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
ST Return Distribution

Median: -0.5%  Mean: -0.7%
FUD vs CURe

Uncertainty Management

Risk Management

Compliance
Thank You!

Gilles.Hilary@georgetown.edu
Panel #2: Measurement and Impact of Cyber Risk

- Gilles Hilary, *Chair 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
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
Example – CYBER Attack on critical service
Example – CYBER FUND MISAPPROPRIATION
Example – customer data compromise

ATTACKERS
ACCESS
ASSETS
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

<table>
<thead>
<tr>
<th>DRIVER</th>
<th>TYPE</th>
<th>ASSESSMENT</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of critical services</td>
<td>Objective</td>
<td>5 services: Cards, Transfers, Trade, Loans, Internet Banking</td>
<td>Business Data, Resiliency Team</td>
</tr>
</tbody>
</table>
| 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 |
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

### Statistics

<table>
<thead>
<tr>
<th>Number of iterations</th>
<th>1 mi</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single Loss</strong></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td>9.5 mi$</td>
</tr>
<tr>
<td>Max Possible</td>
<td>48.5 mi$</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td>0.5</td>
</tr>
<tr>
<td><strong>Cumulated Loss</strong></td>
<td></td>
</tr>
<tr>
<td>Min</td>
<td>0$</td>
</tr>
<tr>
<td>Max</td>
<td>119 mi$</td>
</tr>
<tr>
<td>Mean</td>
<td>5.0 mi$</td>
</tr>
</tbody>
</table>
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 assessment
- 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, Chair 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 -
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
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

NIST CSF and CPMI-IOSCO

- Supply Chain/Dependency Management
- Recover
- Detect
- Protect
- Identify

Added in Response to Regulation

Functions
- Governance

Categories
- SAME Column as in NIST CSF
- SAME Column as in NIST CSF

Subcategories
- Except that some categories have been moved and some have added to fit with new “5 + 2” Function concept.
- Except that some categories have been moved and some have added to fit with new “5 + 2” Function concept.

NEW Column
The risk-based diagnostic statements knit together the multitude of regulatory expectations and the NIST-centric Subcategories; Will aid regulatory agencies with their oversight and examination responsibilities.

Added in Response to Regulation

FFIEC CAT Inspired Addition

Diagnostic Statements

FS Specific Regulatory References
- CPMI-IOSCO, NIST CSF, ISO Standards
- FFIEC CAT and IT Handbooks
- SEC, CFTC, FINRA, NAIC
- NYDFS
- SAMA Information Security Survey
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.

Sector Only Impact – Tier 3
- Firms with a high degree of interconnectedness, and between 1-5 million customer accounts.
- Regional banks, large credit unions.

Customer/3rd Party Impact Only – Tier 4
- Applies to the firms with a relatively small number of customers.
- Community banks, small broker dealers/investment advisors.
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 Profile extends the NIST Cybersecurity Framework to be **more inclusive** of financial services requirements and supervisory expectations

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

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
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:**

[Logos of supporting associations]
Panel #2: Measurement and Impact of Cyber Risk

- **Gilles Hilary**, Chair 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
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:

<table>
<thead>
<tr>
<th>Cyber Risk Methodology</th>
<th>Precision</th>
<th>Agility</th>
<th>Quantification</th>
<th>Ease of Use</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factor Analysis Information Risk (FAIR)</td>
<td>70</td>
<td>100</td>
<td>85</td>
<td>0</td>
<td>90</td>
</tr>
<tr>
<td>CDRA</td>
<td>70</td>
<td>90</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>ISRAM</td>
<td>65</td>
<td>90</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>Facilitated Risk Analysis Process</td>
<td>60</td>
<td>90</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>COBRA</td>
<td>55</td>
<td>85</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>OACTIVE ALLEGRO</td>
<td>55</td>
<td>85</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>NIST 800-30</td>
<td>50</td>
<td>85</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>ISO 30101:2009</td>
<td>45</td>
<td>85</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>COBIT</td>
<td>40</td>
<td>85</td>
<td>85</td>
<td>0</td>
<td>85</td>
</tr>
</tbody>
</table>
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.
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
2019 Cyber Risk Workshop

John DeLong
Operational Risk
Discussion & Questions