STRUCTURED SCENARIOS

A pilot experiment on peer structured scenario assessment

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

Version 31/05/2018

OUTLINE

- Executive Summary
- Scenarios in Operational Risk Assessment
- The XOI (Exposure, Occurrence, Impact) Method
- The Pilot Experiment

EXECUTIVE SUMMARY

- This presentation addresses:
  - The assessment of potential large oprisk events (scenarios)
  - The usage of a structured method (XOI) to define a loss generation mechanism and drivers for each scenario
  - The use of peer benchmarking to improve consistency of loss generation mechanism and individual drivers assessment

- This work has been performed during a 6-month period (2017-2018) with a group of banks and 6 scenarios.
- It was facilitated by ABA.

SCENARIOS IN OPRISK ASSESSMENT

SCENARIOS IN OPRISK MANAGEMENT

- Large events are rare but contribute to the most significant part of oprisk losses: for instance, ORX reports that less than 0.5% of events represent more than 75% of total losses in the last 6 years (1)

- For a given institution, in most cases, not all types of large events have been observed.

- It is therefore useful to consider them as "scenarios" in order to assess their specific consequences within the firm.

- The expected benefits of analysing scenarios are the following:
  - **Management**: a detailed analysis could result in identifying weaknesses, and design new controls
  - **Measurement**: this can help projecting future losses for economic capital, capital adequacy, or CCAR.

(1) Beyond the headlines: Banking – Operational risk loss data for banks submitted in 2016 (ORX, Nov 2017).

SCENARIOS IN OPRISK LOSSES PROJECTION

- Regulatory exercises (CCAR, ICAAP) require the projection of oprisk losses under adverse conditions. These projections need to take into account:
  - Past losses of the bank
  - Pending matters (in particular legal)
  - Potential future events
  - How adverse conditions would impact the above

- Quantitative models can help assessing future losses:
  - Regression models can capture dependencies of losses to economic factors
  - Statistical models of settlements vs provisions can help quantifying legal stressed losses
  - Loss distribution approaches can be used to assess stressed losses as a percentile of the loss distribution.

- The use of scenarios is necessary to complement these projections for potential future events. This involves:
  - Identifying major events potentially relevant to the institution
  - Assessing the likelihood and severity of these events through scenario analysis
  - Carefully selecting the scenarios to include in the projection

CHALLENGES OF SCENARIO ASSESSMENT

- We can identify at least 5 areas of difficulty for scenario assessment:
  - **Identification**
    - Comprehensiveness
    - Granularity (Regulatory fines or Mis-selling? Cyber-attack or DDOS? Internal fraud or Rogue Trading?)
  - **Use of external data**
    - How to generalize or adapt the storyline?
    - How to scale the amount?
  - **Involvement of business experts**
    - How to identify the right experts?
    - Which questions to ask?
  - **Nature of the measurement**
    - Do we want to assess the average cyber-attack, the extreme but plausible cyber attack, the range of potential cyber-attacks?
  - **Validation of the measurement**
    - How to challenge the measurement?
    - Can a measurement of a hypothetical event be validated?

Typical Practice of Scenario Assessment

- Scenarios are usually assessed in workshop(s) with business experts, facilitated by the second line.

- Inputs:
  - A scenario name and storyline
  - External losses
  - Some business metrics

- Process:
  - Often: rescoping of scenario, focus on scaling, decomposition of the potential loss (direct cost, fine, etc), qualitative discussion on controls
  - Less often: Discussion of a simple formula for evaluating the potential loss (size of compromise * cost per record), a range of more or less severe situations.

- Outputs:
  - A frequency and a severity (single situation)
  - Several situations for predefined frequencies (1/10, 1/100, etc.)

- Pros
  - Qualitative discussion with few priors

- Cons
  - Common biases (recency, salience, overconfidence, etc.)
  - Loose relation between assumptions and assessment

THE XOI METHOD FOR SCENARIO ASSESSMENT

- The XOI method ([1], [2], [3]) allows a structured assessment of scenario through:
  - The use of 3 common dimensions for each scenario: Exposure, Occurrence, Impact
  - The use of specific drivers for each dimension (number of units exposed, time to detection, time to recovery, market conditions, etc.)

- The experts are prompted to provide or confirm an assessment (value, range, set of ranges) on each driver. The assessments can be informed by external statistical analysis.

- The XOI method does not add any assumption to expert opinions and generates the implicit distribution of potential losses through probabilistic calculation using:
  - Bayesian inference
  - Monte Carlo simulation

- **The use of distributions in scenario assessmen**t is generally focused on combining observed losses with single point projections to assess the tail of a distribution [4], (5]
- The XOI approach focuses rather on generating a distribution of potential tail events.

[1] Analyse des Risques opérationnels par les réseaux bayésiens, Condamin, L, Naim, P., Revue d'Economie Financière, 2006
[2] Risk Quantification: Management, Diagnosis and Hedging, Condamin, L., Louisot, J.P., Naim, P., Wiley, 2006
(3] Operational Risk Modelling in Financial Services: the Exposure, Occurrence, Impact method, Condamin, L; Naim, P., Wiley, forthcoming Dec 2018
[4] Ergashev, B.A, A theoretical framework for incorporating scenarios into operational risk modelling. Journal of Financial Services Research, Vol 41-3, pp 145-161.
[5] Abdymomunov, A. Blei, S., and Ergashev, B.A, Integrating Stress Scenarios into Risk Quantification Models. Journal of Financial Services Research,. Vol 47-1, pp 57-79.

THE XOI METHOD

OVERVIEW OF THE XOI METHODOLOGY

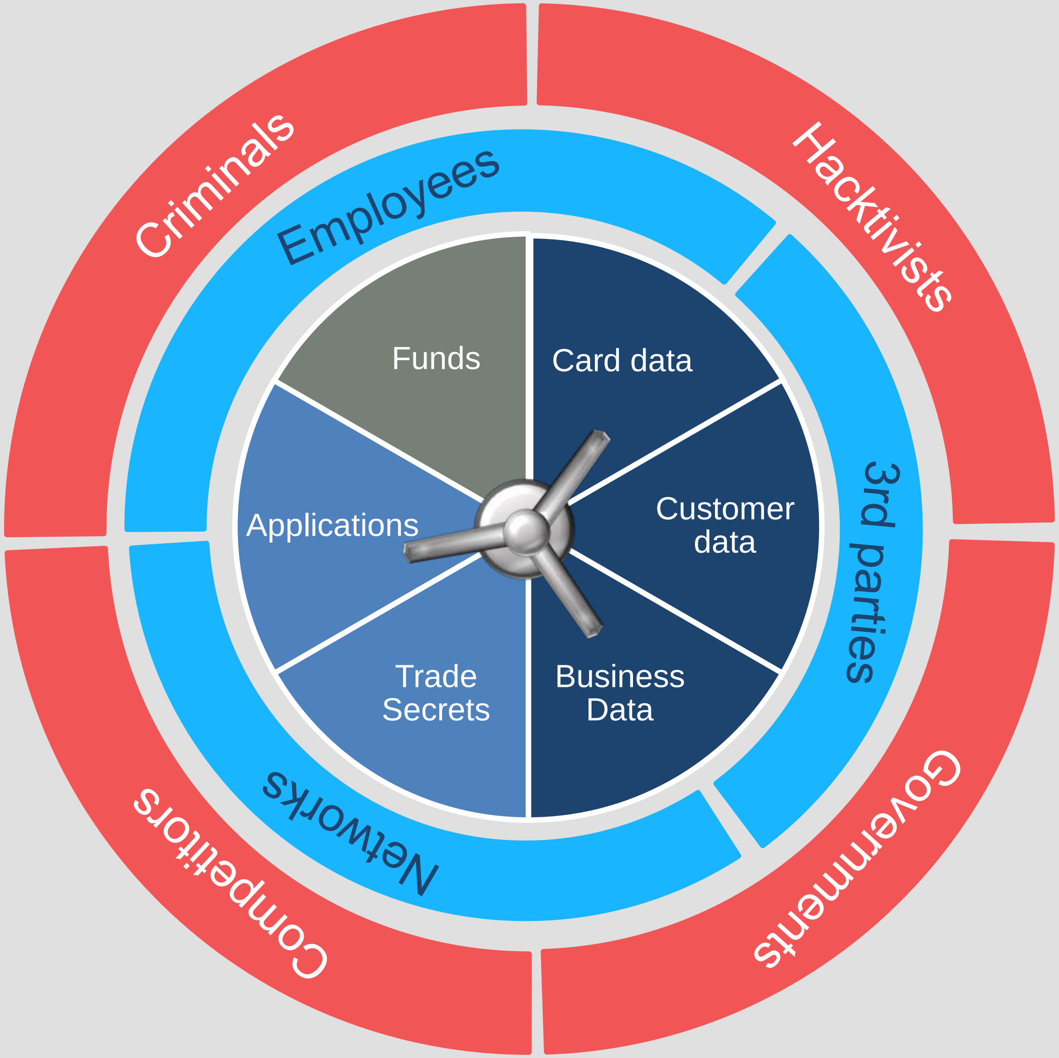
- **A risk is defined by eXposure, Occurrence and Impact.**
- A unit of **Exposure** is a resource used by the firm's business
  - Human (Employees, Traders, IT people, etc)
  - Technical (Systems, Buildings, Products, Models, etc.)
  - Informational (Customer data, IP, etc.)
  - Partner (Suppliers, Brokers, etc.)
  - Financial (Financial Assets)
  - Infrastructure (Regulations, IT infrastructures, etc.)
- The **Occurrence** of an event creates a loss when striking a resource
  - Fraud, Illness for Human resources
  - Error, Disruption, for Technical resources
  - Attack for Informational resources
  - Fraud, Destruction for Informational Resources
- The **Impact** is the amount of the loss
  - This amount of loss is broken down into several components as necessary: direct loss, repair costs, indirect costs, loss of income, fines, etc.
  - It may depend on the object exposed
  - It may depend on circumstances

SOME EXAMPLES OF X,O,I RISKS

INTERNAL FRAUD	EXTERNAL FRAUD	EMPLOYMENT PRACTICES	BUSINESS PRACTICES	DAMAGE TO PHYS. ASSETS	BUSINESS DISRUPTION	EXECUTION
ROGUE TRADING	**MERCHANT COMPROMISE**	**EMPLOYEE CLASS ACTION**	**MIS-SELLING**	**NATURAL DISASTER**	**SUPPLIER FAILURE**	**TRADING ERROR**

TRADERS	MERCHANTS	REGULATIONS	PRODUCTS	BUILDINGS	KEY SUPPLIERS	TRADES
GOING ROGUE	DATA BREACH	CLASS ACTION	CLASS ACTION	NATURAL DISASTER	BANKRUPTCY DISRUPTION	ERROR
POSITION X MARKET CHANGE	FRAUD + CARD REISSUE	SETTLEMENT X N_EMPLOYEES	DETRIMENT X N_CLIENTS	BUILDING + BUSINESS	REPLACEMENT + BUSINESS	AMOUNT x MARKET CHANGE

AN EXAMPLE: CYBER-RISK



ATTACKERS

ACCESS

ASSETS

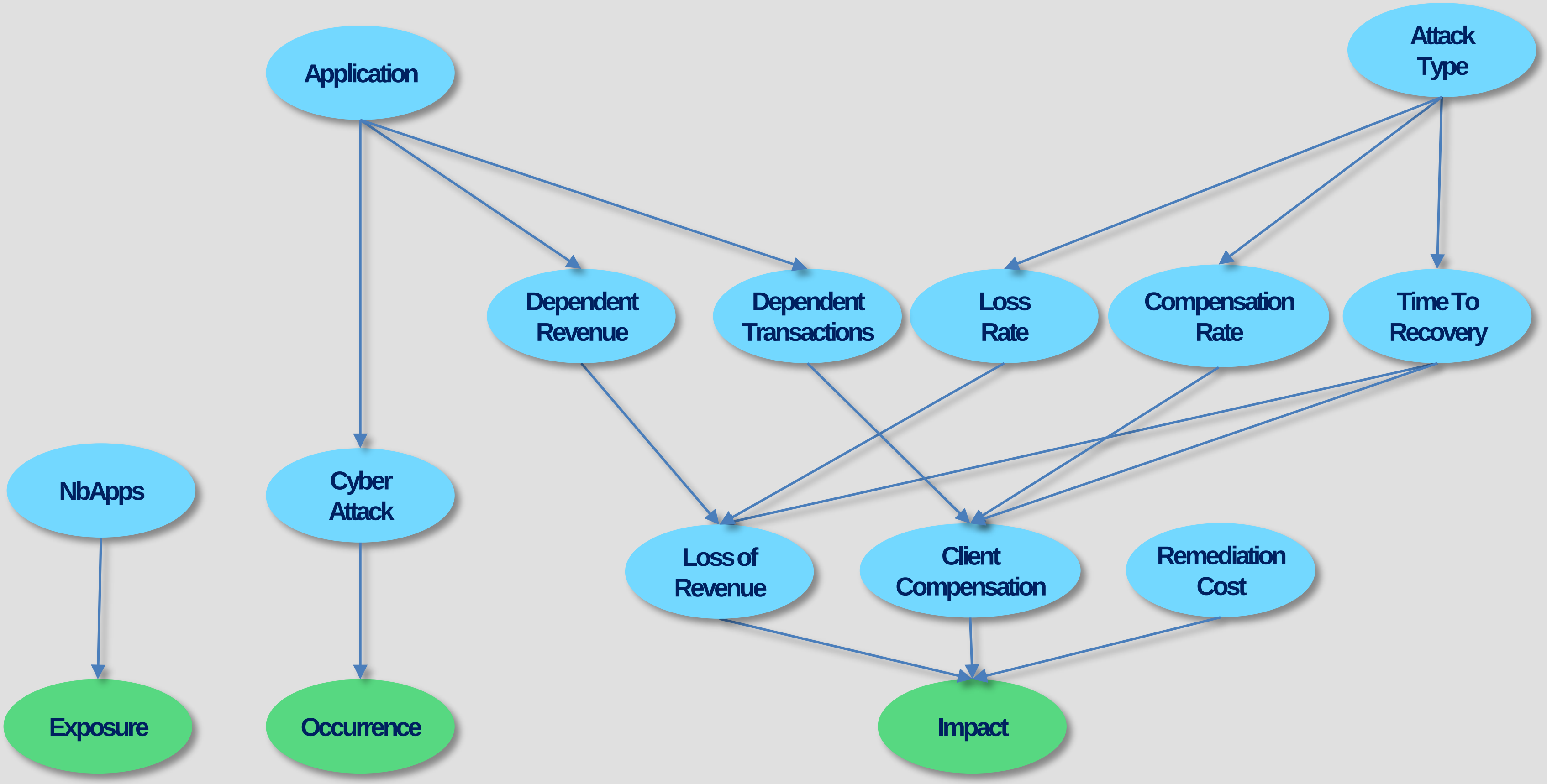
CYBER RISK – LIST OF POTENTIAL SCENARIOS

SCENARIO	DESCRIPTION	EXPOSURE	OCCURRENCE	IMPACT
Merchant /Processor Card Compromise	Theft of customer card data within a large merchant, followed by the subsequent sale of this data to criminal networks.	Merchants or processors handling large volumes of bank card data	Internal fraud or cyber attack within merchant or processor	Cost of fraud and cost of cards reissue
Internal Credit Card Compromise	Internal compromise of large volume of credit card data (either from issuer or acquirer systems), followed by the subsequent sale of this data to criminal networks.	Employees having access to large volumes of bank's card data (issuer or acquirer side)	Internal fraud	Cost of fraud and cost of cards reissue
External Credit Card Compromise	External attack of large volume of credit card data (either from issuer or acquirer systems), followed by the subsequent sale of this data to criminal networks.	Systems storing credt cards data	External fraud	Cost of fraud and cost of cards reissue
Internal Customer Data Compromise	Losses due to compromise of customer data (with the exception of credit card data considered in other scenarios).	Employees having access to large volumes of bank's customer data (excluding cards)	Internal fraud	Potential direct losses, client protection, legal, and regulatory costs.
Cyber attack - Customer Data Compromise	Losses due to compromise of customer data (with the exception of credit card data considered in another scenario).	Systems storing large volumes of customer data (excluding cards)	External fraud	Potential direct losses, client protection, legal, and regulatory costs.
Cyber attack - Critical Application Disruption	External attack that makes a critical application or a group of those unavailable and limit or stop operations..	Critical business applications.	External fraud	Loss of business and customer detriment
Cyber attack - Fund Misappropriation	External attack directly targeting funds misappropriation.	Systems, employees (social engineering)	External fraud	Funds misappropration
Cyber attack - Data alteration	External attack targeting integrity of firm data (sabotage) . This affects outcomes of business operations.	Systems, employees (social engineering)	External fraud	Potential direct losses and correction costs.

CYBER ATTACK CRITICAL APPLICATION – STRUCTURE

A structured story describes how a potential loss could be generated

This scenario occurs in case of an **external attack** that makes a **critical application** or a group of those **unavailable** and **limit or stop operations.**
This scenario focuses on significant attacks, either in duration or in magnitude



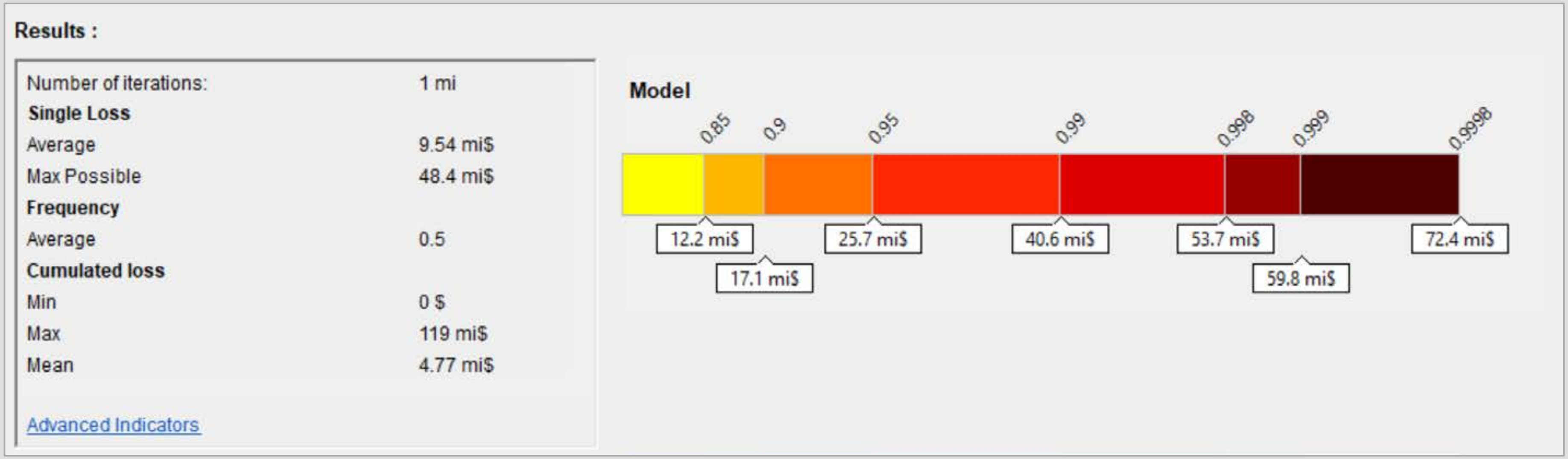
CYBER ATTACK CRITICAL APPLICATION - QUANTIFICATION

DRIVER	TYPE	ASSESSMENT	SOURCE
Number of critical applications	Objective	5 applications: 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

Structure and Driver Distributions are compiled into a Bayesian Network that is sampled through Monte Carlo simulation to estimate the distribution of the potential losses over the next year

```
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
```



Results :

Number of iterations:	1 mi
Single Loss	
Average	9.54 mi$
Max Possible	48.4 mi$
Frequency	
Average	0.5
Cumulated loss	
Min	0 $
Max	119 mi$
Mean	4.77 mi$

Advanced Indicators

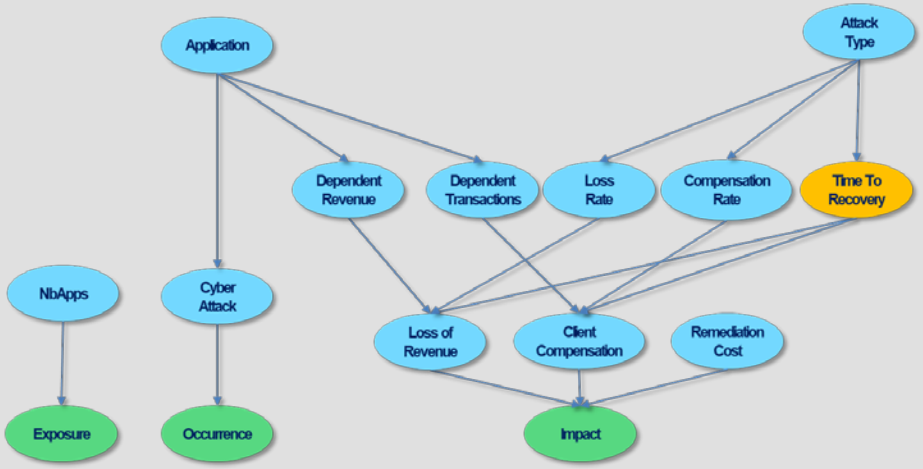
CYBER ATTACK – CRITICAL APPLICATION – WHAT IF

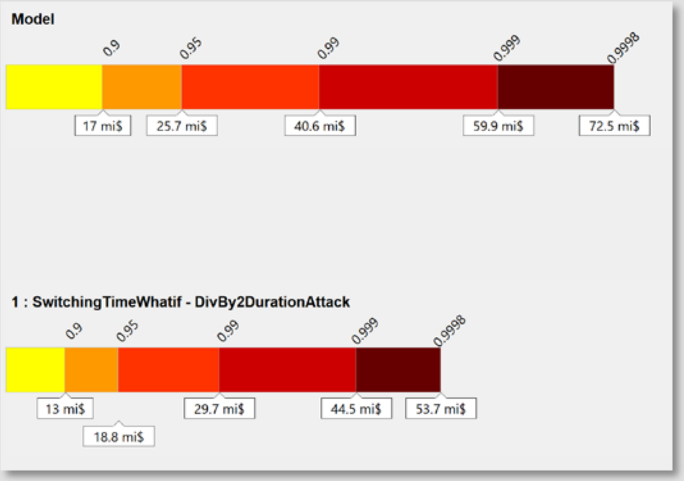
What if analyses are performed for:

- Risk Management: assess the impact of a mitigation action
- Stress Testing: assess the impact of a stress on a driver
- Model Quality Assessment: assess the impact of uncertainty on results

Test a mitigation action that would divide the time to recovery for a duration attack by 2. The Time To Recovery distribution is changed.

Loss distribution is re-sampled using the new assumption, to estimate the benefits of the mitigation action.





Q &A

What is a Scenario according to this method?

This is not an instance of a possible occurrence of the risk, but rather a generator of possible situations. When starting from single points scenarios, they are still very useful to identify drivers and also discuss the possible ranges of the assumptions.

Is this a model?

This is a model because this is a representation of the reality - how things could happen and unfold. However the model does not try to approach a "true distribution", but rather to produce the distribution implied by expert assessments.

How to validate this model?

The validation of this model is not easy as backtesting would in theory require being able to reconstitute past expert opinions.

However:

- The generated distribution can be checked for consistency with observed cases.
- Each piece of information can be challenged by independent experts

To this extent, **the use of peer benchmarking** is a good candidate to challenge and justify assessments.

THE PEER BENCHMARKING EXPERIMENT

THE ABA PILOT

- An experiment has been launched with the ABA and a group of banks
- 6 scenarios have been analysed:
  - Cyber Attack on Critical Application
  - Mis-Selling Retail
  - Rogue Trading
  - Customer Data Compromise
  - Breach of Antitrust Regulation
  - Employee Litigation
- Collaborative work to agree on the loss generating mechanism
  - Structure of the X,O,I scenario
  - List of drivers
- Bank specific quantification for each of the drivers

PROCESS OVERVIEW

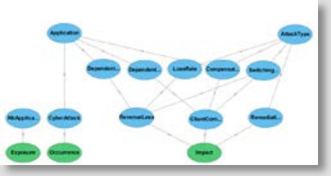
Identification Project members select the list of material scenarios they want to address.

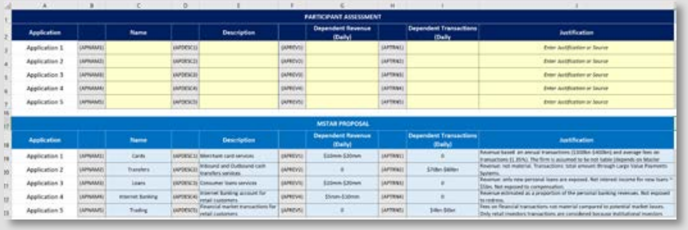
Structure Initial design stylized from industry cases, workshop with member to review and agree.

Quantification A standardized Data Request form is sent to the members to collect the data for each driver.

Simulation The scenario is sampled for each member with its own drivers. The results (VaR etc.) are reviewed with each member.

Benchmarking Results and drivers are scaled and compared between the members. Gaps are analyzed and can lead to scenario revision.



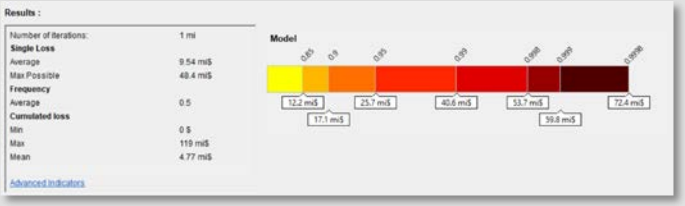


PARTICIPANT ASSESSMENT

Application		Name		Description		Dependent Revenue (Daily)		Dependent Transactions (Daily	Justification
Application 1	(APNAM1)		(APDESC1)		(APREV1)		(APTRN1)		Enter Justification or Source
Application 2	(APNAM2)		(APDESC2)		(APREV2)		(APTRN2)		Enter Justification or Source
Application 3	(APNAM3)		(APDESC3)		(APREV3)		(APTRN3)		Enter Justification or Source
Application 4	(APNAM4)		(APDESC4)		(APREV4)		(APTRN4)		Enter Justification or Source
Application 5	(APNAM5)		(APDESC5)		(APREV5)		(APTRN5)		Enter Justification or Source

MSTAR PROPOSAL

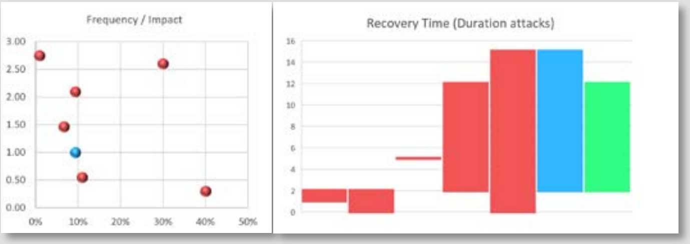
Application		Name		Description		Dependent Revenue (Daily)		Dependent Transactions (Daily)	Justification
Application 1	(APNAM1)	Cards	(APDESC1)	Merchant card services	(APREV1)	$10mm-$20mm	(APTRN1)	0	Revenue based on annual transactions ($100bn-$400bn) and average fees on transactions (1.35%). The firm is assumed to be not liable (depends on Master
Application 2	(APNAM2)	Transfers	(APDESC2)	Inbound and Outbound cash transfers services	(APREV2)	0	(APTRN2)	$70bn-$80bn	Revenue: not material. Transactions: total amount through Large Value Payments Systems.
Application 3	(APNAM3)	Loans	(APDESC3)	Consumer loans services	(APREV3)	$10mm-$20mm	(APTRN3)	0	Revenue: only new personal loans are exposed. Net interest income for new loans ~ $10m. Not exposed to compensation.
Application 4	(APNAM4)	Internet Banking	(APDESC4)	Internet Banking account for retail customers	(APREV4)	$5mm-$10mm	(APTRN4)	0	Revenue estimated as a proportion of the personal banking revenues. Not exposed to redress.
Application 5	(APNAM5)	Trading	(APDESC5)	Financial market transactions for retail customers	(APREV5)	0	(APTRN5)	$4bn-$6bn	Fees on financial transactions not material compared to potential market losses. Only retail investors transactions are considered because institutional investors



Results :

Number of iterations:	1 mi
Single Loss	
Average	9.54 mi$
Max Possible	48.4 mi$
Frequency	
Average	0.5
Cumulated loss	
Min	0 $
Max	119 mi$
Mean	4.77 mi$

Advanced Indicators



LESSONS LEARNED

- Data collection:
  - The collection of expert opinions is easier thanks to the precise definition of each driver.
- Dispersion of assessments
  - There exists a significant dispersion between assessments of potential extreme impact of scenarios: for some scenarios, the severity at the 1 in 1000 level ranges from 1 to 10 (scaled in days of revenue).
  - Part of this dispersion is explained by differences in business structures
  - The other part relies more on expert perception of controls
  - The decomposition helps focusing on the most subjective part of the assessment.
- Benefits perceived by participants
  - The benchmarking is the main perceived benefit
  - The loss generation mechanism allows to identify key drivers and define controls
  - The analysis and results can be used as an useful input for economic capital, capital adequacy, CCAR.
- Improvements foreseen by participants after the pilot
  - Augment the library of scenarios
  - Offer the ability to add specific drivers on top of a common structure
  - Offer the ability to design specific scenarios and share them with peers