Q&A session: Valuing TfNSW Reputation Damage from Cyber Risk

Thursday 18th June 2020 @9:30am

Please note this email or the associated problem statement is not an offer or invitation to enter into a legal relationship, contract, agreement or other arrangement with TfNSW, in respect of the research that is the subject of the problem statement. Nothing in the problem statement or this email obliges TfNSW to enter into any agreement with respondents.

Please note the session is being recorded

Thank you for attending

1. **Housekeeping**
   a. Mute microphones
   b. Raise hands for questions
   c. Type your questions
   d. The Q&A session is being recorded

2. **Q&A session is 30min only and will conclude at 10am**

3. **Agenda:**
   a. Context and purpose of the study
   b. Q&A

Please note the session is being recorded

Problem Statement: Context

1. **Transport for NSW's (TfNSW) Transport Cyber Defence (TCD)** is analysing and quantifying key cyber security risks.

2. **Not all cyber security risks can be measured** in dollar value terms. In particular, the risks associated with reputational damage as a result of a cyber-attack, are challenging to measure.

3. **TfNSW's TCD** is using – Factor Analysis of Information Risk (FAIR) – as a trusted modelling framework to analyse these risks. FAIR identifies six forms of loss two of which are difficult to apply to the public sector. The 'competitive advantage' loss type is applicable to the commercial sector. Reputation Damage loss type is the most challenging to quantify and there are no clear methodology or framework for quantifying them for government entities.

4. **The research objective:** produce a rigorous evidence base around the economic cost of reputational damage from a cyber-attack to TfNSW and the Government more broadly, as well as understanding the economic value of a personal record to TfNSW.

Problem Statement: Purpose

5. **Research hypothesis:**
   "TfNSW's reputation will be significantly impacted by cyber-attack, in an economically quantifiable way."

6. **The study aims to quantify reputational damage** focussing on:
   a) An economic valuation framework for reputational damage to TfNSW arising from a cyber-attack.
   b) An economic value of a record of personal (customer) information.

7. **Research impact:** The study will assist in developing a more robust justification for including cyber-security related economic parameters in the "TfNSW Principles and Guidelines for the TfNSW Cost-Benefit Analysis Guide."

TfNSW Cost benefit analysis guide

TfNSW Cost Benefit Guidelines

Section	Key Audience	Focus
2. Why is a cost-benefit analysis needed?	Senior project representatives	What is needed and why
3. The scope of a cost-benefit analysis	Those new to CBA or refreshing knowledge Project teams and CBA practitioners	Core concepts for cost benefit analysis, common concepts and issues, and an overview of the process for undertaking CBA Recommendations for CBA practitioners to be aware of are in **bold text**
4. Cost-benefit analysis concepts		
5. The key steps in doing a cost-benefit analysis		
6. Common mistakes and issues		
7. When to ask for help		

Feedback or questions regarding the Guide should be directed to the Transport for NSW (TfNSW) Evaluation and Economic Advisory team at: EconomicAdvisory@transport.nsw.gov.au

NSW Treasury Business Case Guidelines

What is a Business Case?

A multipurpose proposal for action that meets Government's objectives and informs an investment and policy decision.

What are the characteristics of a good business case?

A good business case should:

- Be clear and concise
- Be planned early in the investment process
- Reflect stakeholder views and consultation outcomes
- Contain the right evidence, inc. reference of previous experiences and outcomes in implementing similar initiatives
- Treated as a living document, that is continuously updated and repurposed

When should a business case be prepared?

Business cases are prepared for different reasons:

- To inform prioritisation, an investment or regulatory decision and an assurance process
- To demonstrate that adequate due diligence and thinking was undertaken
- To gain funding

How much time does it take to develop?

It depends on the complexity, size, potential risks etc. It can be a short document of few pages, but contain all relevant aspects including key objectives, costs, benefits, risks, stakeholders etc., which can be completed in a few days. Or it can involve a robust analysis, and hence require few months and be a more resource intensive process.

What are the key components of a business case?

A business case contains:

- A case for change i.e. a clear rationale for government action that is based on an identified community need
- Evidence that the options achieve selected objectives and maximise social welfare and value for money (cost benefit analysis)
- Evidence that the options are financially viable (financial analysis)
- Evidence that there is capacity and capability required to procure, implement and maintain the proposal and realise the benefits anticipated (commercial analysis)
- Evidence that the solutions put forward can be delivered (management analysis)

How is a business case developed?

A business case is a continuously evolving document that at its most complex can develop over three main stages:

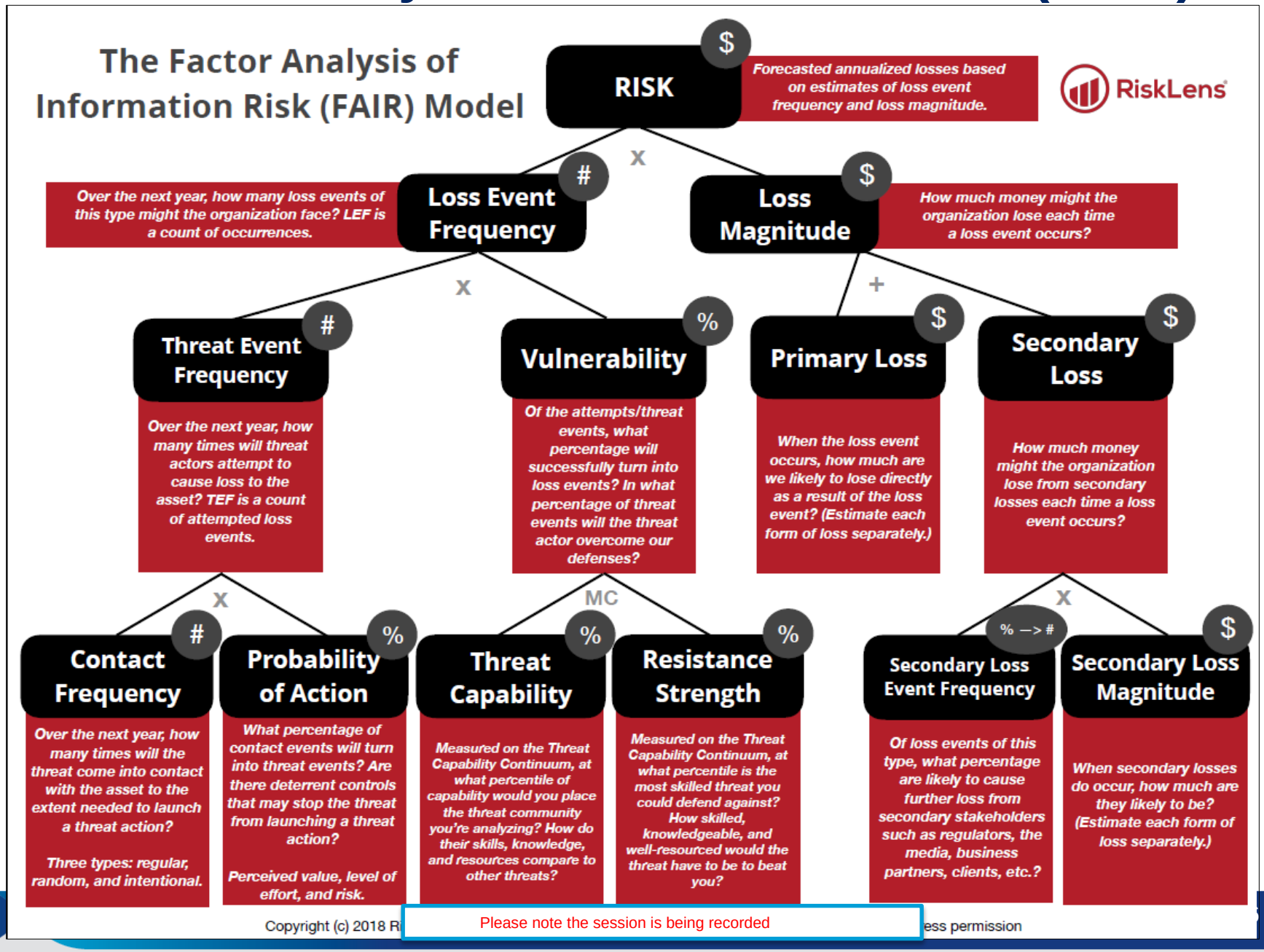
- Stage 0: Problem Definition - Focus on a case for change
- Stage 1: Strategic Business Case – Focus on option identification and analysis
- Stage 2: Detailed Business Case – Focus on option selection and deliverability

Who should be contacted for questions relating to business cases?

Your relevant Agency Budget and Policy Group Treasury contact.

Please note the session is being recorded

Factor Analysis of Information Risk (FAIR)



Please note the session is being recorded

The Risk Analysis Process

FAIR-based risk analyses are conducted in 4 phases:

1. Scoping
Create a scenario to analyze by defining an asset, threat, and effect. (see right) Optionally, you can specify a "method" or "vector" to more narrowly define the scenario being analyzed.

2. Collecting Data and Estimates
Write context-specific questions for each variable, research available internal and external data, identify subject-matter experts and obtain calibrated estimates for the variables of the model you choose to use.

3. Running and Conducting Quality Assurance on Analysis
Run the analysis and think critically about the results generated. Do they seem reasonable given your inputs? (Check for typos!) Have you thoroughly documented adequate rationale for all inputs? Does your analysis answer the questions you set out to answer?

4. Presenting Results
Craft a presentation that informs decision-makers of your results. It's important to clearly communicate the scope of the analysis and be able to interpret resulting data, tables, and graphs with ease.

Elements of Scenario Scoping

Scoping refers to clearly identifying a loss event for which frequency and magnitude can be estimated. The required elements are:

1. Asset
What thing of value are you concerned about being impacted in a way that would result in loss?
Ex. sensitive data, facility, critical application, successful completion of a business process

2. Threat
What person, group of people, or entity are you concerned about acting on an asset in a way that would result in loss?
Ex. cybercriminals, malicious insiders, forces of nature, etc.

3. Effect
How will the threat impact the asset in a way that causes loss?
Ex. Confidentiality, availability, integrity

A properly scoped scenario
Analyze the risk associated with a breach of client PIFI stored in the Sales Database by malicious external hackers.

Calibrated Estimation

Start with an absurd range to combat the tendency to say "I don't know" or provide a point estimate. Remember, we want **accuracy with a useful level of precision.**

Eliminate highly unlikely values and **reference what you know** to narrow the range to something you think is reasonable.

Play a calibration game to identify the range in which you have 90% confidence of accuracy.

Decompose the question if estimating directly proves challenging. Can you break it into questions that are easier to estimate?

Six Forms of Loss

Productivity Loss: Inability to generate value. Wages of idle workers, lost sales in an outage, etc.
Response: Costs of responding to the loss event. Incident response, ext. counsel/forensics fees, etc.
Replacement: Replacing lost/stolen/damaged capital assets. Replacing stolen or infected laptops, repairing facilities damaged by acts of nature, etc.
Competitive Advantage: Loss from compromise of trade secrets, intellectual property, etc. Value of market share a competitor could capture if IP were obtained and exploited.
Fines/Judgments: Legal, regulatory, or contractual penalties levied against the organization.
Reputation Damage: Loss from negative perceptions. Uncaptured revenue, increased cost of capital, etc.

4 Parameters of Estimates

FAIR estimates require a **minimum** and **maximum value** derived from calibrated estimation. Within that range a **most likely value** is selected. A **confidence level** is chosen reflecting how confident we are that the most likely value truly is the most likely.

The RiskLens Academy offers further training on the skills needed to conduct FAIR-based risk analyses in your organization. Check out the FAIR Analyst Learning Path to move beyond fundamental knowledge of the FAIR Model.

Please note the session is being recorded

Next steps

1. **Submit proposal** by 29 June COB to research@transport.nsw.gov.au
2. **Stage 1 –** TfNSW will review responses to Problem Statement – this is currently scheduled w/c 6 July 2020
3. **Stage 2 –** TfNSW will invite presentation of proposals to an Evaluation Committee – this is currently scheduled w/c 20 July 2020 or week after
4. **Stage 3 –** final proposals will be submitted for final assessment
5. *Note that formal appointment is currently scheduled to be given in August 2020*

Thank you

Please note the session is being recorded

Please note the session is being recorded