Cyber Quantification

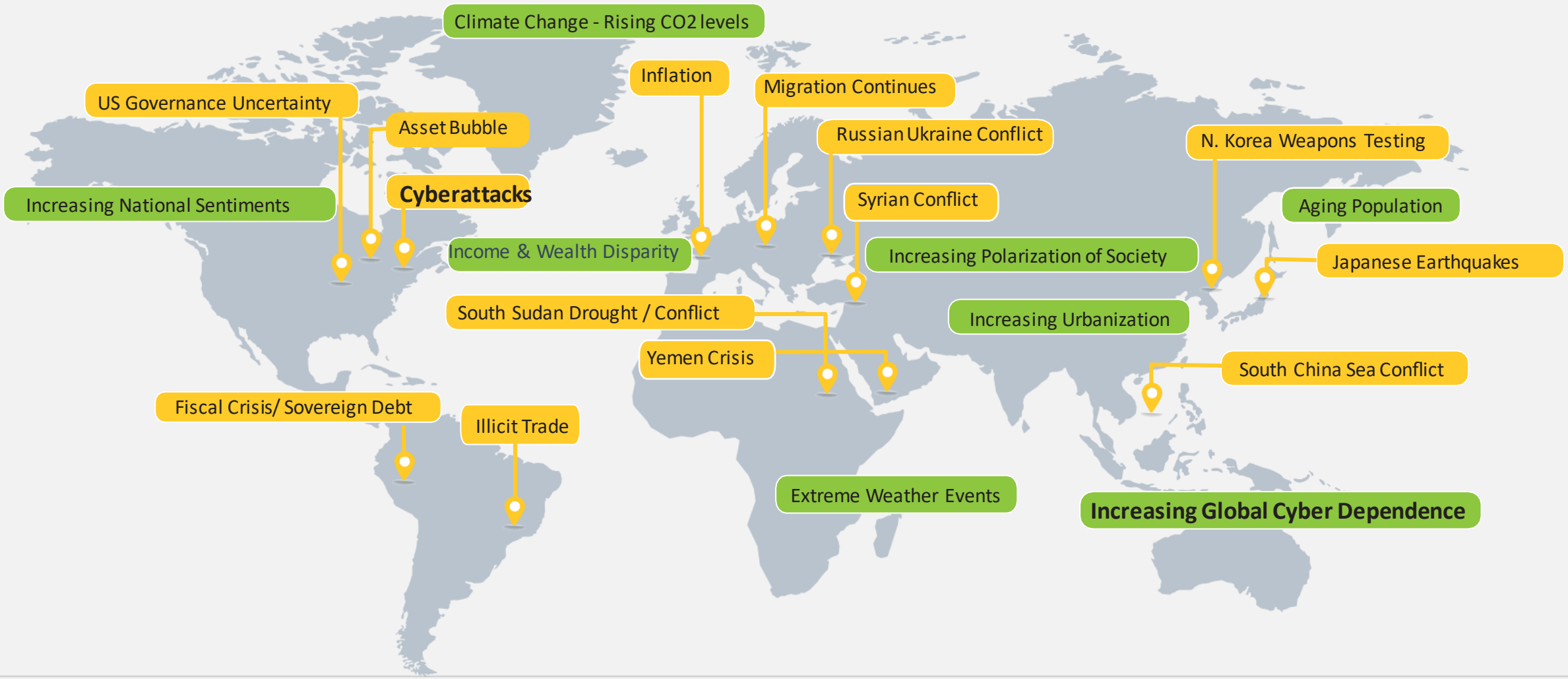
Non-financial Risk Management

GRAFT & DAIR

Lois Tullo
GRI
Email: ltullo@globalriskinstitute.org

Sohail Farooq
BankingBook Analytics (BBA)
Email: sohail@bba.to

Drivers of nonfinancial risk



Nonfinancial Risk Regulatory Expectations

OSFI's 2020 plan include the goal for Federally regulated financial institutions and pension plans to be better prepared to identify and develop resilience to non-financial risks before they negatively affect their financial condition.

OSFI is pursuing efforts in the oversight of non-financial risks to support their effective management by FRFIs and pension plans. Key objectives related to this priority include:

- Continuing to develop OSFI's regulatory and supervisory approaches to technology risks, including digitization, cloud computing, risk modelling and cyber risk.

Nonfinancial Risk Regulatory Expectations

The EU has issued The Non-Financial Reporting Directive (2014/95/EU) requires large public interest entities with over 500 employees (listed companies, banks, and insurance companies) to disclose certain non-financial information.

- A company is required to disclose information on environmental, social and employee matters, respect for human rights, and bribery and corruption, to the extent that such information is necessary for an understanding of the company's development, performance, position and impact of its activities.
- Non-Financial Risk information should be reported if it is necessary for an understanding of the development, performance and position of the company.

Non-Financial Risk Management Using the Global Risks and Trends Framework (GRAFT)

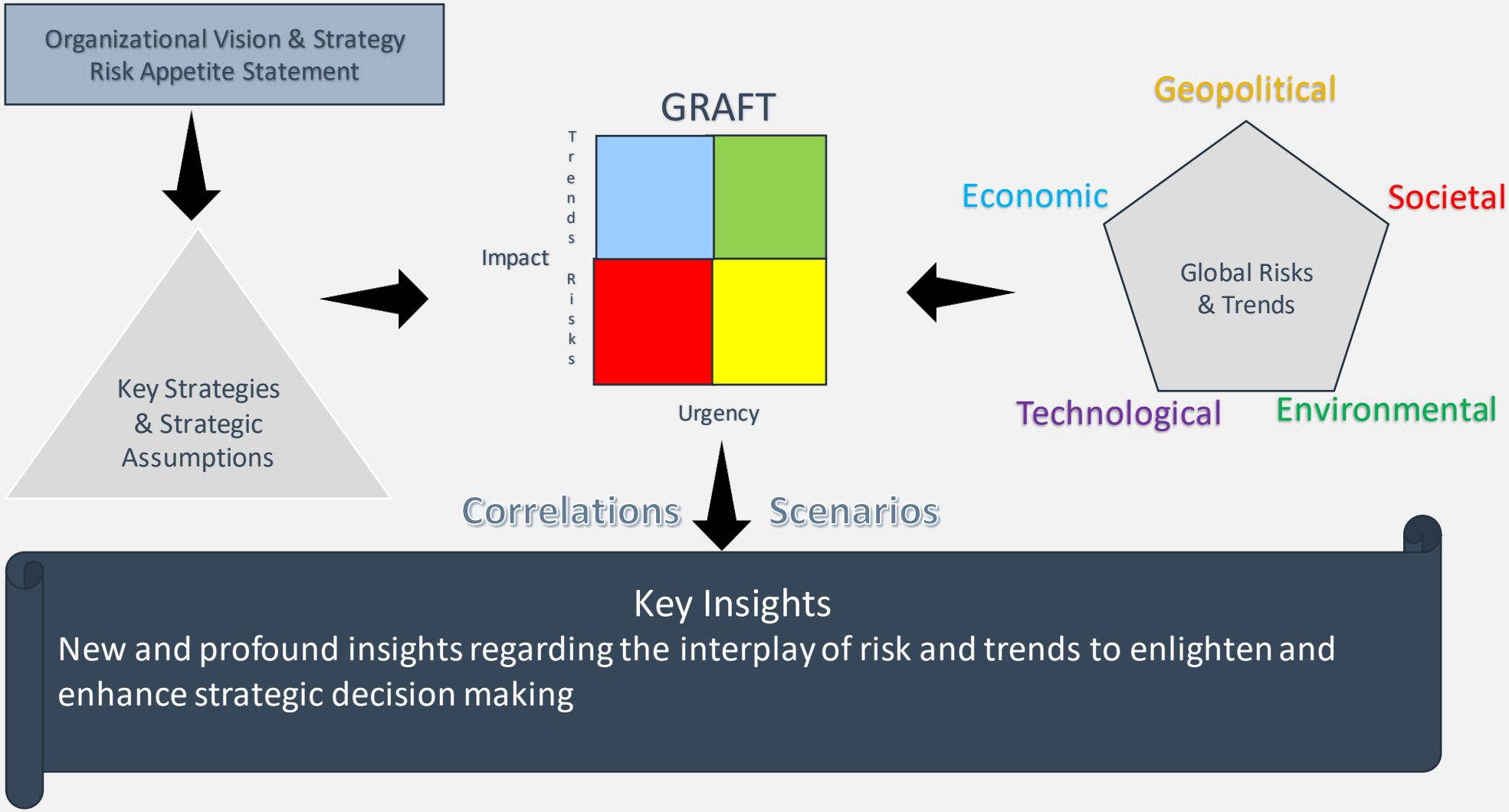
GRAFT is a new approach designed to help organizations including banks, insurance companies, pension funds and asset managers identify, assess and respond to Non-Financial Risk.

- Used in order to avoid pitfalls that could threaten an organization's long-term survival or conversely to leverage for the benefit of the organization.

A method that:

- Compares the assumptions supporting your strategic plan with the correlations of prioritized Global Risks and Trends to identify Key Insights for the organization;
- Promotes a common language, shared understanding and quantification of the implications of Global Risks and Trends on your organization's strategic plan; and
- Defines the roles of the BOD, Sr Mgt, RM, BU, IA. And enables more informed decisions making process.

Overview of Global Risks and Trends Framework for Nonfinancial Risk Management



GRAFT Implementation Continuum

In managing cyber risk, focus is pre-dominantly on identifying causes and managing them

Causes

- Denial of service
- Web-based attacks
- Malicious insiders
- Phishing and social engineering
- Stolen devices
- .....
- .....
- Malware
- Viruses, worms, trojans

- Buy more bandwidth. …
- Build redundancy into your infrastructure
- Configure your network hardware against DDoS attacks. …
- Deploy anti-DDoS hardware and software modules. …
- Deploy a DDoS protection appliance. …
- Protect your DNS servers….
- Using prepared statements with parameterized queries. This ensures that the SQL code is defined first and then the queries are passed later. The effect is that the database can differentiate between SQL code and SQL data. This means that the code is not vulnerable to SQL injection …
- …….

Impact

A balanced approach is needed to classify and model losses attributed to cyber events

Direct

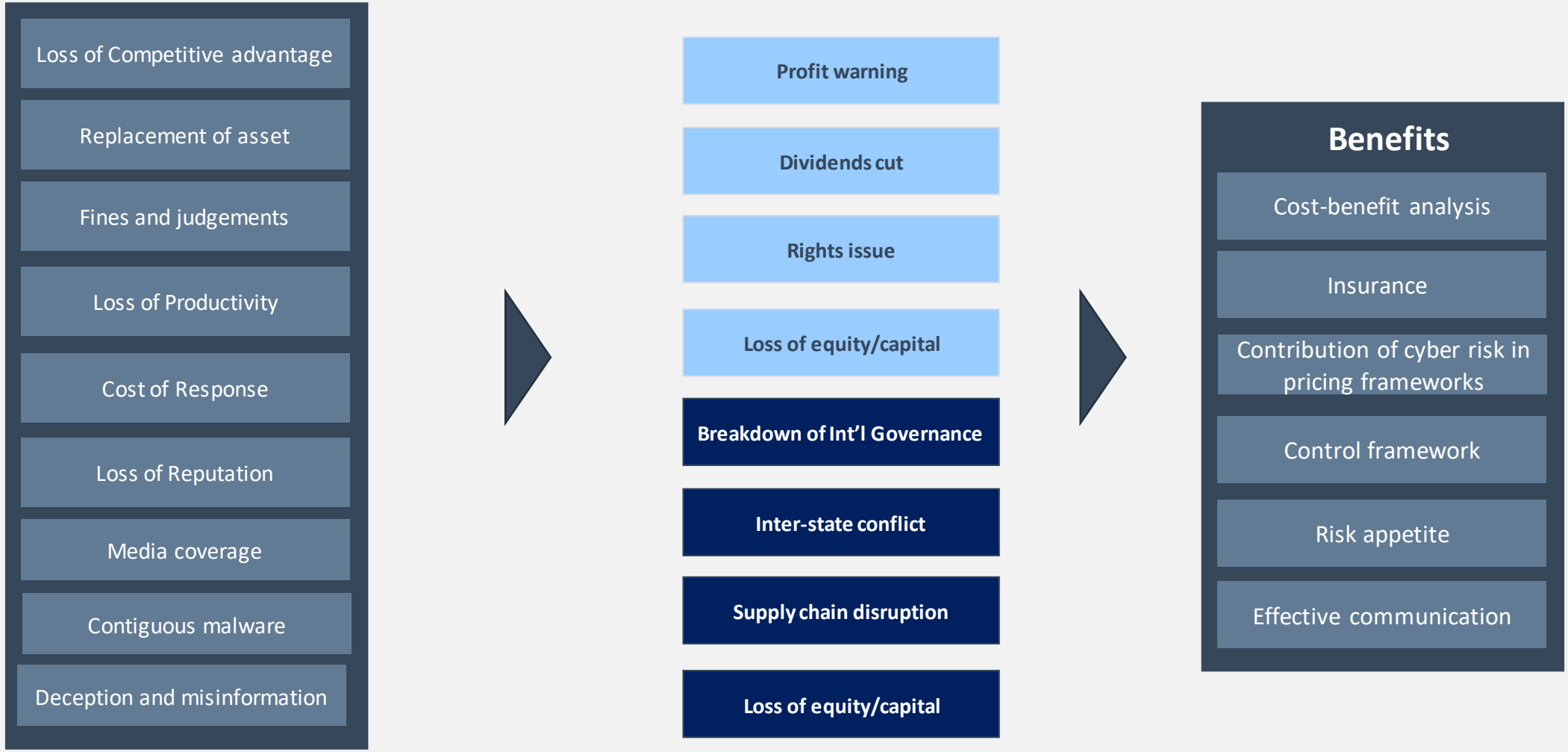
- Profit warning
- Dividends cut
- Rights issue
- Losses

Indirect

- Media coverage
- Loss of credibility and customer-base
- Reputational loss
- Drop in rating/Share price

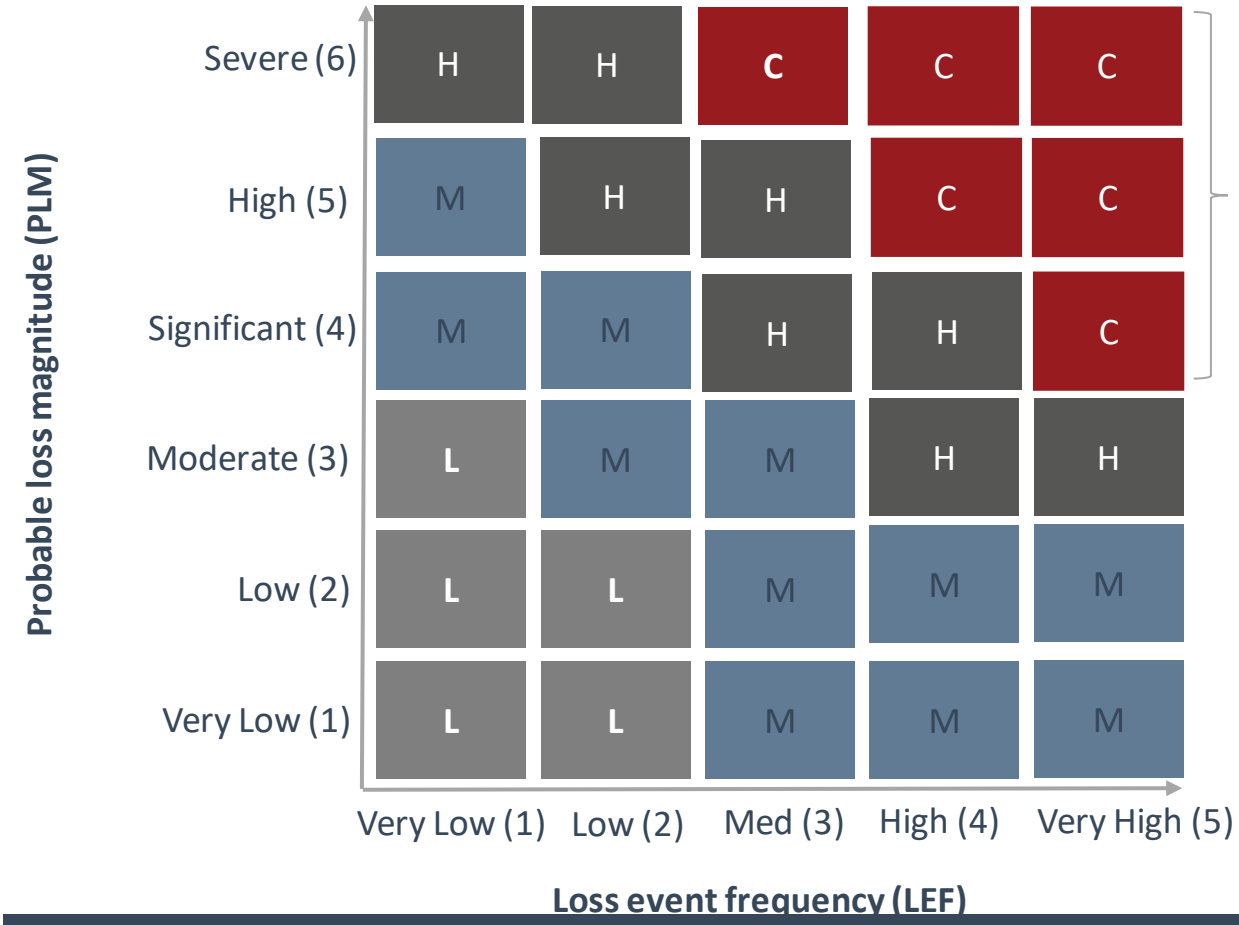
Quantifying cyber-attack losses

Developing an impact-based approach



Practice survey: Factor Analysis of Information Risk (FAIR) approach

Risk = *f(probable frequency, probable magnitude)*



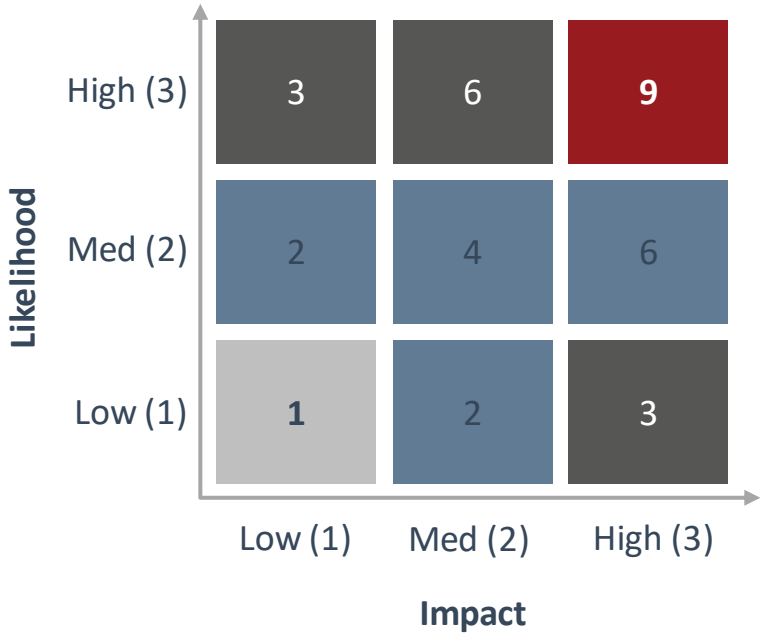
Worst case outcomes by FAIR: Type of loss that occurs hundreds of times a year and each time causes billion dollar in losses

Challenge with the with the modelling of FAIR approach

- Views events in terms of one likelihood parameter and one impact parameter rather than the entire set of such pairs that in fact describe an event
- Focuses on "phantom" risks (high likelihood, high impact) and gives insufficient attention to real risks (low likelihood, high impact)
- Fails to recognize that it is the potential high impact but low likelihood manifestation of each type of event that poses the challenge in terms of risk quantification (capital)
  - Can put you out of business or cause severe harm
  - Difficult to understand and prioritise in advance
- Fails to capture the fact that it is events with significant low likelihood but high impact "tails" that pose the challenge rather than events for which a low likelihood and high impact has arbitrarily been picked

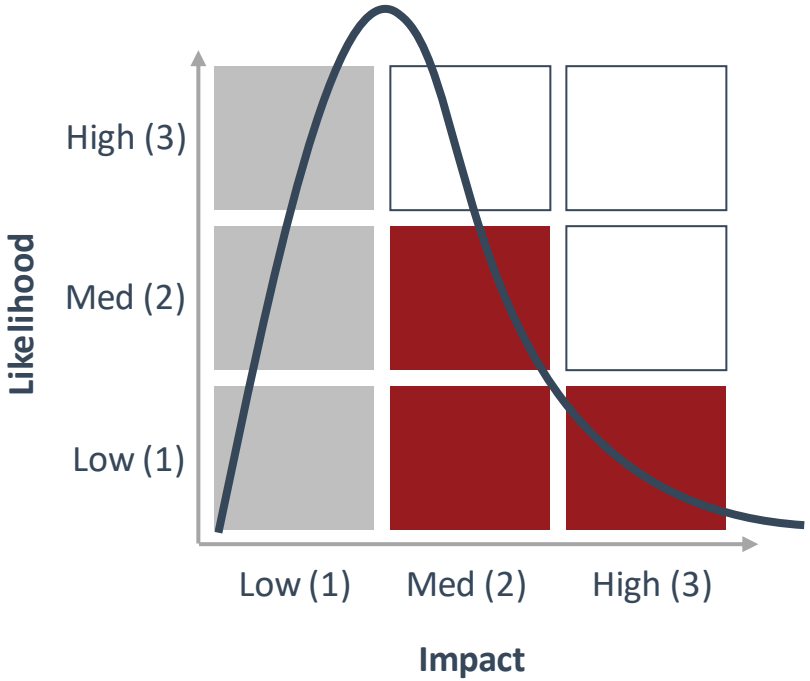
Difference between FAIR and DAIR

FAIR approach



FAIR describes cyber risk as probability-weighted severity or "mean severity"

Impact-based approach - DAIR



DAIR defines cyber risk impact modelling in terms of severity or as Unexpected Loss

Distribution Analysis for Information Risk (DAIR) framework.

DAIR is a cyber quantification methodology that maps cyber events with a hierarchical risk taxonomy to evaluate the impact of cyber loss events.

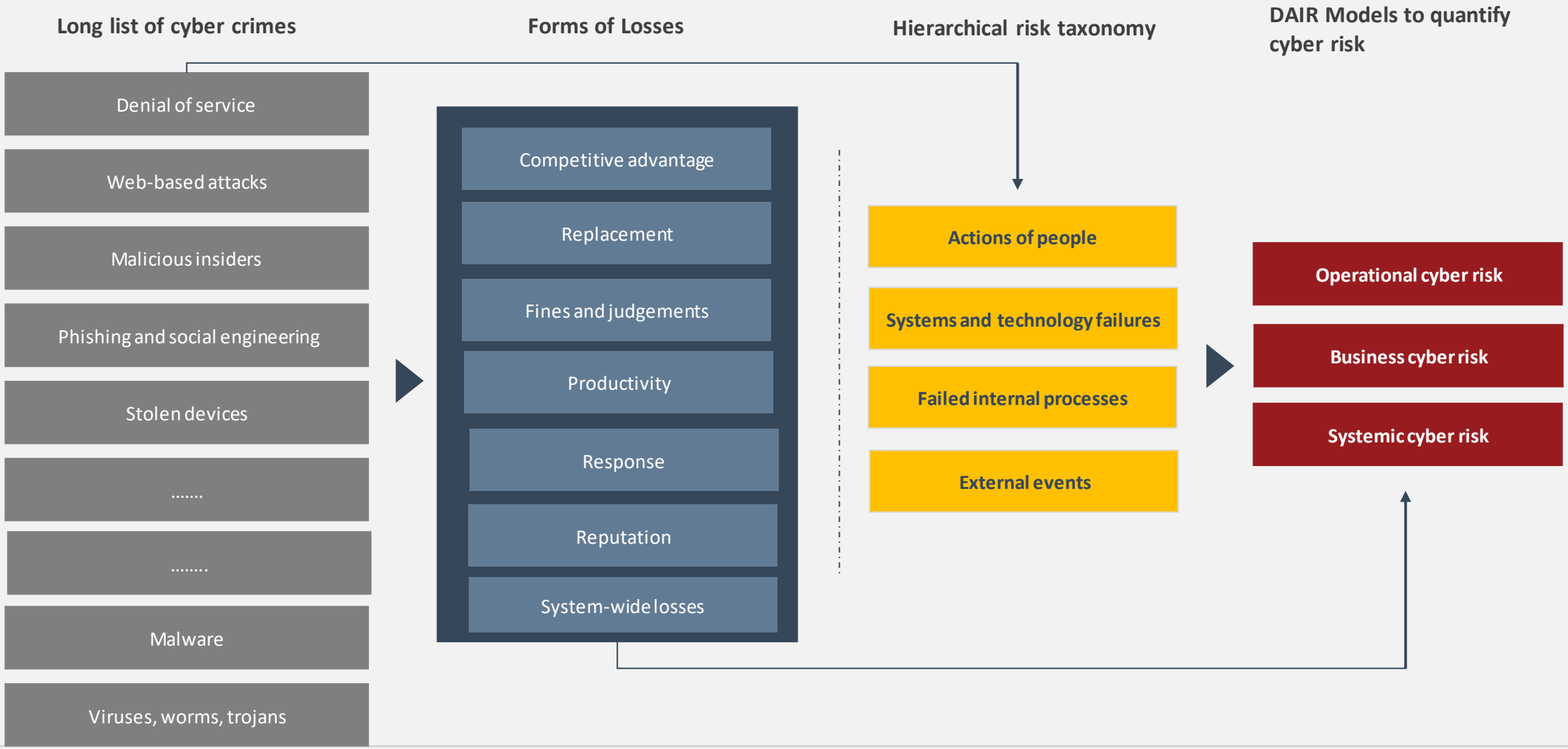
DAIR enhances a firm's understanding of cyber risk exposure by:

- highlighting where the highest dollar level of threat may be coming from;
- helping management and boards set and monitor their cyber risk appetite, make decisions based on the organization's risk tolerance level;
- helping to make better informed decisions relating to expenditures on cyber risk mitigation, insurance and internal capital requirement; and
- helping the management demonstrate to regulators that they are managing cyber risk in a comprehensive way

Variants of Cyber Loss Factors and Meta-Risk Classification

Key Variants of Cyber Loss	Organization-wide Classifications
• Loss of cyber and/or physical property due to a cyber event	• Operational risk: Within the context of operational risk, cyber risk can be defined as "operational risk to information technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems". Basel's includes legal risk, but excludes strategic and reputational risk. [BIS 2006]
• Loss of reputation and/or damage to stakeholders' perception of an institution's franchise due to a cyber event	• Business risk: Business risk is the risk of having costs higher than revenues due to shocks to margins, volumes or costs.
• Loss of cyber and/or physical property due to contagion or systemic event caused by a cyber event, e.g., breakdown of international governance, cyber warfare	• Systemic risk: Systemic risk is the risk of disruption to financial services that is (i) caused by an impairment of all or parts of the financial system and (ii) has the potential to have serious negative consequences for the real economy. Fundamental to the definition is the notion of negative externalities from a disruption or failure in a financial institution, market or instrument. [BofE 2019]

Mapping Cyber Events With DIAR Hierarchical Framework



- **Operational cyber risk**

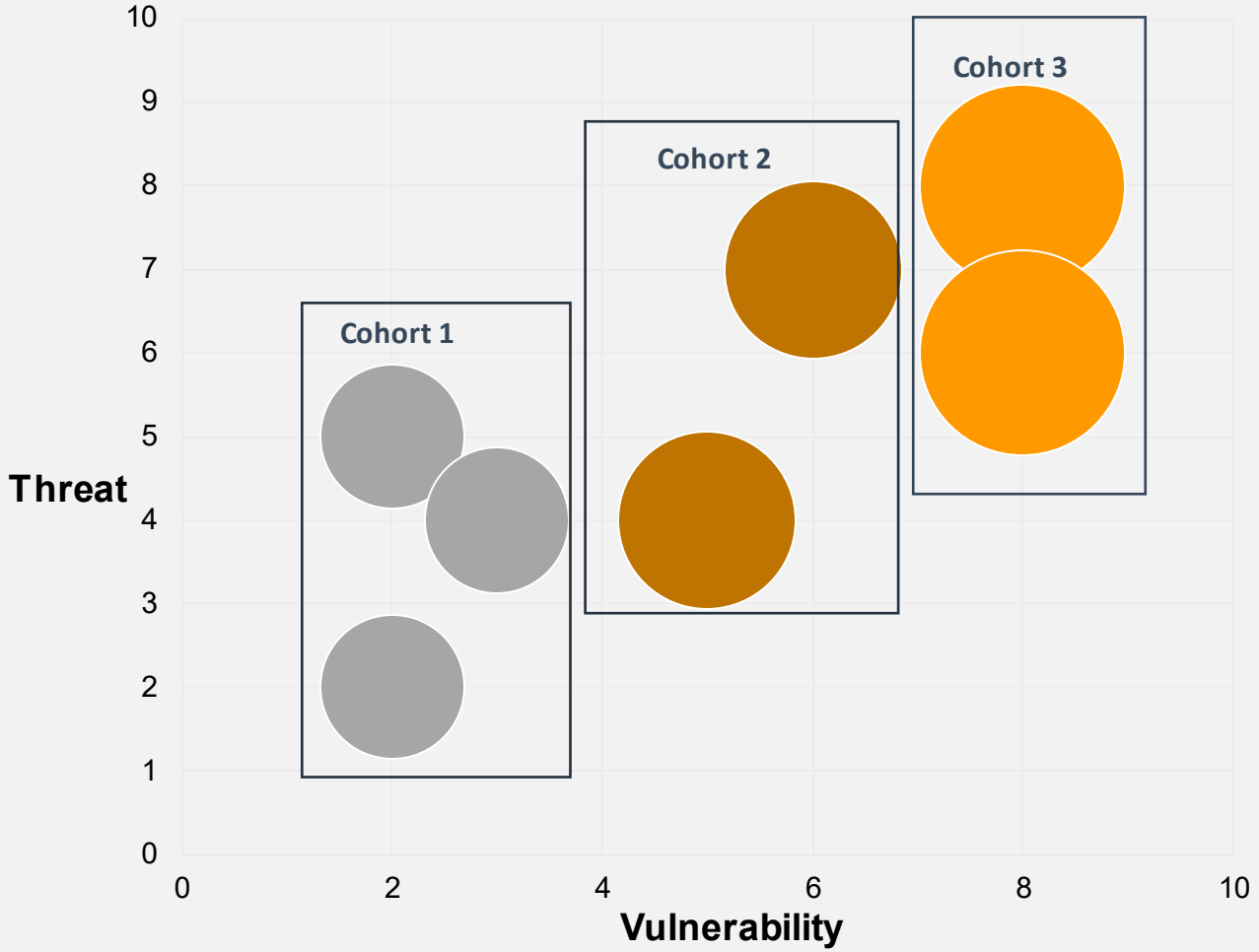
Business cyber risk

Systemic cyber risk

Operational Cyber Risk Quantification Steps

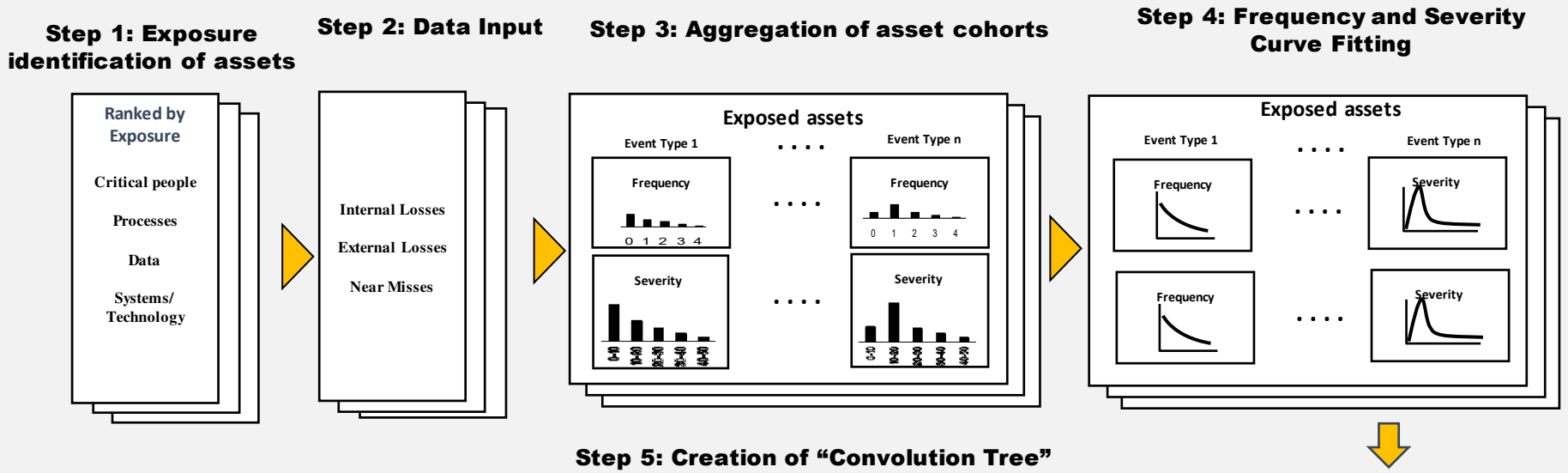
1. Asset Bucketing
2. Scenario Analysis
3. Frequency Distribution
4. Severity Distribution
5. Convolution process
6. Simulation (Monte Carlo example)
7. Loss Adjustment Using Control Scorecard

DAIR Identifies an Exposure indexation of crucial assets



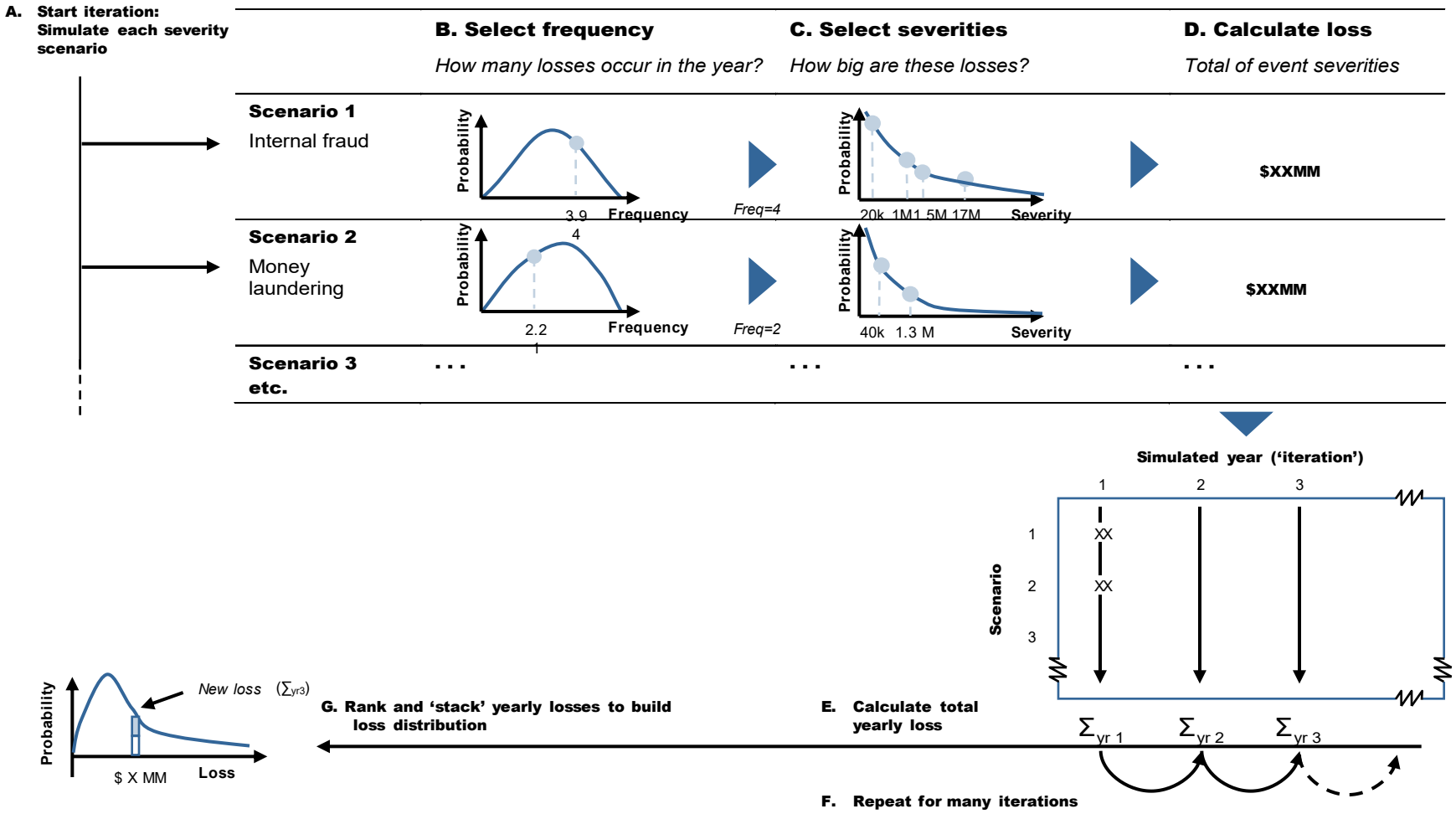
Size of bubble reflects relative Exposure risk of assets

Quantification: Curve fitting and convolution Process



	External Fraud	Internal Fraud	Damage to Physical Assets	Execution Delivery and Process Management	Business Disruption and System Failures	Execution Delivery and Process Management	Clients, Products, and Business Processes	VaR ($)
Scenario 1: Phishing	X			X	X	X		
Scenario 2: Ransomware					X		X	
Scenario 3: Data breach/Hack	X	X			X	X	X	
.			X		X	X	X	
Scenario (n): Malware			X	X	X	X	X	

Loss distribution is generated stochastically on the basis of a frequency and a severity distribution for each scenario



Loss Adjustment Using Control Scorecard

- After cyber loss estimates are determined for each cohort across business units, KRIs can be drawn together for each asset cohort.
- The KRIs are then evaluated for controls against potential losses.
- Capital is then allocated based on the effectiveness of.

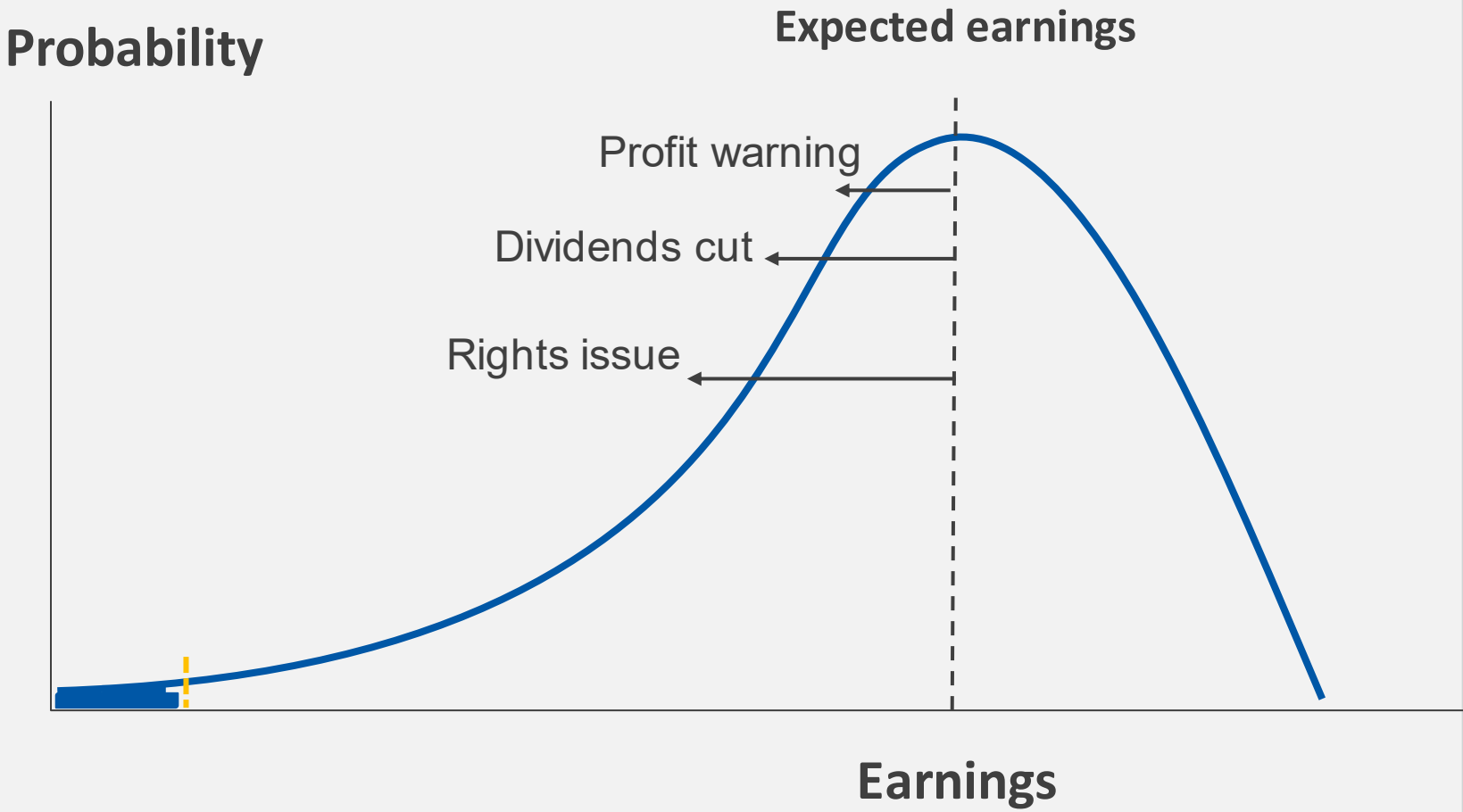
- Operational cyber risk

- **Business cyber risk**

Systemic cyber risk

Business Cyber Risk Quantification

- Business cyber risk captures the knock-on effects of cyber events, such as reputational risk. Some secondary impacts include:
  - negative media coverage
  - loss of creditability
  - reputational loss
  - loss of customer base
  - credit rating downgrade
  - significant drop in share price
  - large fines



Modeling Business Risk

Business risk capital (BRC) is the amount of capital required to be held against unexpected cyber losses.

The calculation of BRC is based upon the following assumptions:

- Known fixed cost bases (non-volume dependent)
- Volume-dependent costs (VDC)
- Operating revenue (OR) is revenue derived from margins, spreads or commissions.
- Variable Margin (VM) is log-normally distributed and defined as:

$$VM = OR - VDC$$

Modeling Business Risk

In a mature business, variable margin is log-normally distributed with mean μ_{VM} and standard deviation σ_{VM}. Worst case variable margin at the appropriate confidence interval is calculated from the normal distribution of LnVM with mean μ_{LnVM} and standard deviation σ_{LnVM}.

Business risk capital is thus defined in terms of a multiple, *m*, of the volatility of variable margin. The value of the multiple is determined from the desired solvency standard.

$$WorstcaseVM_{Desired\ Solvency\ Standard} = e^{(\mu_{LNVM} - m.\sigma_{LNVM})}$$

The difference between mean VM and worst case VM is the amount of business risk capital:

$$Businessrisk\ capital = \mu_{VM} - WorstCaseVM_{Desired\ Solvency\ Standard}$$

- Operational cyber risk
- Business cyber risk
- **Systemic cyber risk**

Systemic Cyber Risk

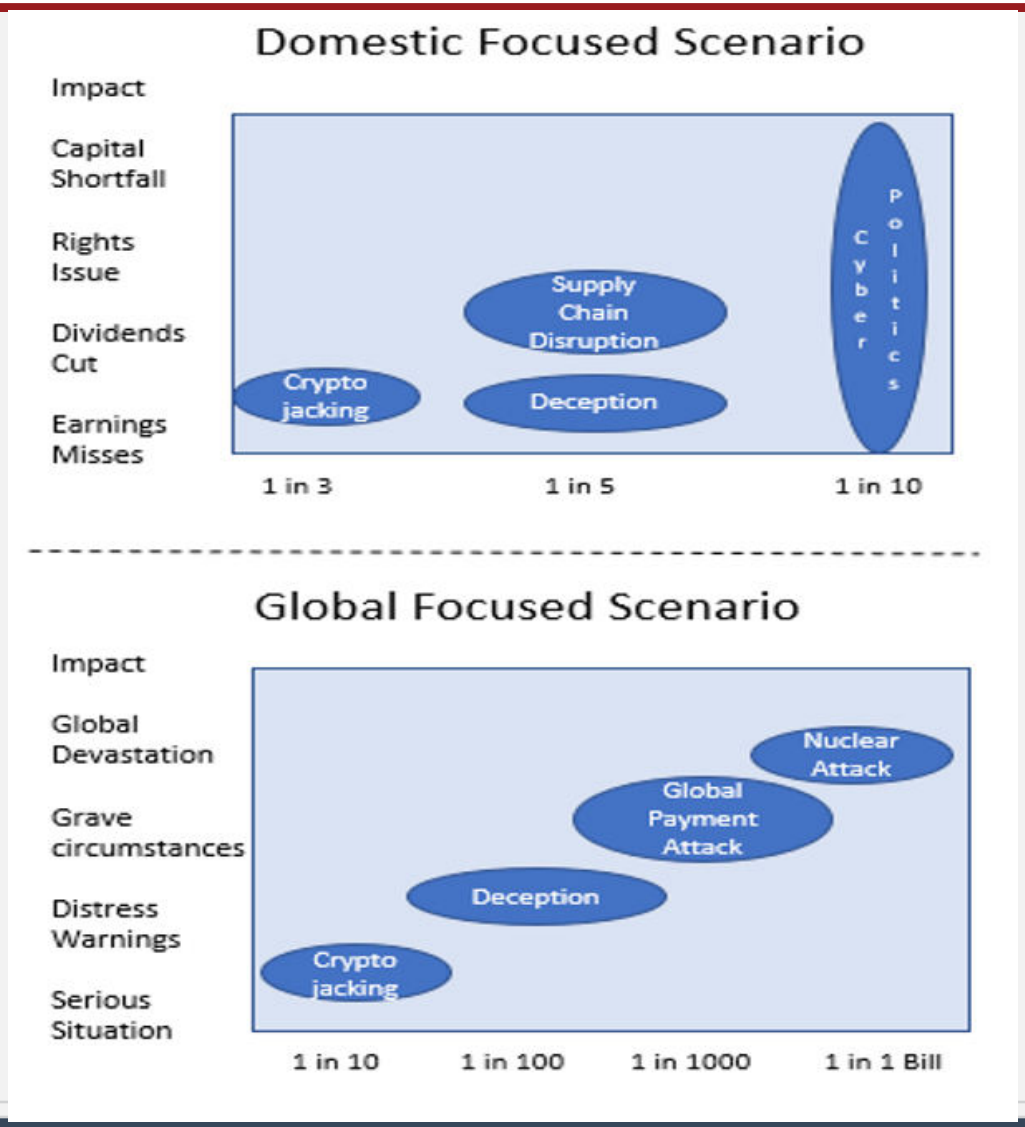
WannaCry Chronology

Systemic Cyber Risk – Scenario Design

Figure 9: Scenario design with GRAFT

Global Risk/Trends
- Illicit Trade
- Interstate Conflict
- Data Fraud & Theft
- Cyber Attacks
- Cyber Dependency
- Failure of Critical Infrastructure
- National Sentiments
- Populism

GRAFT Cyber Risk Scenerios
- Crypto Jacking
- Supply chain disruption
- Cyber politics
- Deception & misinformation in cyber space
- Contagious malware: e.g. WannaCry ransomware
- SWIFT Attack
- Rolling Brown/Black outs



Calculating Systemic Cyber Risk

Business risk and Earning-at-Risk (EAR) underpin business risk as maximum frequency of earnings shortfalls of a given severity.

- Define top-down GRAFT scenarios
- Develop explanatory variable from the scenarios to forecast earning volatility.
- The earning volatility rate is a function of the values of the systemic risk factors triggered by GRAFT scenarios.
- Example (stock market crash, inflation, etc.) $(\overrightarrow{x_1},\ \overrightarrow{x_2}$ and $\overrightarrow{x_3})$
- Earnings at Risk $\widehat{EaR} \sim f(\overrightarrow{x_1}, \overrightarrow{x_2}, \overrightarrow{x_3})$.

Calculating Systemic Cyber Risk

$$\widehat{EaR}_{\propto} = NI_{t-1}(1 - \exp(\mu_{L/P} - \sigma_{L/P} z_{\propto}))$$

NI_{t-1} Last period's net income

$\mu_{L/P}$ is the mean of earnings

$\sigma_{L/P}$ is the standard deviation of earnings

$z_{\propto}$ is the confidence level

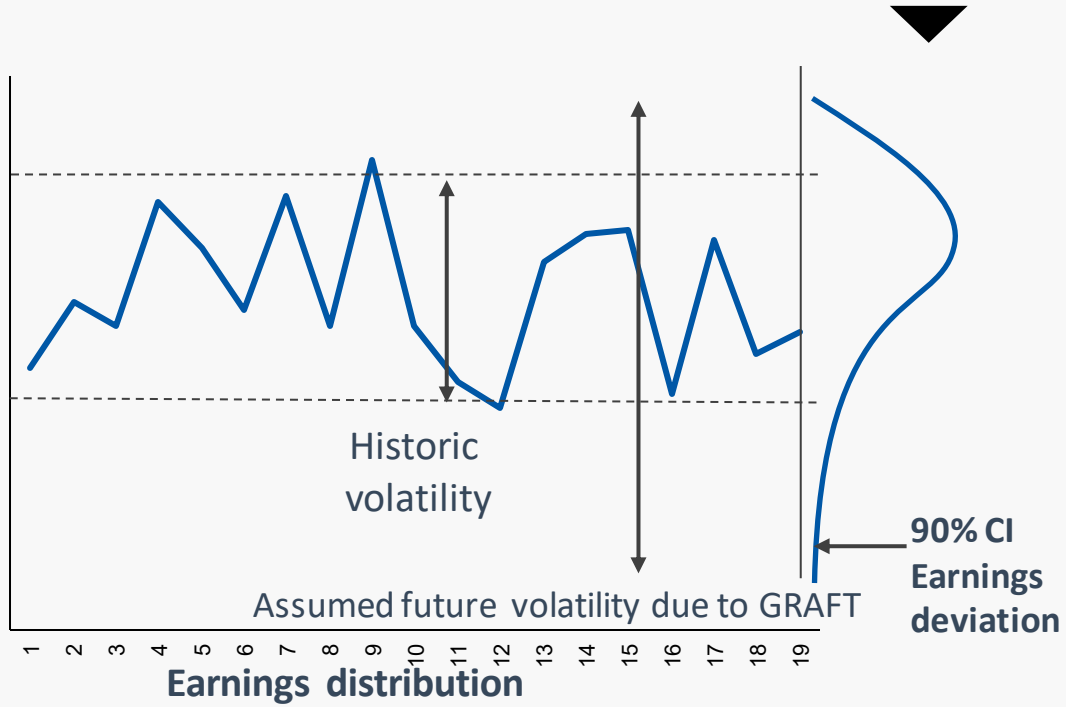
Once the systemic risk parameters are finalized, experts can then forecast medium term values for both the base and stressed GRAFT cases.

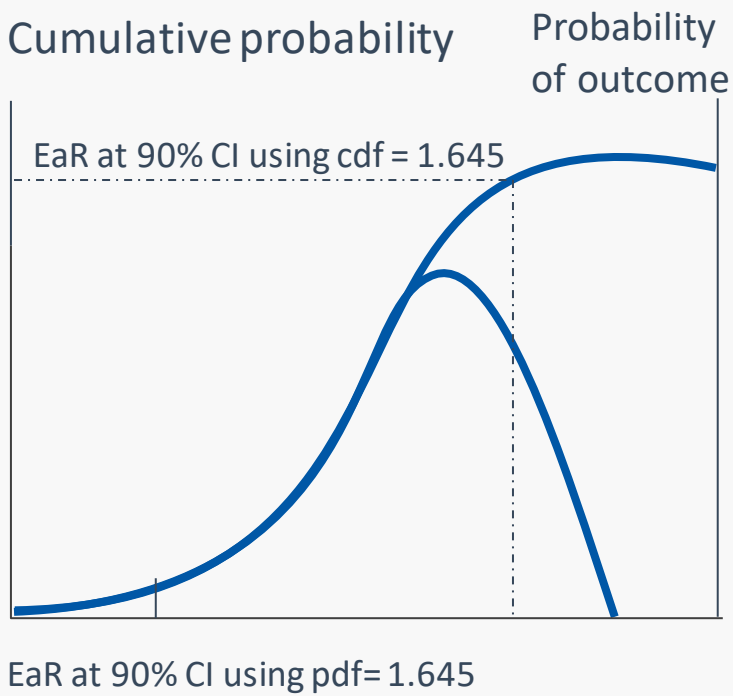
Systemic Cyber Risk – Normally Distributed Earnings Data

GRAFT Scenarios

Sources of systemic risks and correlated risks, e.g., reputational risk

- Breakdown of Int'l Governance
- Supply chain disruption
- Deception and misinformation in cyber space
- Cyber politics
- …





EaR at 90% CI using pdf= 1.645

Insurability of Cyber Risk

- Case by case basis
- Limited effect on capital reducing
- Often effected by per-claim limits
- Scope limitations

Next Steps

- Data collection
- Consolidation of cyber risk into a single organization wide taxonomy
- Use cyber scenarios and quantification to improve controls frameworks and prevent attacks
- Include cyber quantification in risk appetite and development of key risk indicators to develop a robust control framework
- Deep dives
- Enhanced communication with stakeholders