

# 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 Olagbemi**, *Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond*

---

# Cyber: a risk management perspective

March 2019

Steve Bishop

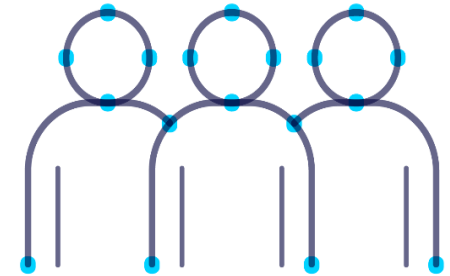
Head of Risk Information, ORX



# ORX: Introduction

O.R.X

- 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

## 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



Public

## 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 disintermediation





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

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



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



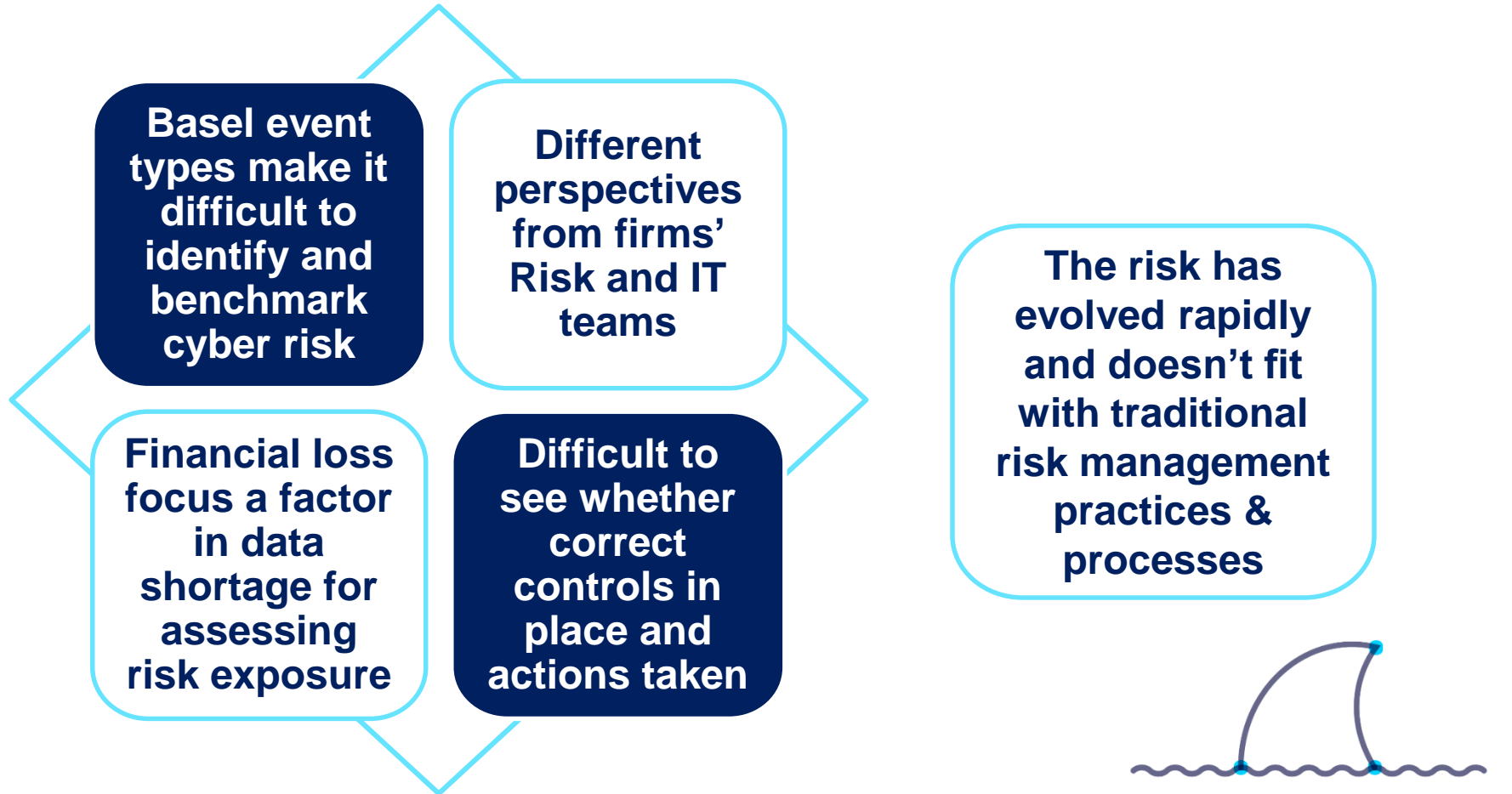
British Airways suffers data breach compromising information on 429,000 customer cards

**Banco de Chile**

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.












# 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.

O.R.X

Developments in risk taxonomies

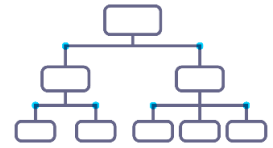
Level one risk name	Example risk themes included in risk taxonomies submitted
<b>Conduct</b> 	<ul style="list-style-type: none"> <li>Culture, unethical behaviour or fiduciary breach</li> <li>Mis-selling, inappropriate products/advice</li> <li>Behaviour towards customers, clients or markets</li> <li>Impersonal business or market practices</li> <li>Collusion and conflict of interest</li> </ul>
<b>Legal</b> 	<ul style="list-style-type: none"> <li>Breach of law (civil and criminal)</li> <li>Dispute management</li> <li>Current or prospective litigation</li> <li>Failure to follow legal advice or legal documents</li> <li>Failure to manage legal obligations to key stakeholders</li> </ul>
<b>Financial crime</b> 	<ul style="list-style-type: none"> <li>Anti-money laundering, counter-financing of terrorism and sanctions screening</li> <li>Anti-bribery and corruption</li> <li>Facilitated using third-parties, or products and services</li> <li>Actions resulting in regulatory breaches</li> </ul>
<b>Regulatory compliance</b> 	<ul style="list-style-type: none"> <li>Intentional or negligent failure to meet regulations, laws and other rules</li> </ul>
<b>Third party</b> 	<ul style="list-style-type: none"> <li>Supplier, vendor and outsourcing</li> <li>Selection, contracting, onboarding, management and termination of suppliers</li> <li>Failures of suppliers</li> </ul>
<b>Information security (including cyber)</b> 	<ul style="list-style-type: none"> <li>Unauthorized access, change, destruction</li> <li>Loss, theft or misuse of information</li> <li>Cyber-attack affecting privacy/confidentiality, availability, integrity of information (link to Fraud where cyber-attack leads to theft of money)</li> </ul>
<b>Financial reporting and tax</b> 	<ul style="list-style-type: none"> <li>Inaccuracy, incomplete or untimely reporting</li> <li>Internal and external financial or regulatory reporting</li> <li>Losses in the form of additional tax costs and penalties</li> <li>Failure to comply with tax law in a timely, transparent and effective manner</li> </ul>
<b>Data management</b> 	<ul style="list-style-type: none"> <li>Failure to effectively and efficiently govern data, or manage data quality or data knowledge</li> <li>Entire data lifecycle, including when data is acquired or created; processed; used; stored; accessed; retained and disposed</li> </ul>
<b>Model</b> 	<ul style="list-style-type: none"> <li>Error in the model design, implementation, usage, coding, input or data source</li> <li>Misuse of models</li> </ul>



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.

Incident Type	Event Type	Action	Actor Origin	Affected Kind of Data*	Business Impact*	Status
Confidentiality	External Fraud	Malware - Targeted	External Actor	Customer: PII (Personally Identifiable Information)	Business Interruption, Interruption of Operations, Loss of Profit	Open
Integrity	Employment Practices and Workplace Safety	Malware - Generic	Internal Actor	Unknown	Contingent Business Interruption (CBI) for non-physical damage, Loss of Profit	Closed
Availability	Malware - Unknown	Malware - Unknown	Unknown	Customer: PCI (Payment Card Information)		Date of Discovery
Unknown	Clients, Products, and Business Practice	Denial of Service	External Actor Selection	Customer: PCI (Payment Card Information)		Discovery date
Dominant Threshold Triggered	Damage to Physical Assets	Environmental	Ext Actor - Activist	Customer: PHI (Personal Health Information)	Data and Software Loss - Restoration, reconstitution	Occurrence Date
Customer Detriment	Business Disruption and System Failures	Error	Ext Actor - Nation State	Corporate: Intellectual property	Financial Theft and/or Fraud - Pure financial losses	Date of first activity leading to the incident
Direct Financial Impact	Execution, Delivery, and Process Management	Hacking	Ext Actor - Organised Crime	Corporate: Financial Data	Cyber Ransom and Extortion	
Legal / Regulatory	Management	Unknown	Ext Actor - Former Employee	Corporate: Financial Data	Intellectual Property Theft - Pure Financial Losses	Currency
Reputational Impact	Root Cause	Asset*	Ext Actor - Force Majeure	Corporate: PII	Incident Response Costs	Currency options
Business Interruption / Employee Detriment	People	Server	Ext Actor - Unaffiliated Hacker	Corporate: Other	Breach of Privacy, Compensation costs	Impact Location
	Systems	Network	Ext Actor - Terrorist	Systems: Authentication	Network Security/ Security Failure, Compensation costs	Country options
	Processes	User Device	Ext Actor - Act of war	Systems: Published	Regulatory and Legal Defence costs	Event Description
	External Causes	Data Storage	Ext Actor - Partner	Systems: Other	Fine and Penalties	Free field
Threshold Rating	Not Yet Reported	Media	Ext Actor - Unknown	Not relevant / None	Communication and Media	Exposure Indicators
Medium	Discovery Method	User	Malicious Event	Financial Impact	Legal protection - Lawyer fees	Number of Employees
High	Audit	Application/ Software	Yes	Gross loss value	Assistance coverage - Psychological support	Yearly Turnover
Near Miss	Security Control	Business Process	No	By indicated Business Impact area (up to 3 areas)	Directors & Officers (D&O)	Minimal Financial Threshold
Yes	Third Party	External Provider			Technology Errors & Omissions (Tech E&O)	
No	User	Smart Device, IoT, ICS			Professional Services E&O, Professional indemnity	
	Monitoring Service	Attacker			Environmental Damage	
	Attacker	Other			Physical Asset Damage	
	Other	Unknown			Bodily Injury and Death	

\*Field is multiple selection

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 **2<sup>nd</sup> 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.



# ORX: Addressing the issue

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.**

---

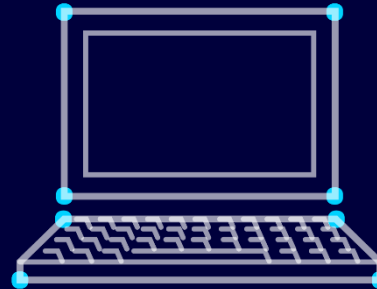
**Steve Bishop**

**Head of Risk Information, ORX**

**[Steve.bishop@orx.org](mailto:Steve.bishop@orx.org)**



**Follow ORX  
on LinkedIn**



**Visit  
[www.orx.org](http://www.orx.org)**

# Panel #1: Identification and Classification of Cyber Risk

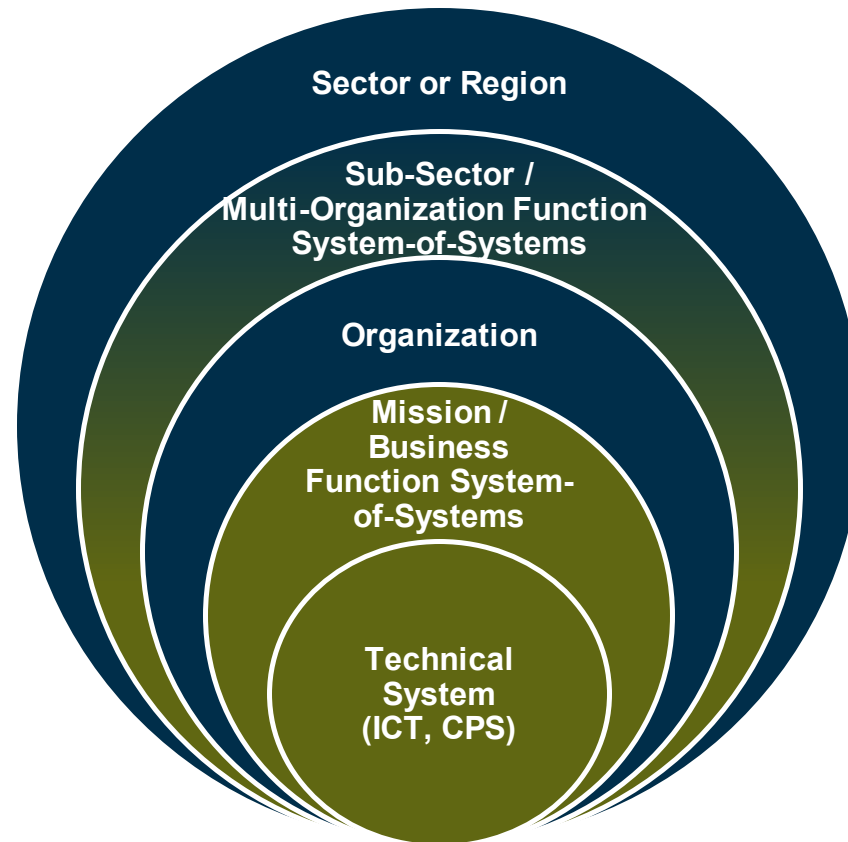
- **Steve Bishop**, *Head of Risk Information & Insurance, ORX*
- **Deborah Bodeau**, *Senior Principal Security Engineer, Cyber Solutions Division, The MITRE Corporation*
- **Todd Waszkelewicz**, *Assistant Vice President, Cybersecurity Policy, Federal Reserve Bank of New York*
- **Trevor Watkins**, *Risk & Control Manager, PNC*
- **Albert Olagbemi**, *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](mailto:dbodeau@mitre.org)**

# 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**

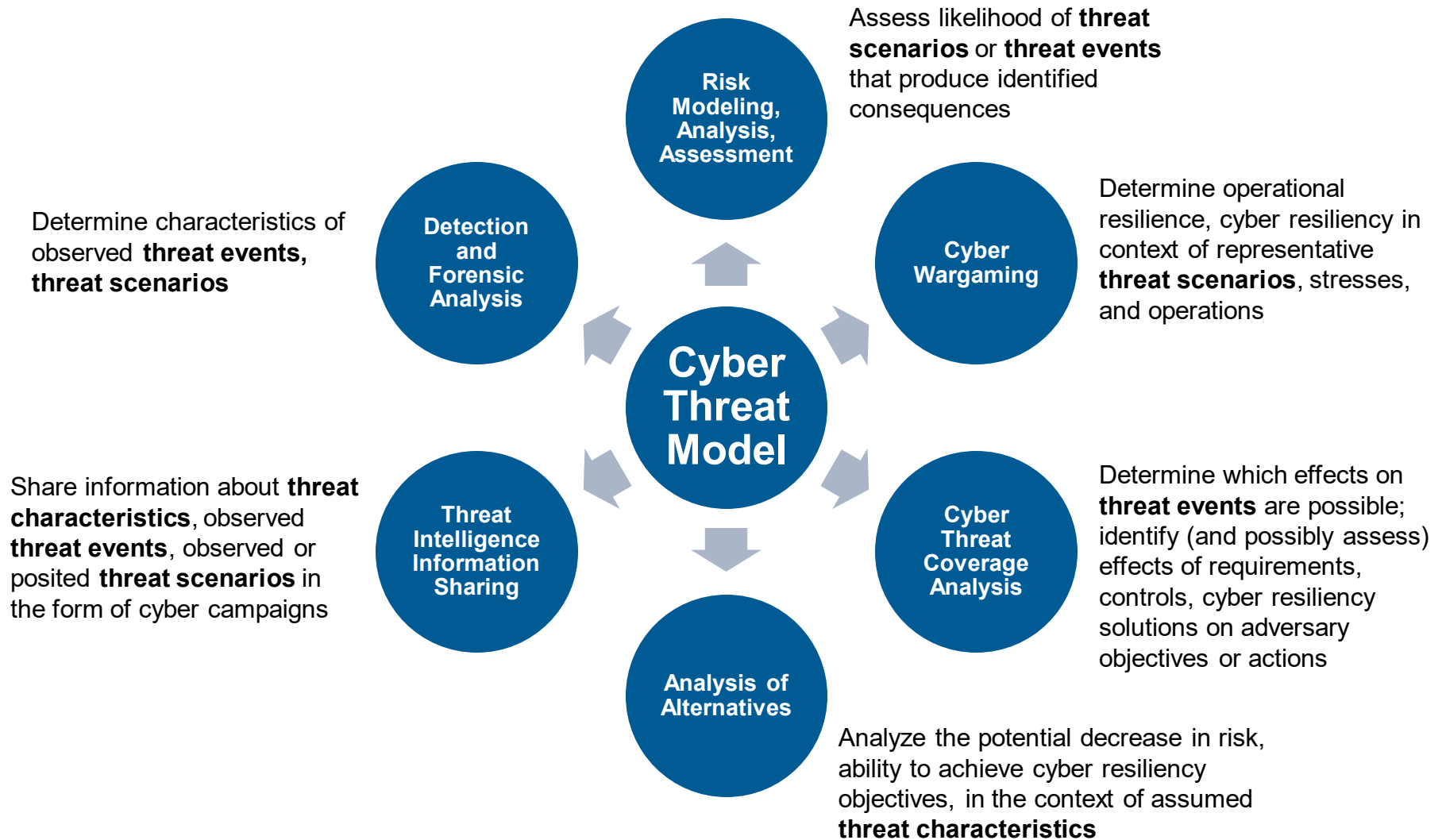


# Starting with Threats Can Simplify Discussions and Facilitate Characterization and Identification

---

- **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

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



# Threat Models Can Include Many Factors ...

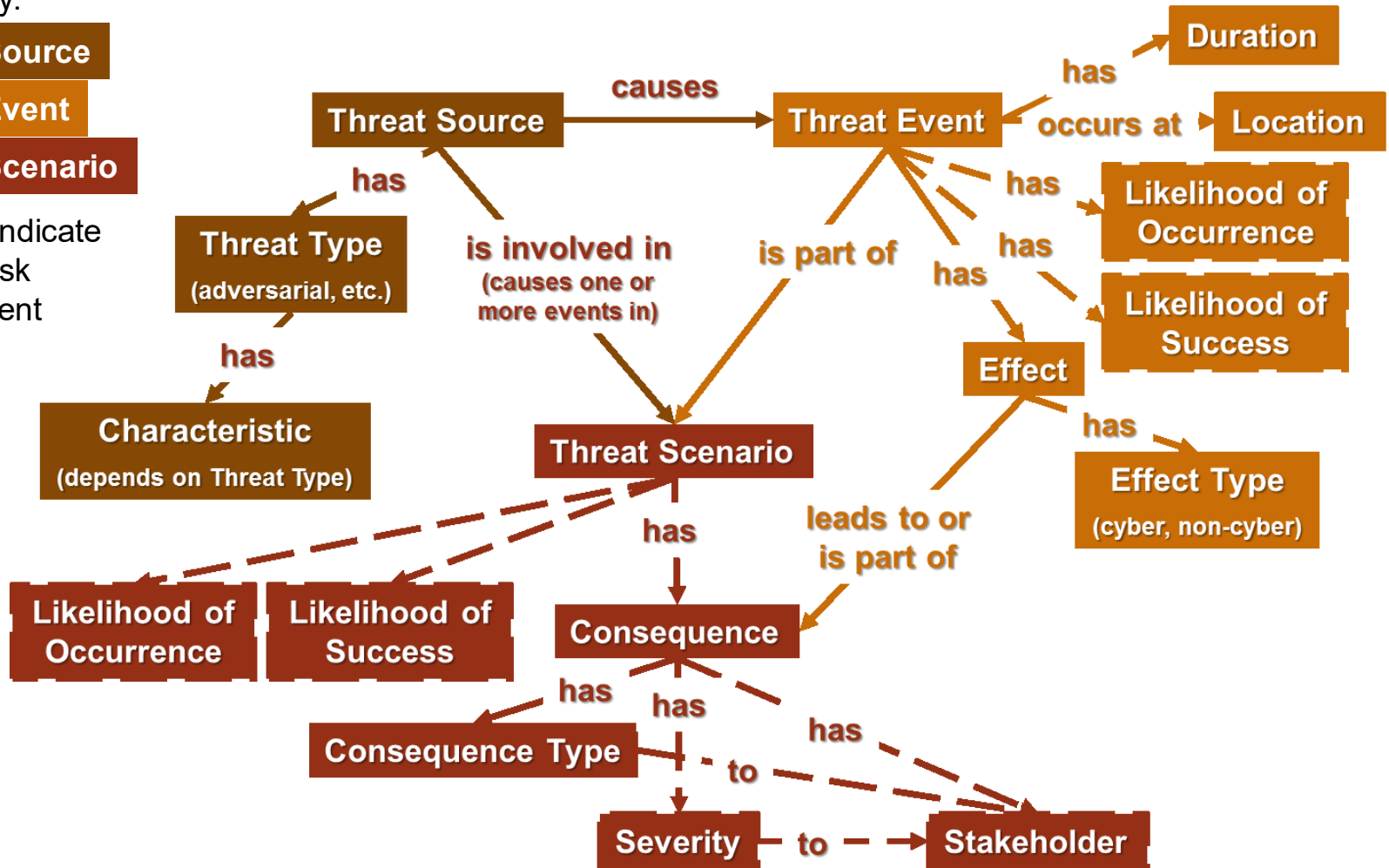
Color Key:

Threat Source

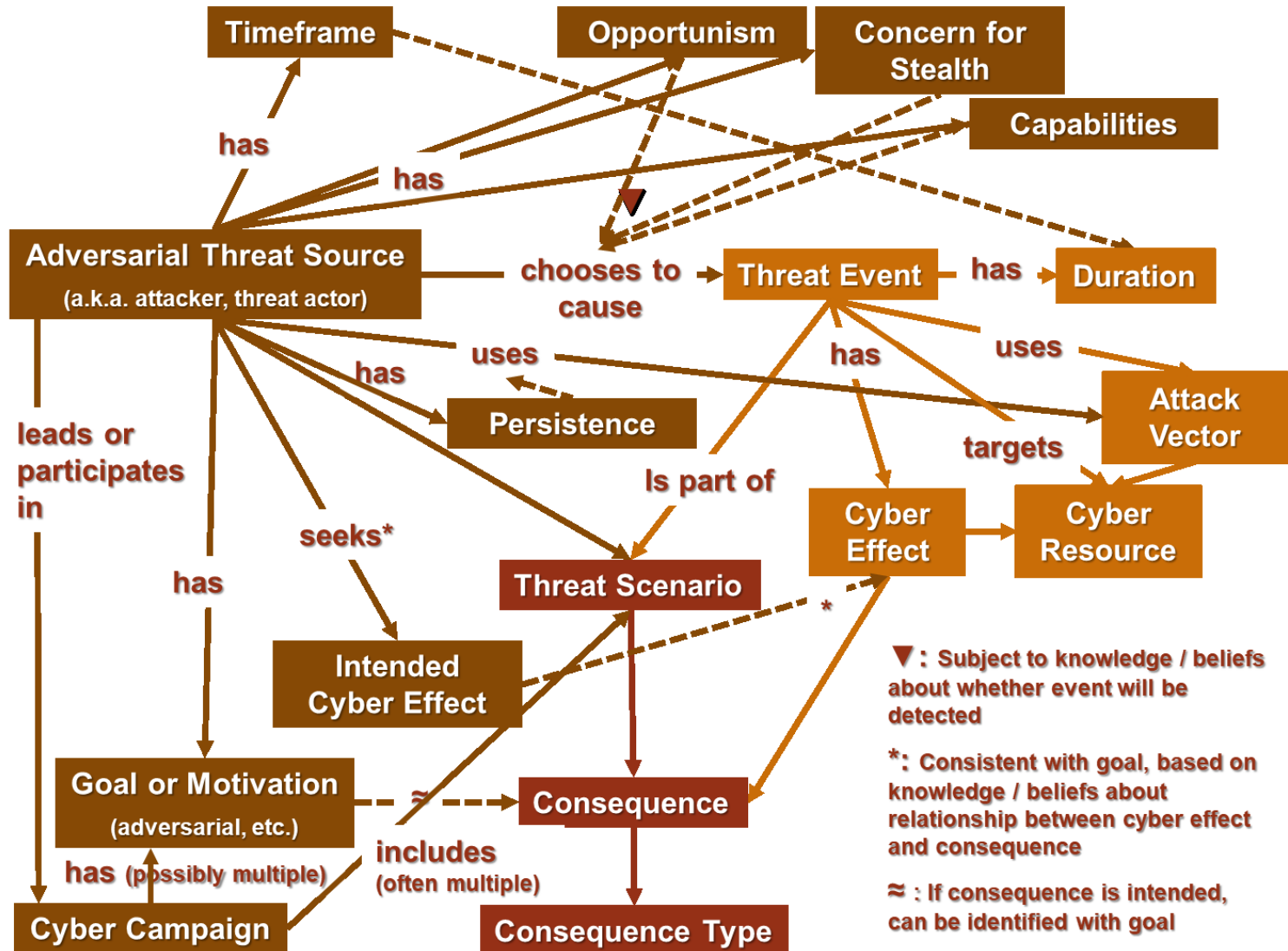
Threat Event

Threat Scenario

Dashes indicate links to risk assessment



# ... 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



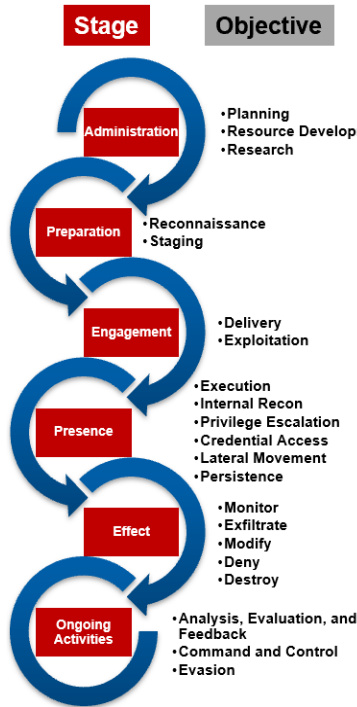
# One Common Theme ... Identify Threat Events Using a Framework Following the Structure of a Threat Scenario or Cyber Campaign



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



**Action**

- Examples of Research actions:
- Gather information
  - Identify capability gaps
  - Identify Information gaps

- Examples of Reconnaissance actions:
- Conduct social engineering
  - Scan devices
  - Scrape websites

- Examples of Delivery actions:
- Alter communication
  - Send malicious email
  - Use legitimate remote access

- Examples of Execution actions:
- Create scheduled tasks
  - Replace existing binaries
  - Write to disk

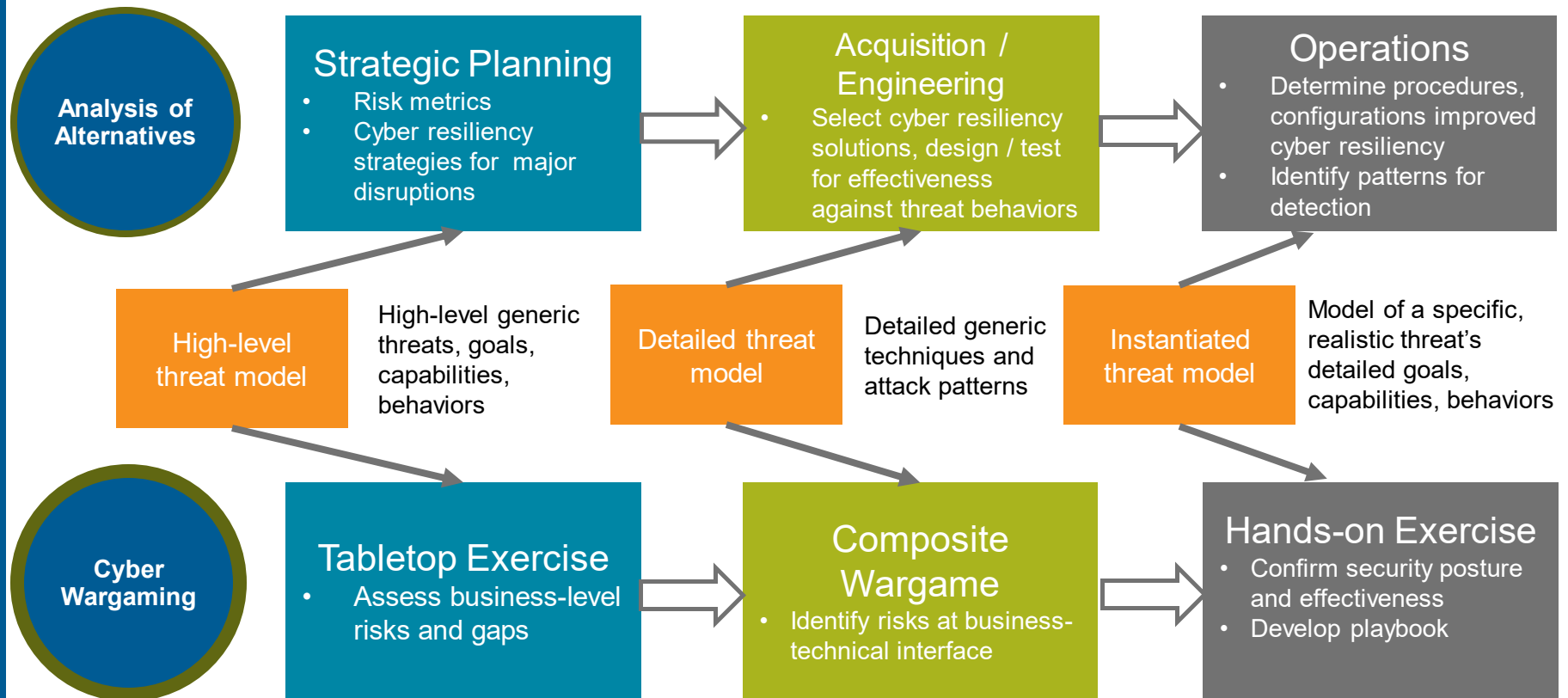
- Examples of Monitor actions:
- Activate recording
  - Log keystrokes

- Examples of Evasion actions:
- Block indicators or signatures
  - Obfuscate data
  - Remove toolkit

## 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 →	Execution	Internal Reconnaissance	Privilege Escalation	Credential Access	Lateral Movement	Persistence	
	Implementation Approach							
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	

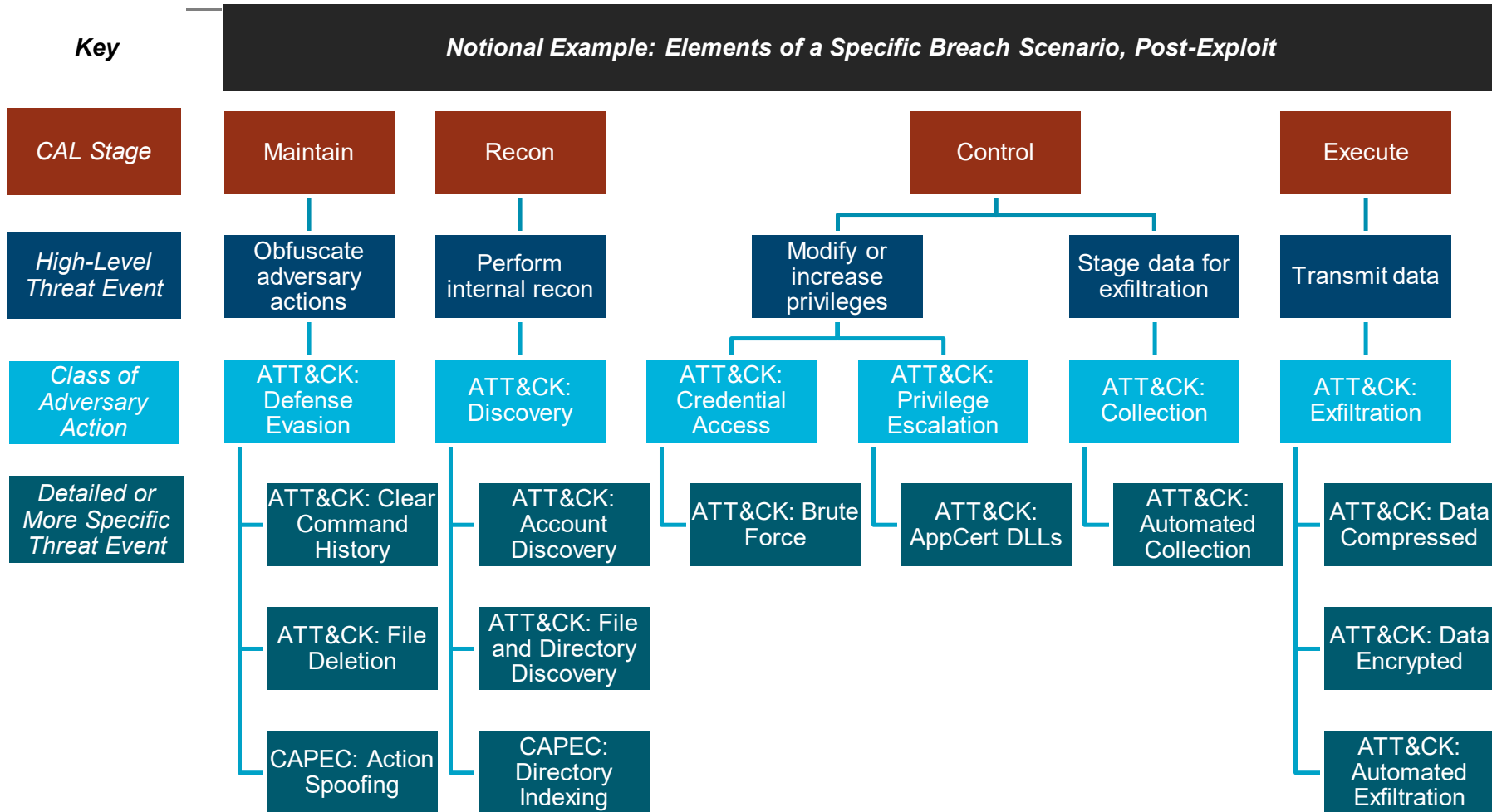
# A Common Framework for Identifying Cyber Threat Events Can Align Different Uses and Different Scales ...



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

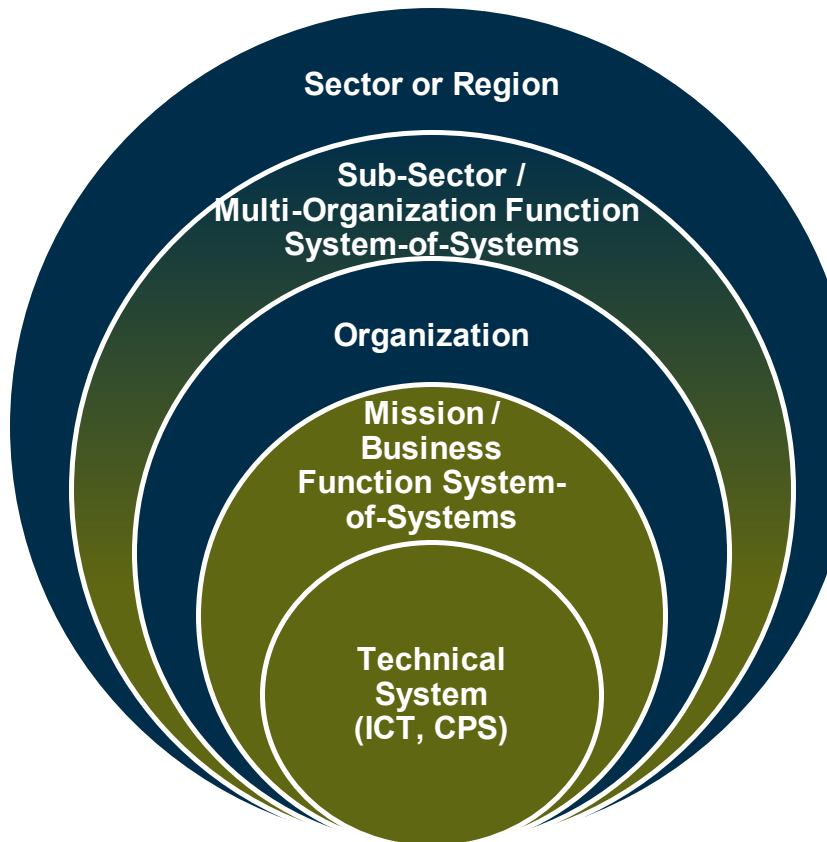


# ... As Long as the Threat Modeling Framework Supports Refinement and Decomposition ...



**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>

The MITRE logo consists of the word "MITRE" in a bold, blue, sans-serif font, centered within a solid black rectangular background.

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](http://www.mitre.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 Olagbemi**, *Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond*





FEDERAL RESERVE BANK *of* NEW YORK

# 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

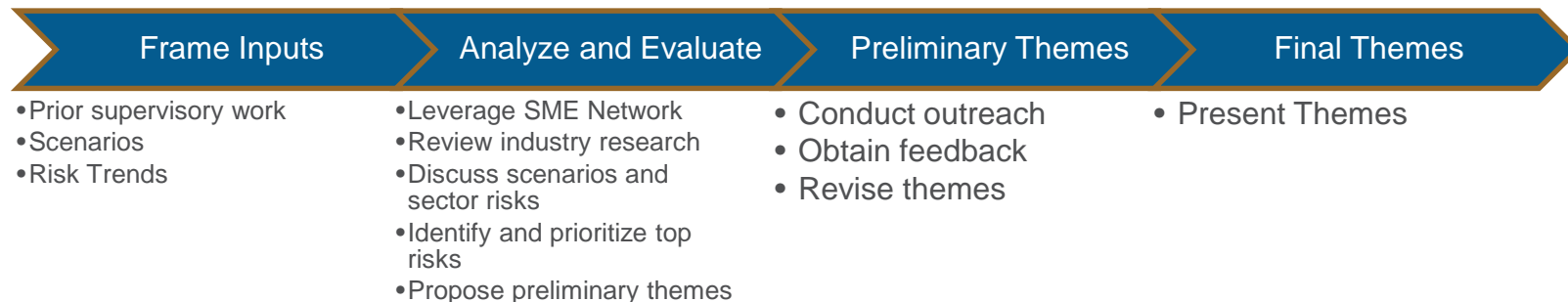
## Examples of key initiatives to strengthen cyber risk identification

- 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

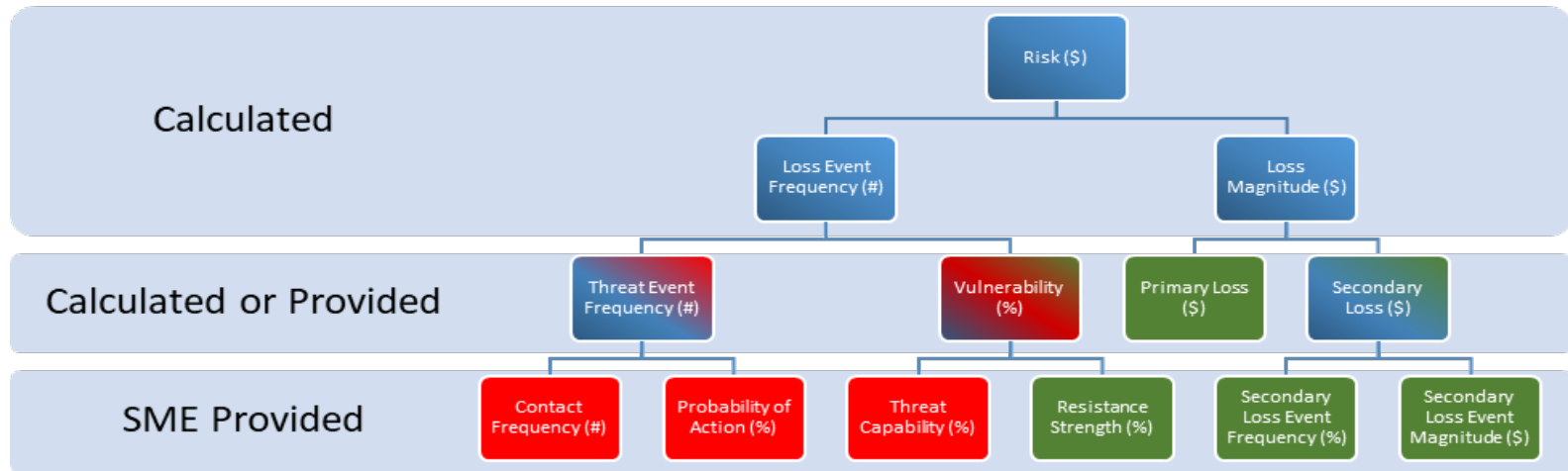


- One component of the process is to conduct scenario analysis to identify and prioritize top risks
- Utilize industry framework to estimate risks (e.g., Factor Analysis of Information Risk (FAIR))
- Enumerate plausible and concerning cybersecurity-related risk scenarios for the U.S. financial sector
- 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

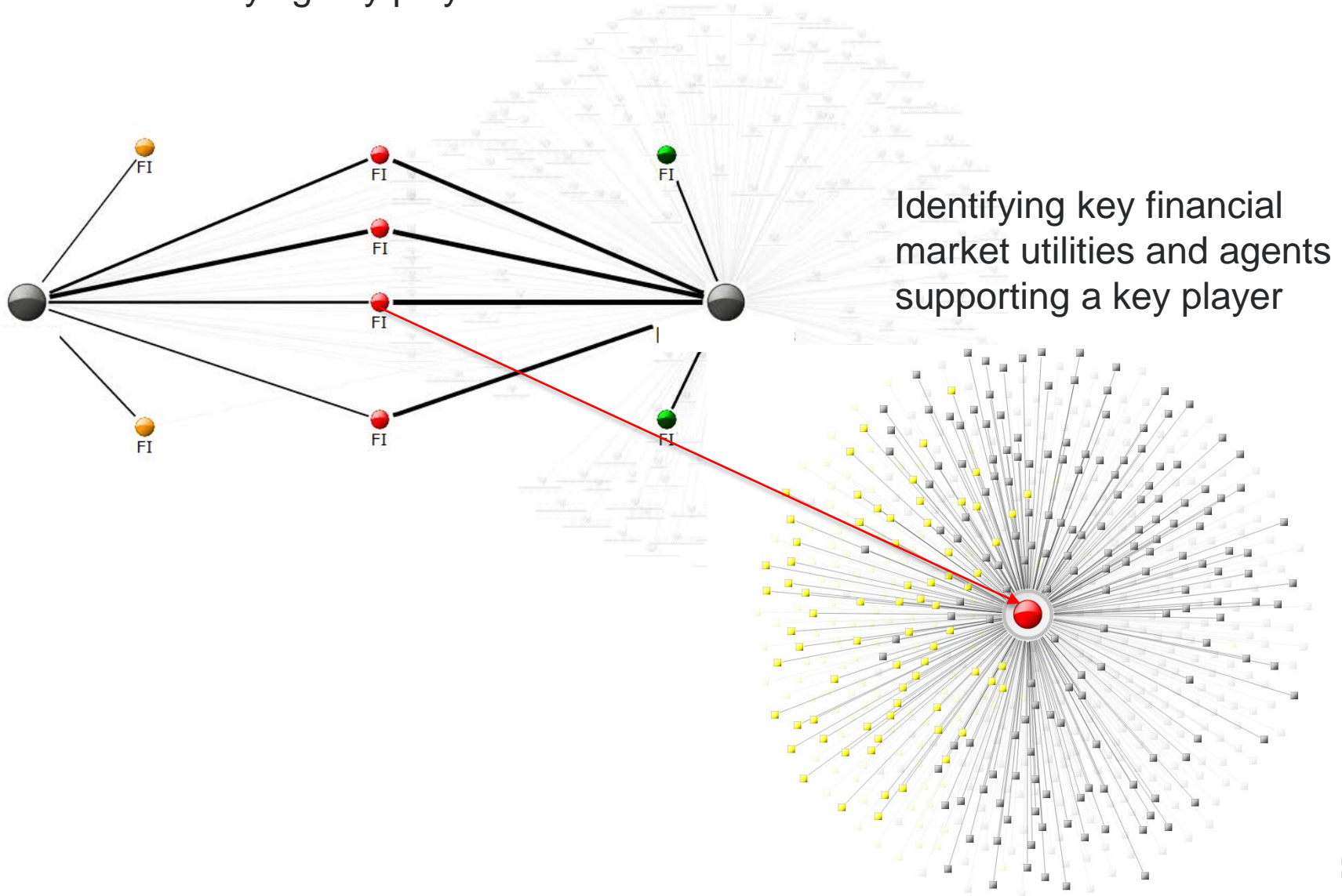
# Mapping Financial Sector Interconnectedness

- 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?



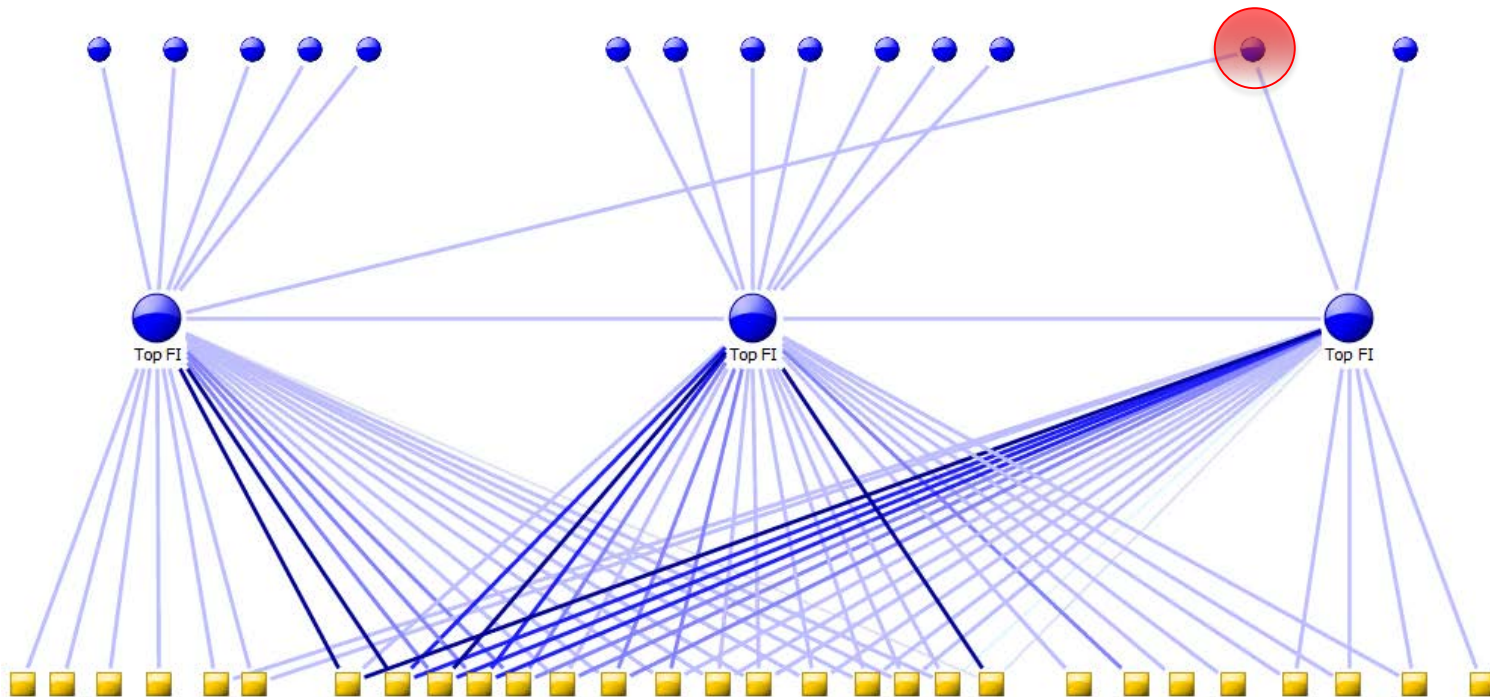
# Analyzing the breadth, depth and complexity of Interconnectedness

Identifying key players



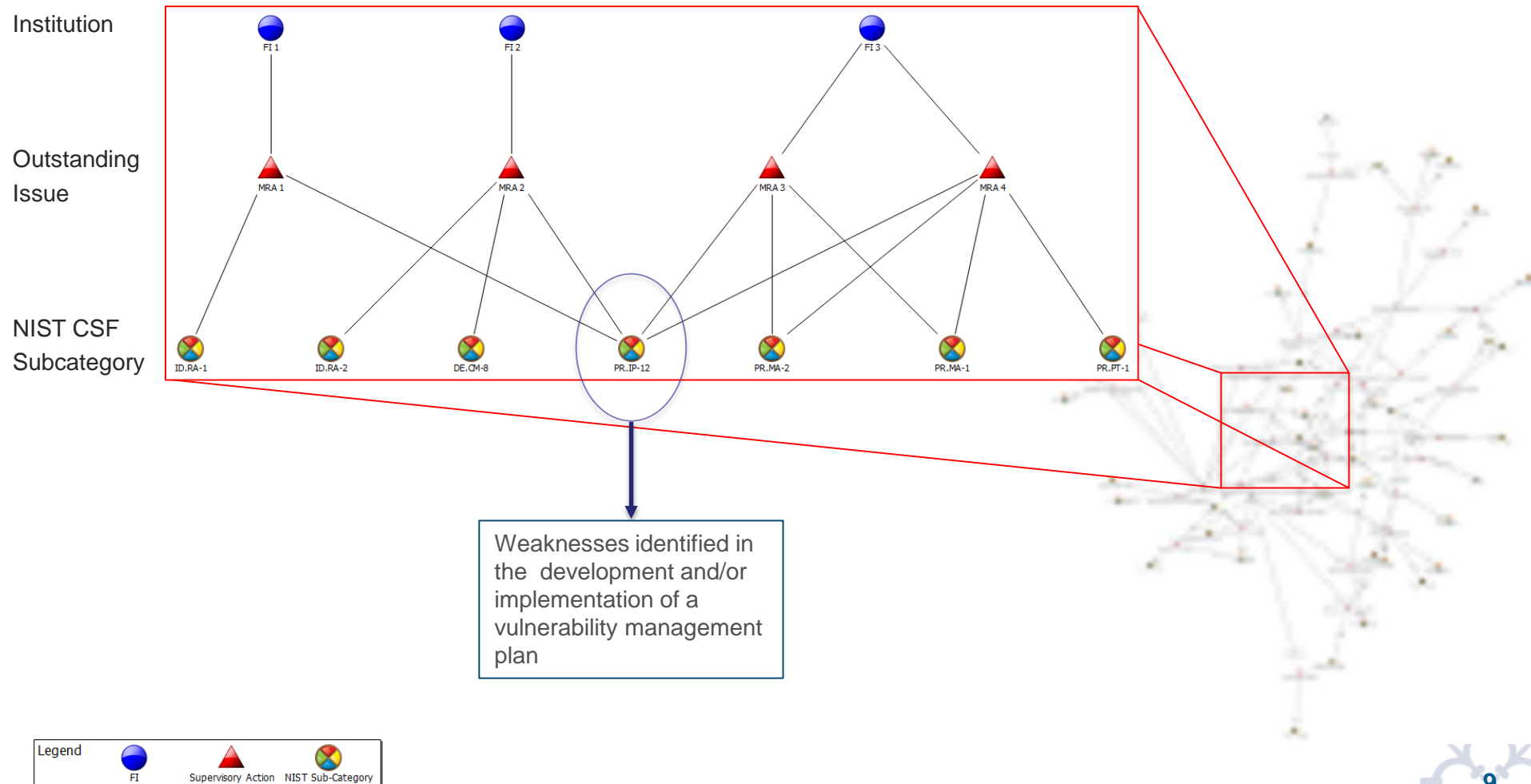
# Identifying key dependencies

- 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 Olagbemi**, *Advanced Bank Examiner, Cybersecurity Risk Specialist, Federal Reserve Bank of Richmond*



# Cyber Risk Workshop

Identification and Classification



## ➤ 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.

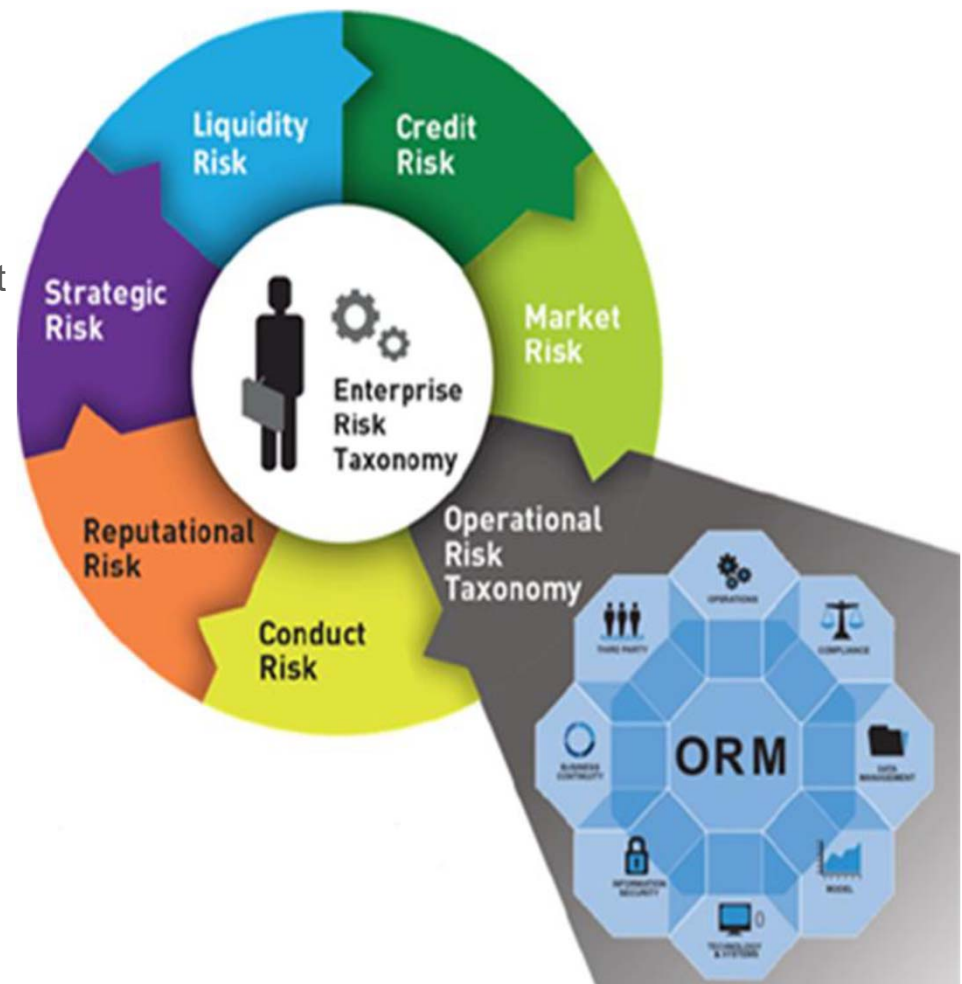










Figure 1: Risk Taxonomies

# PNC Operational Risk Domains

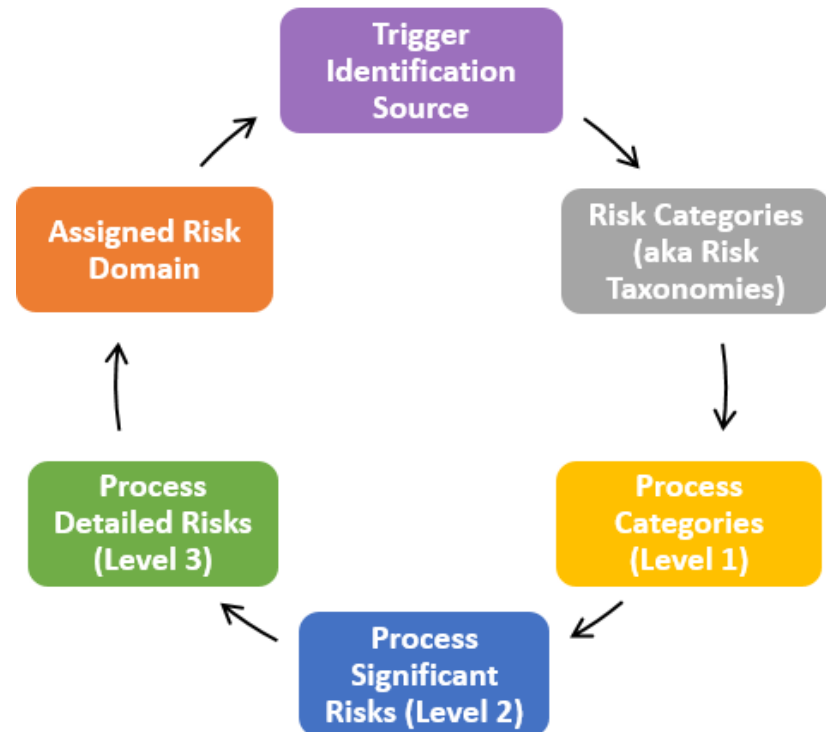
Icon	Domain	Focused on managing:
 OPERATIONS	Operations <i>(People/ Processes)</i>	Risk resulting from inadequate or failed internal processes, misconduct or errors of people and fraud
 COMPLIANCE	Compliance	Risk associated with failure to comply with applicable laws and regulations or contractual obligations
 DATA MANAGEMENT	Data Management	Risk associated with incomplete or inaccurate data
 MODEL	Model	Risk associated with the design, implementation, and ongoing use and management of a model
 TECHNOLOGY & SYSTEMS	Technology & Systems	Risk associated with use, operation and adoption of technology
 INFORMATION SECURITY	Information Security	Risk resulting from the failure to protect information and ensure appropriate access to, and use and handling of information assets
 BUSINESS CONTINUITY	Business Continuity	Risk of potential disruptive events to business activities
 THIRD PARTY MANAGEMENT	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
    - Identification and Investigation
    - Action Planning and Management Response
    - Monitoring and Reporting
    - Resolution

## Classification



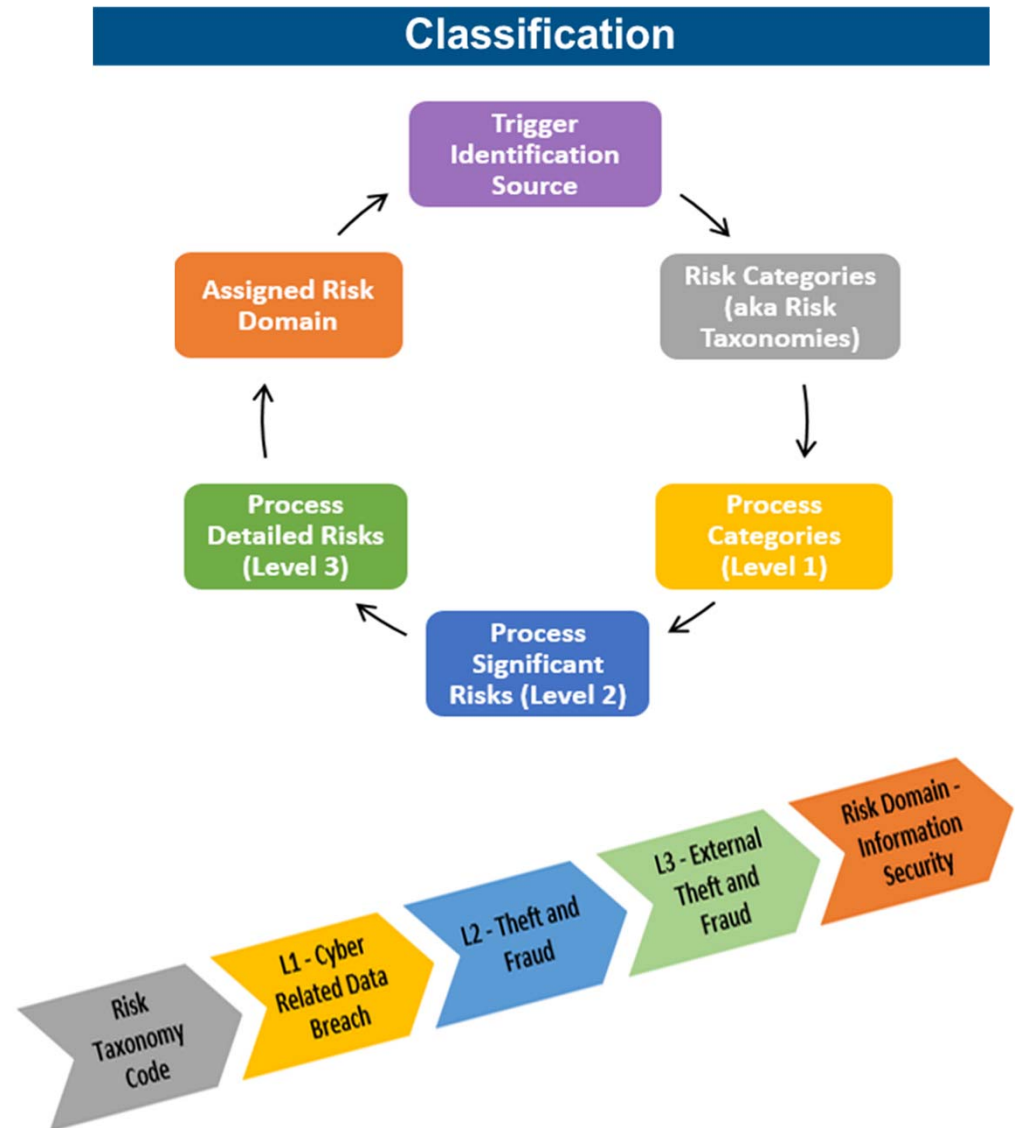
# ELD Examples

## 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

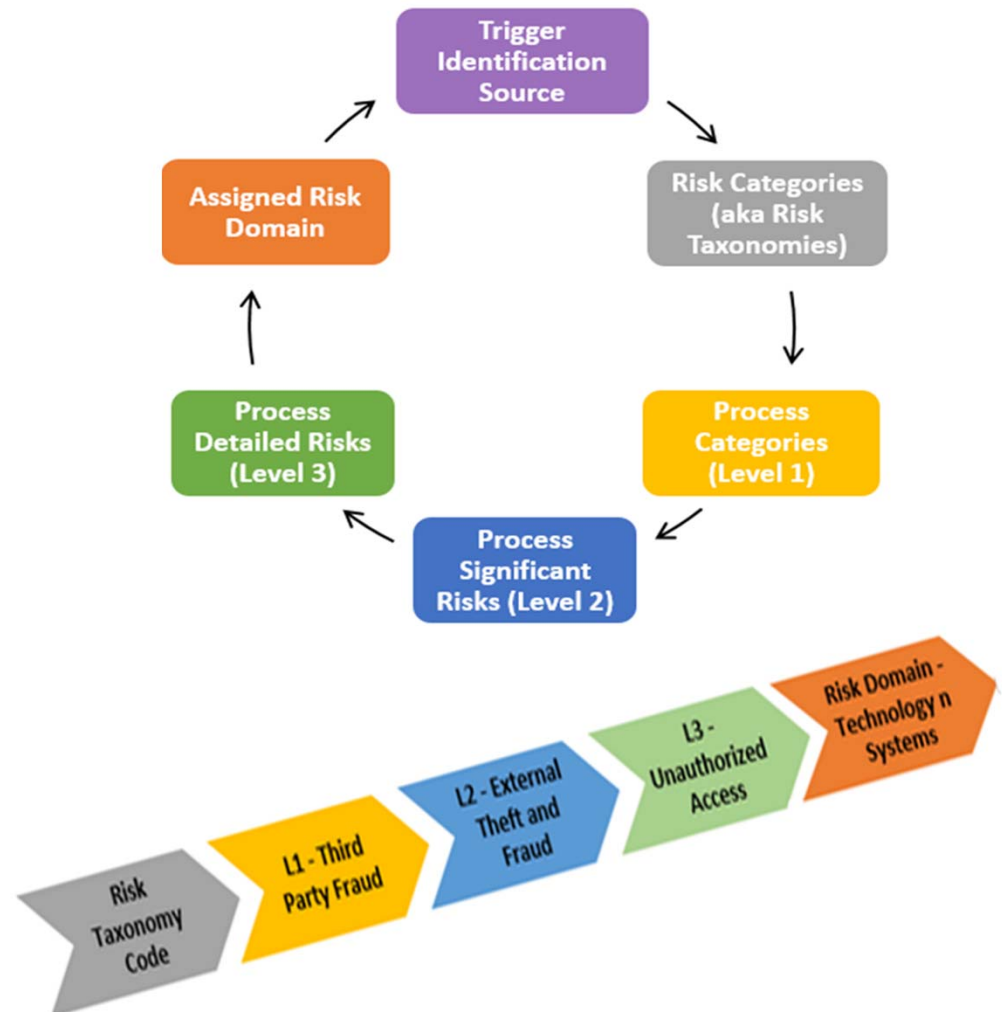
On 24 August 2018, BuzzFeed News reported that a **security flaw in Apple's online store** had inadvertently exposed over 77 million T-Mobile **customer account PINs**, which often constitute the last four digits of a customer's Social Security Number (SSN).

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.

## Classification





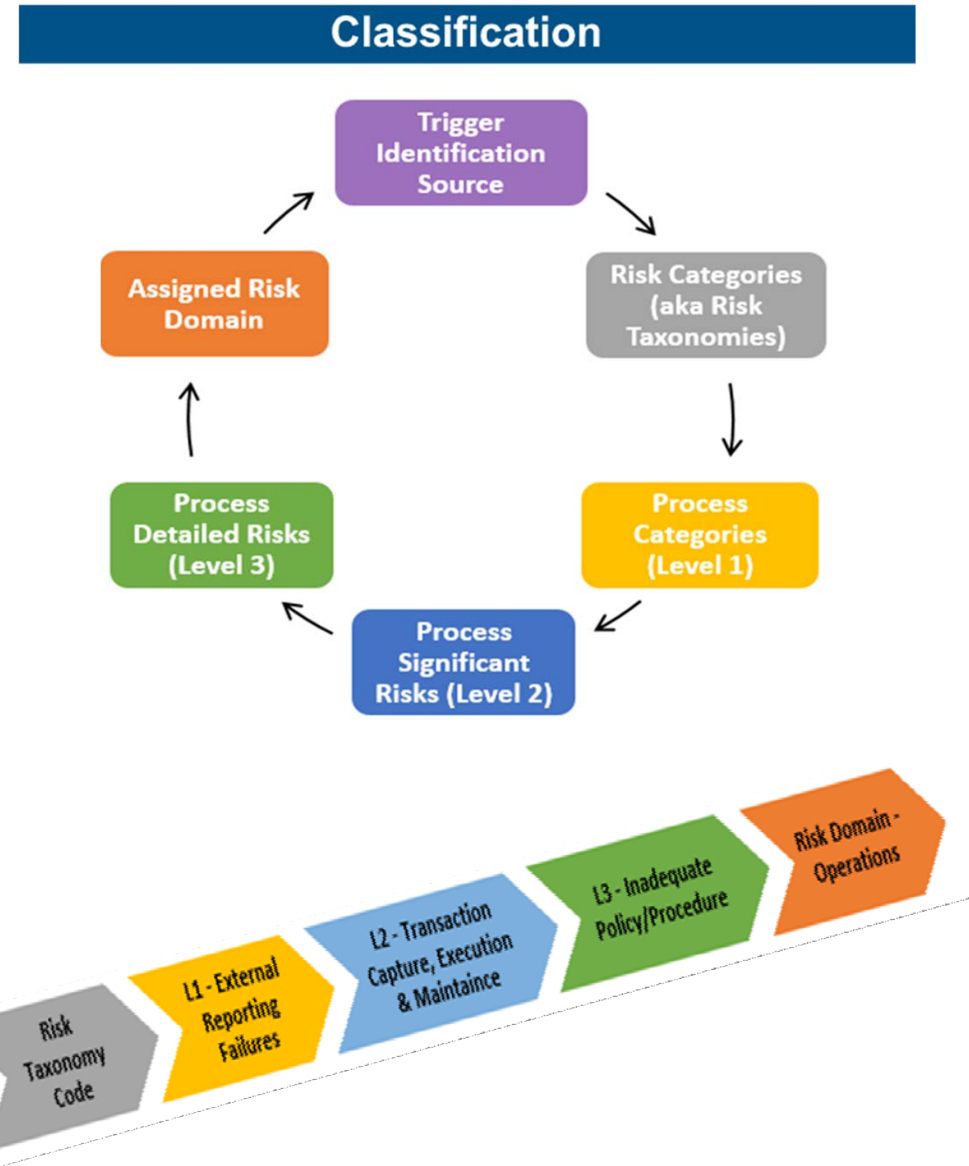
# ELD Examples

## 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