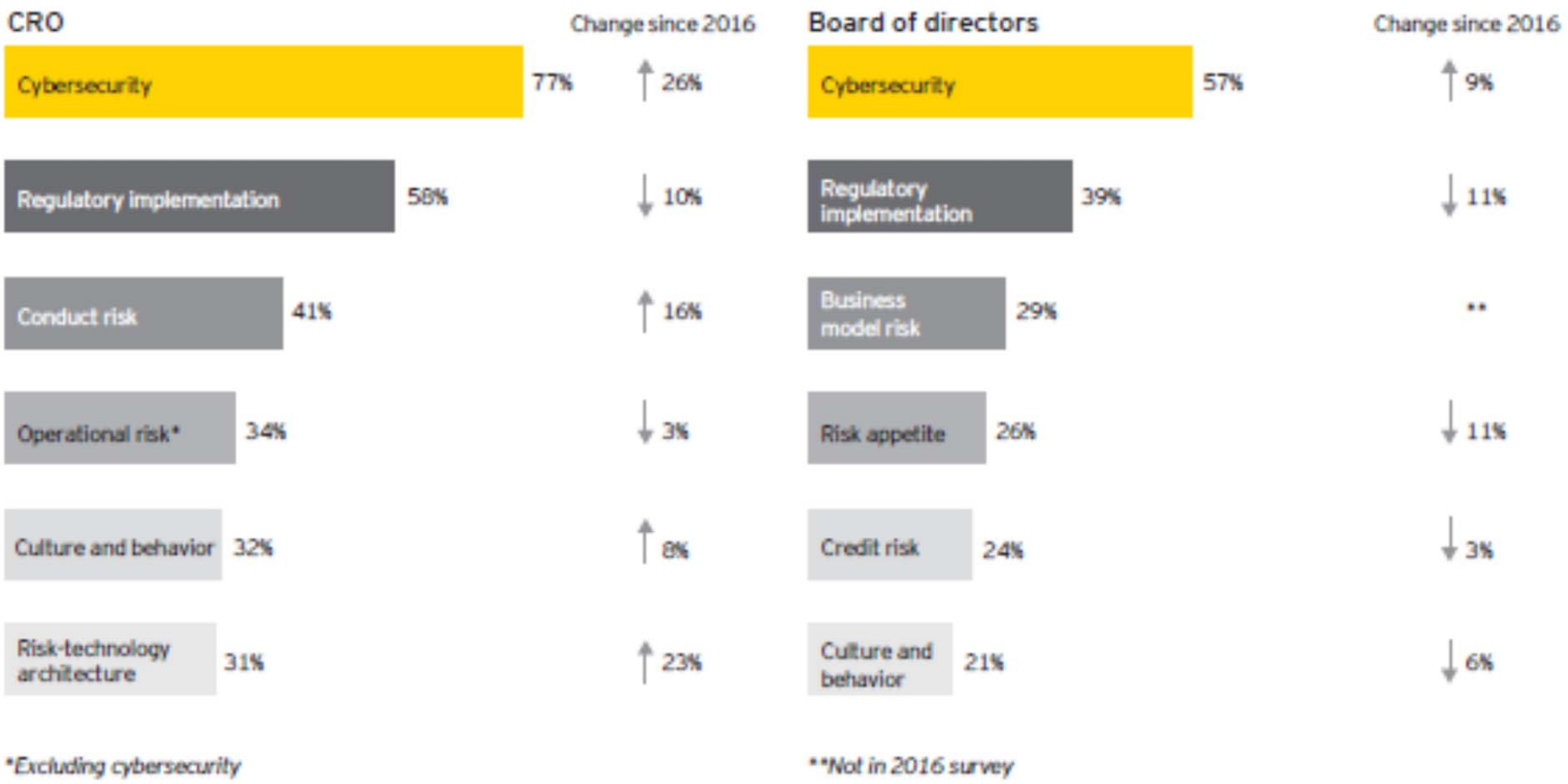
- **René Stulz**, *Everett D. Reese Chair of Banking and Monetary Economics, The Ohio State University*
- **Todd Vermilyea**, *Senior Associate Director, Risk & Surveillance, Board of Governors of the Federal Reserve System*
- **Keith Gordon**, *Chief Information Security Officer, Ally*
- **Nida Davis**, *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

Conclusion

- You'll receive a brief feedback survey soon.
- Refreshments will available in the pre-function area from 4-5pm for the networking session.
- Transportation
  - Address is 530 East Trade Street; pickup is directly in front of the building.
  - Taxi number is 704-444-4444
- Thank you for attending!