Dr. Phil Legg

Associate Professor in Cyber Security

Information Risk Management

05: Factor Analysis of Information Risk

Date

UWE Bristol | University of the West of England

The FAIR Risk Ontology

"Essentially, all models are wrong. But some are useful."

- George Box, 1987

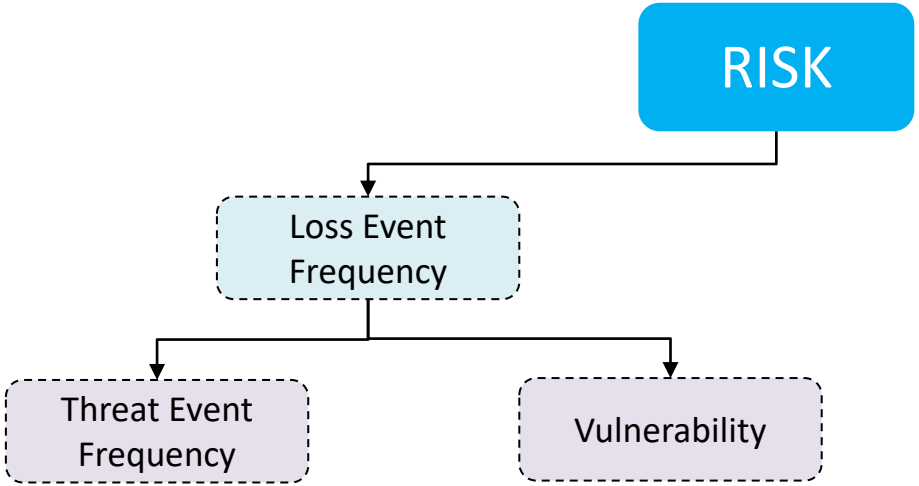
UWE Bristol | University of the West of England

Factor Analysis for Information Risk (FAIR)

Risk

“the probable frequency and probably magnitude of future loss”

Factor Analysis for Information Risk (FAIR)



- A data center outage due to extreme weather
- A corrupt database
- An employee injuring themselves on a wet floor
- A hacker stealing sensitive customer information

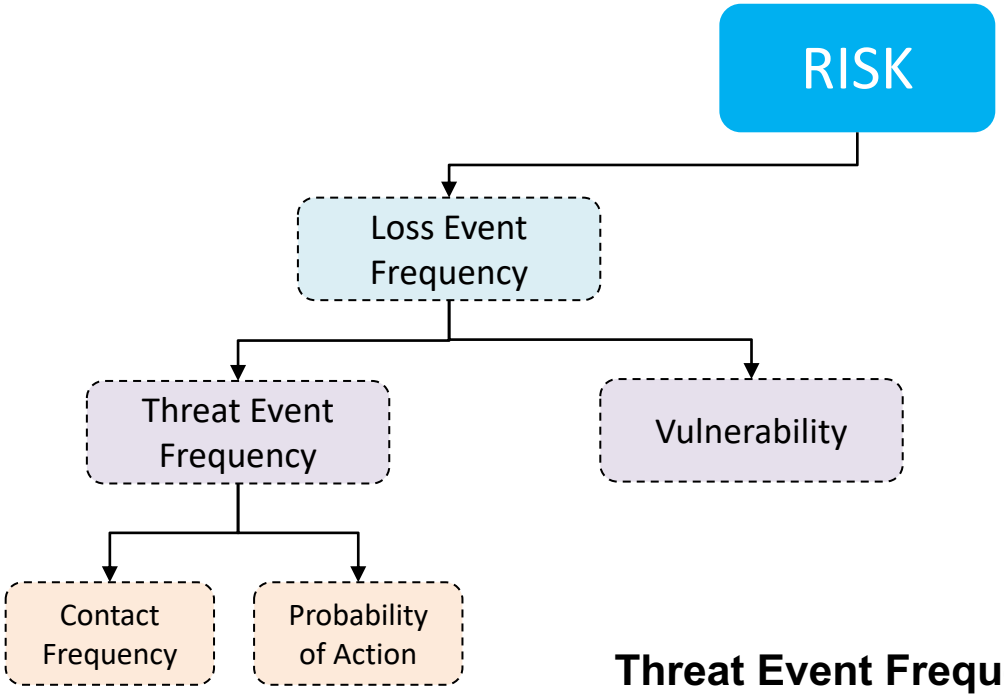
Could be estimated directly, or could be derived from TEF and Vuln.

Expressed as a distribution using annualized values: e.g., between 5 and 25 times a year, with the most likely frequency of 10 times per year.

Loss Event Frequency

"the probable frequency, within a given time-frame, that loss will materialize from a threat agent's action"

Factor Analysis for Information Risk (FAIR)



- A hacker attacking a website is a threat event. If they manage to damage the site or steal information, that would be a loss event.
- Pushing a software release into production is a threat event. Having a problem with the release that results in downtime would be a loss event.
- Someone thrusting a knife at you would be a threat event. Being cut would be the loss event.

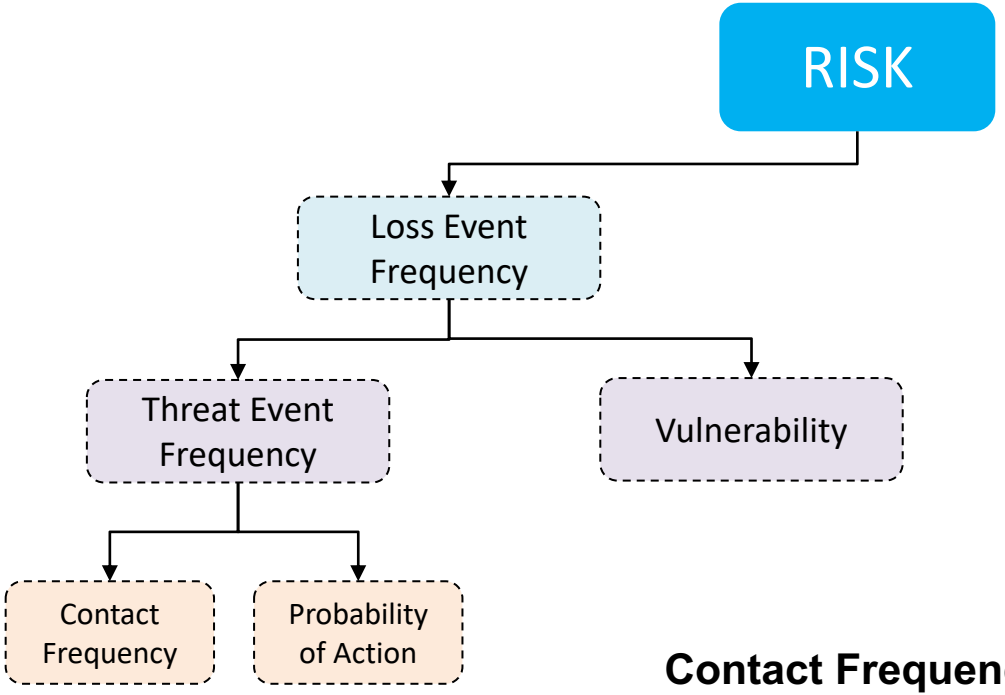
Could be estimated directly, or could be derived from CF and PoA.
Expressed as a distribution using annualized values: e.g., between 0.1 and 0.5 times a year, with the most likely frequency of 0.3 times per year.

Threat Event Frequency

"the probable frequency, within a given time-frame, that threat agents will act in a manner that may result in loss"

UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



- Random (e.g. tornado), regular (e.g., cleaning crew in office at 5:15pm each day), or intentional (e.g., burglar targeting a particular house).

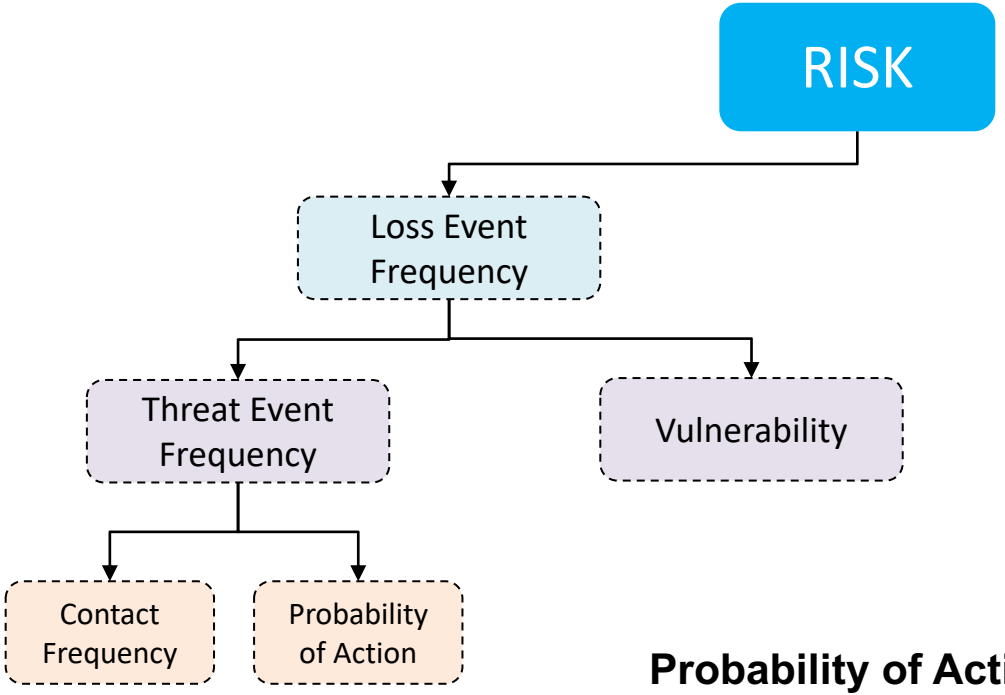
- If we want to reduce risk by reducing CF, what can we do?

Contact Frequency

"the probable frequency, within a given time-frame, that threat agents will come into contact with assets"

UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



- Perceived value of the act from the threat agent's perspective
- Perceived level of effort and/or cost from the threat agent's perspective
- Perceived level of risk to the threat agent

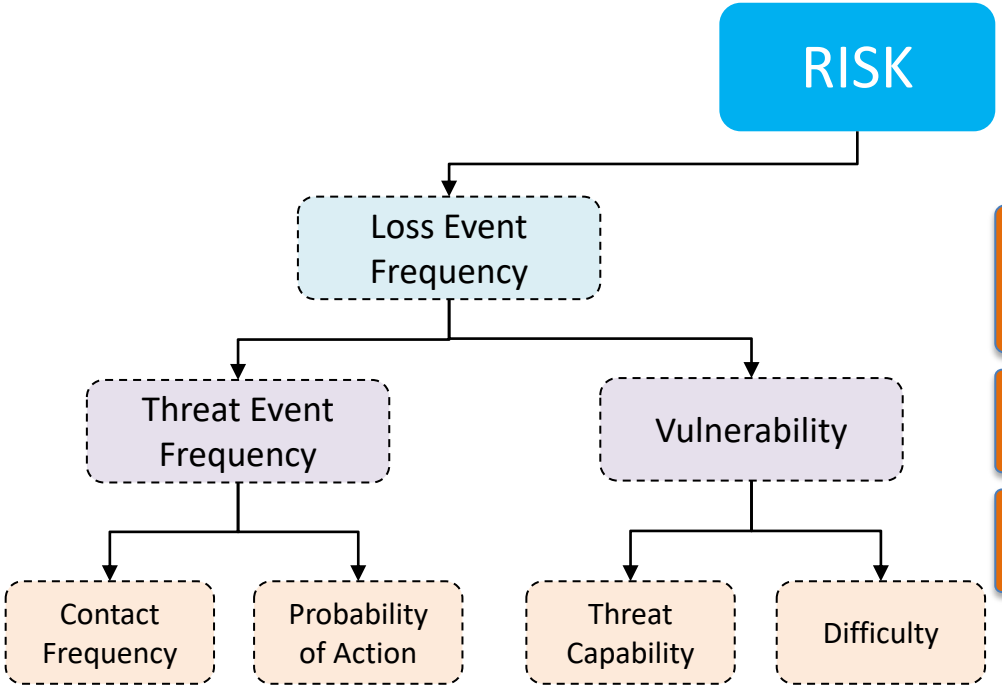
- If we want to reduce risk by reducing PoA, what can we do?
- Affect apparent value of asset (e.g., camouflage), increase apparent level of effort (e.g., hard appearance), or increase perceived level of risk (e.g., camera, monitoring)

Probability of Action

"the probable that a threat agent will act upon an asset once contact has occurred"

UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



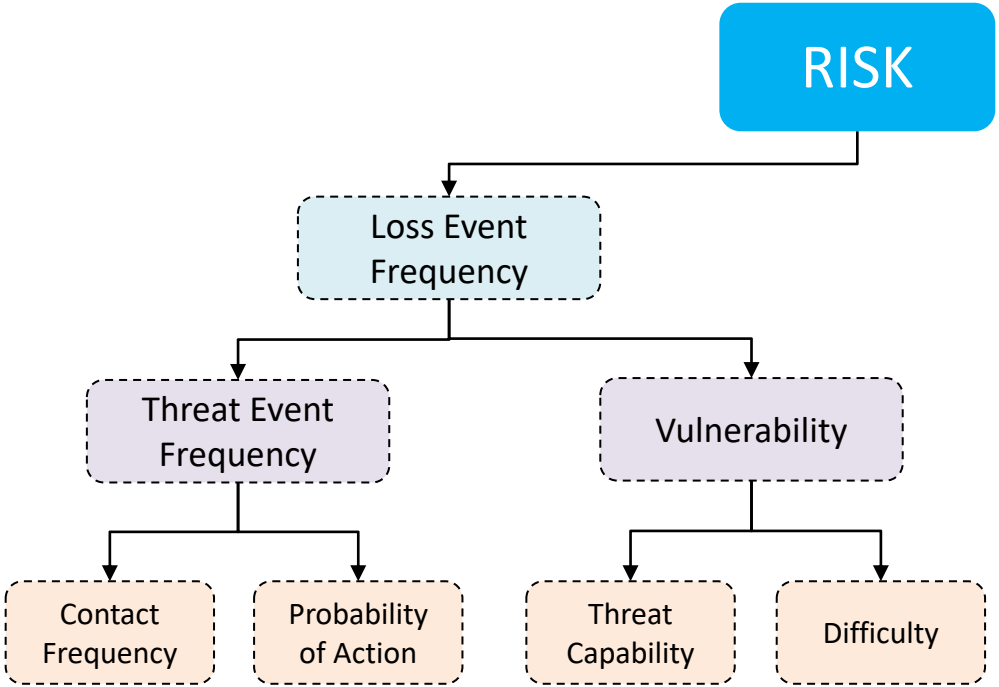
Vulnerability
"the probable that the threat agent's actions will result in loss"

In ISMS, vulnerability has different meaning (e.g., weak password, open window). Strong passwords are vulnerable too, however, the level of effort required is different.

Expressed as a probability distribution, either directly or from Tcap and Difficulty.

E.g., That lock is between 5% and 20% vulnerable, most likely 10% vulnerable, against the Threat Community.

Factor Analysis for Information Risk (FAIR)



Threat Capability
"the capability of the threat agent"

Tcap continuum is a percentile scale between 1 and 100 that represents the capability of the threat community under analysis (e.g., cyber criminals, staff members).

We could say: least capable cyber criminals are at the 60th percentile, most capable are at 100th percentile, and most are at the 90th percentile.

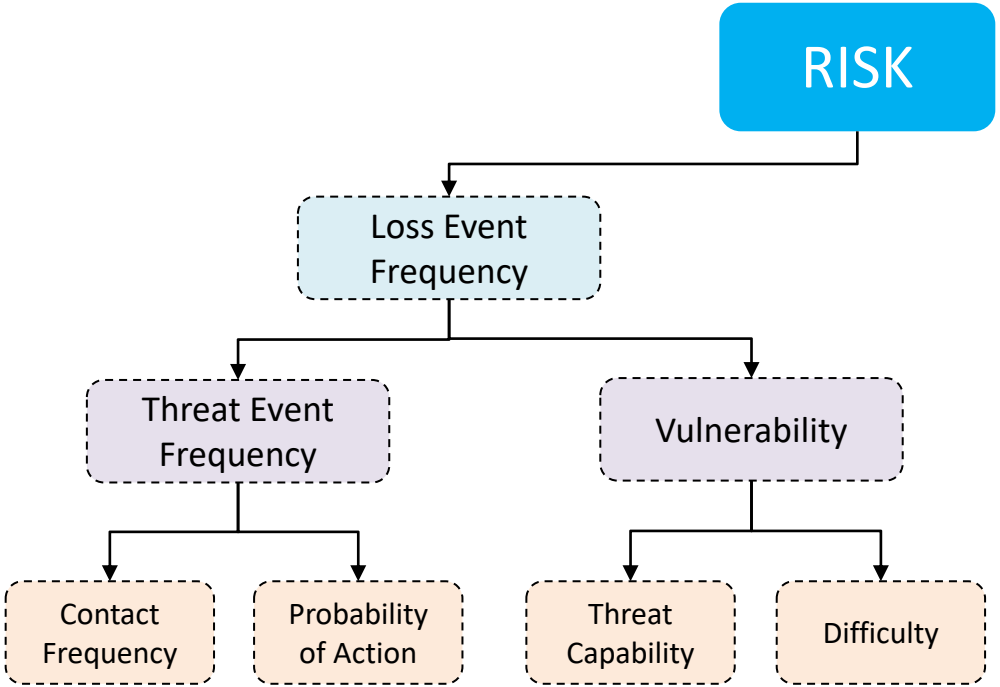
High Tcap is bad in malicious scenarios and good in human error scenarios.

In human error scenarios, we can improve Tcap by providing additional training, improved tools, or time.

In malicious scenarios, we could reduce Tcap by reducing amount of time the threat agent has to complete their attempts to breach resistive controls.

UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



Difficulty

"the level of difficulty that a threat agent must overcome"

Uses the Tcap continuum to represents the difficulty for the population to accomplish. Difficulty is always measured against Tcamp continuum and not the specific threat community.

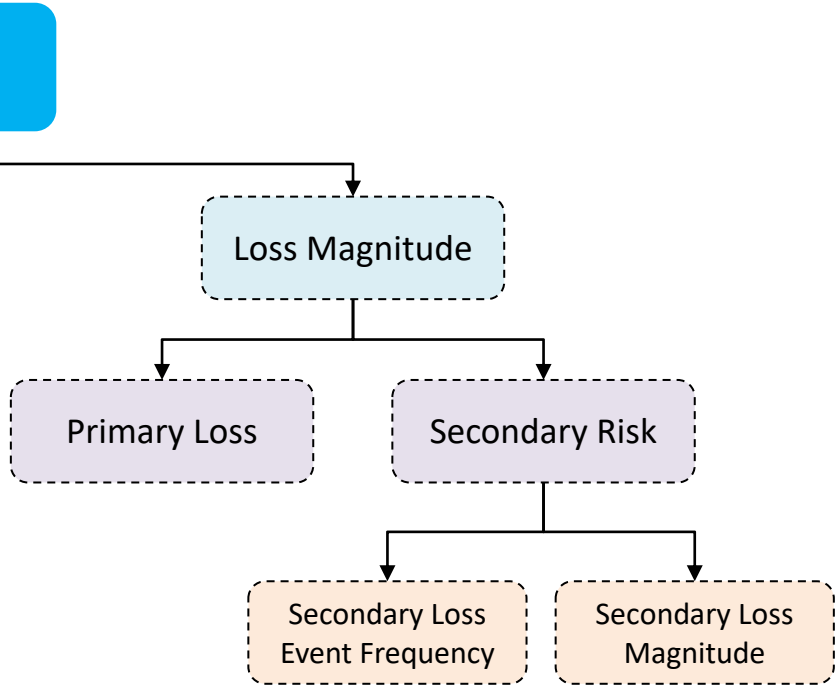
We could say: this will stop anyone below 70th percentile. Anyone above 90th is percentile is gurenteed to succeed. Most would be at 85th.

It must make the threat agent's job more difficult (in malicious case) or easier (in human error case).

E.g., authentication, access, patching, encryption
E.g., training, documentation, simplification

UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



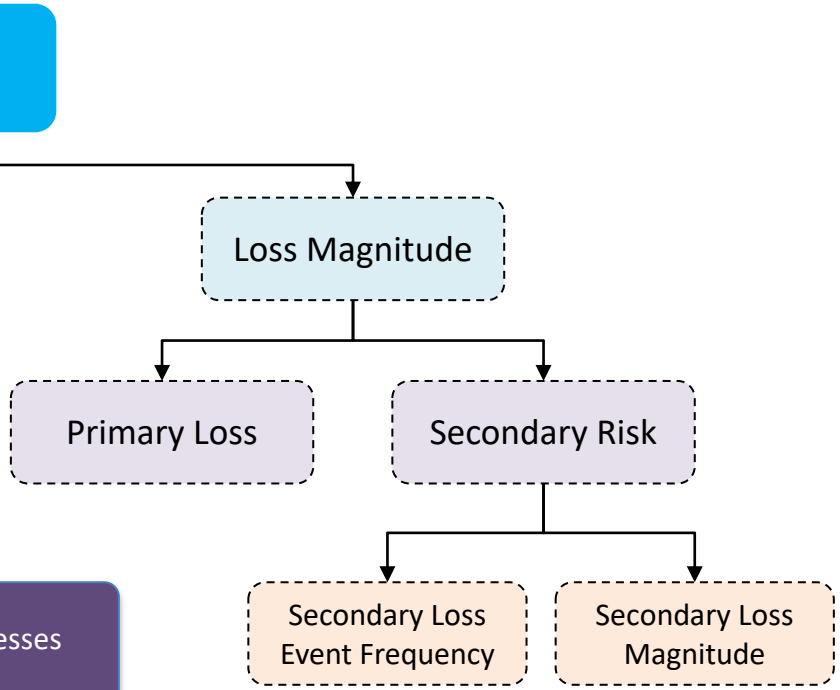
Loss Magnitude

"the probable magnitude of primary and secondary loss resulting from an event"

Primary stakeholders are those individuals or organizations whose perspective is the focus of the risks analysis.

Secondary stakeholders are defined as anyone who is not a primary stakeholder that may be affected by the loss event being analyzed, and then may react in a manner that further harms the primary stakeholder.

Factor Analysis for Information Risk (FAIR)



Primary Loss Magnitude

"primary stakeholder loss that materializes directly as a result of the event"

- Lost revenue from operational outages
- Wages paid to workers when no work is being performed due to outage
- Replacement of the organization's tangible assets (including cash)
- Person-hours spent restoring functionality to assets or operations following an event

- Disaster recovery and business continuity processes and technologies
- Efficient incident response processes
- Process or technology redundancy

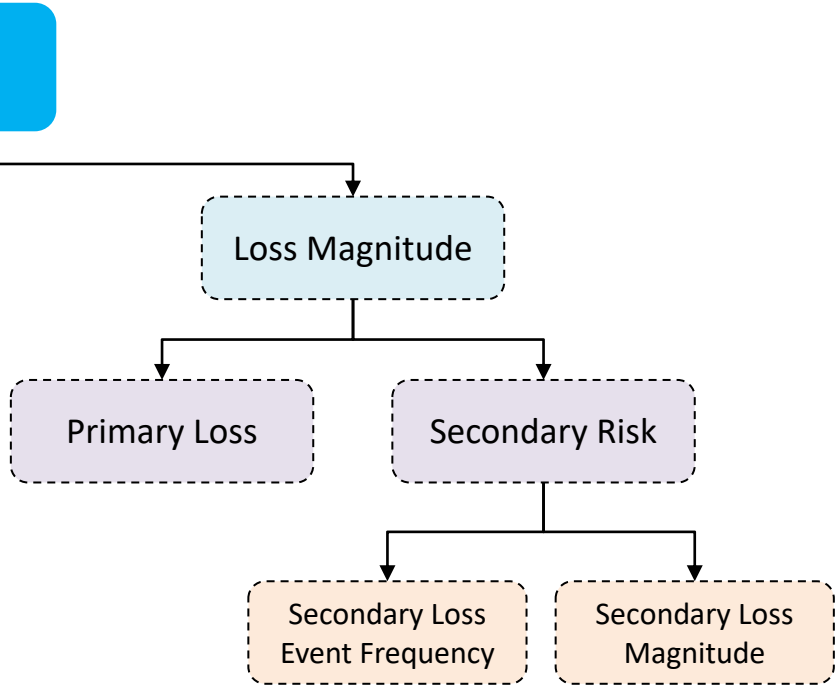
UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)

Secondary Risk

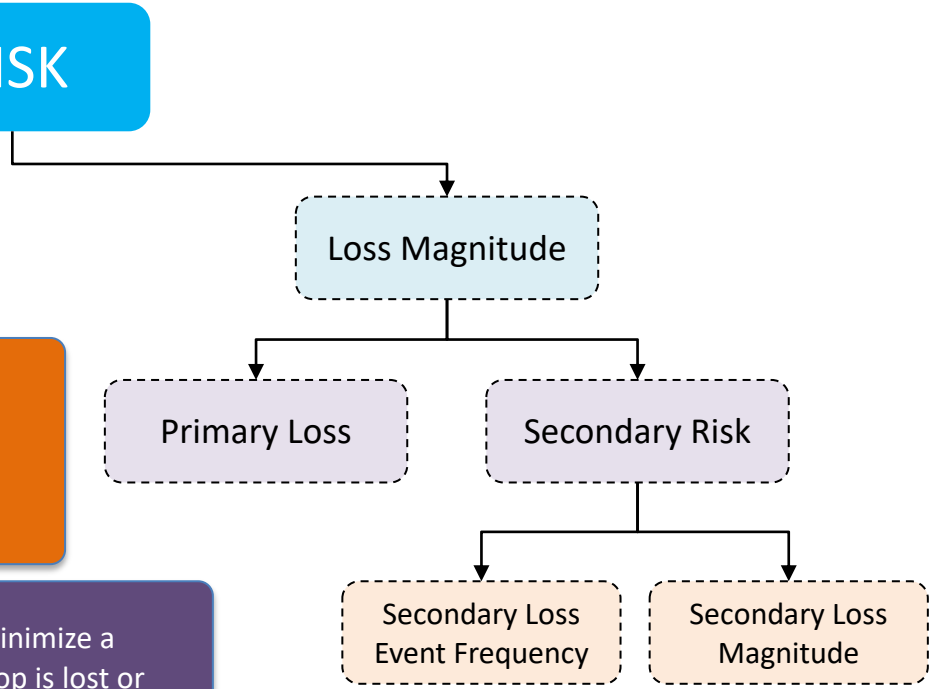
"primary stakeholder loss-exposure that exists due to the potential for secondary stakeholder reactions to the primary event"

- The "fallout" from the primary event – including reputational damage, fines and judgements, and other forms of loss.



UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



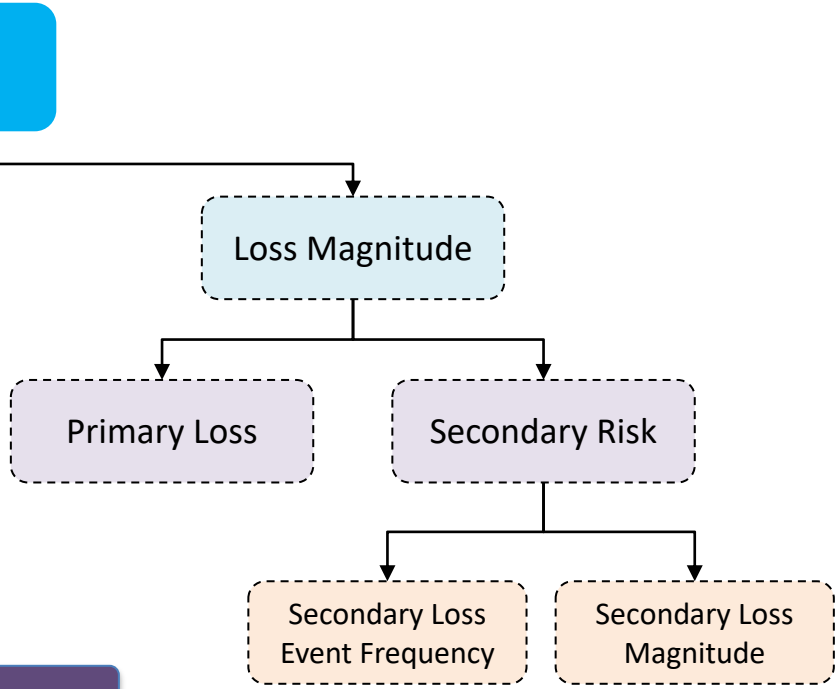
Secondary Loss Event Frequency
"the percentage of primary events that have secondary effects"

- SLEF is represented as a percentage of the primary LEF

- E.g., Encrypted laptops would help to minimize a secondary loss event, such that if a laptop is lost or stolen (a primary loss event) then the data can not be accessed.

UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



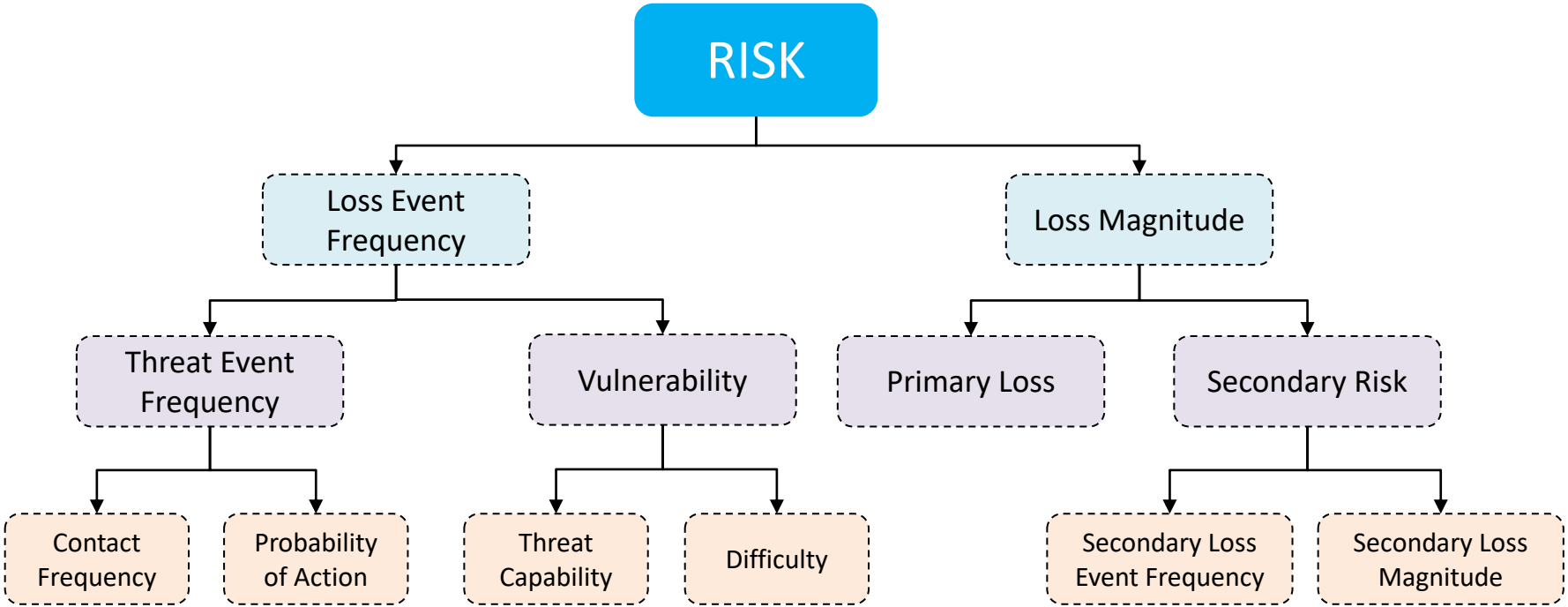
Secondary Loss Magnitude
"loss associated with secondary stakeholder reactions"

- Lost market share, dimished stock price, increased cost of capital, legal defense costs, notification costs, PR costs, fines, etc.…
- 6 forms of (primary and secondary) loss that are commonly referred to in FAIR analysis:
- Productivity, Response, Replacement, Competitive Advantage, Fines and Judgements, and Reputation.

- E.g., timely notification, strong public relation efforts

UWE Bristol University of the West of England

Factor Analysis for Information Risk (FAIR)



Measuring Risk

But we don’t have enough data…

- How does the insurance industry manage this problem?
- “Event cancellation insurance”
- “Cyber insurance”

- “You need less data than you think, and you have more than you think” [Douglas Hubbard, “How to measure anything”]

- Single Loss Event (SLE) losses
- Annualised Loss Event (ALE) losses

Calibration

- How do we measure how much you do or don't know about something?
- How can we use this to improve our estimates?

- Equivalent Bet Test

Equivalent Bet Test

- Either bet on the range containing the right answer, or bet on whether the pointer will spin and land in the orange region (10%).

- Estimators choose the range – suggests the range is too easy
- Estimators choose the wheel – suggests the range is too hard
- Difficult decision - probably 90% confident in answer then

Starting with the Absurd

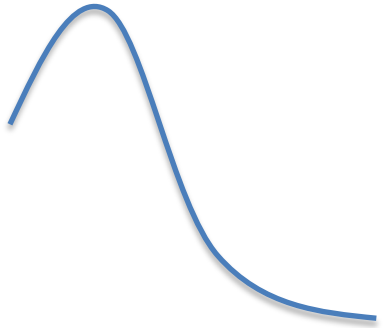
- If someone says it **can not possibly** be estimated
- Set a range that is wildly absurb
  - It's between 1 and 1000000
  - "Well of course it's in that range somewhere"
- Then slowly add to (or subtract from) the range to refine the answer.

- i.e., think about what the answer couldn't possibly be, in order to refine what it may be

UWE Bristol | University of the West of England

Analysing Risk

Monte Carlo Simulation



- We have purposefully defined our model using probability distributions
  - (i.e., min, max, mode)

- Therefore, we could draw sample values for each of our attributes to derive a value of risk (and a SLE and an ALE).

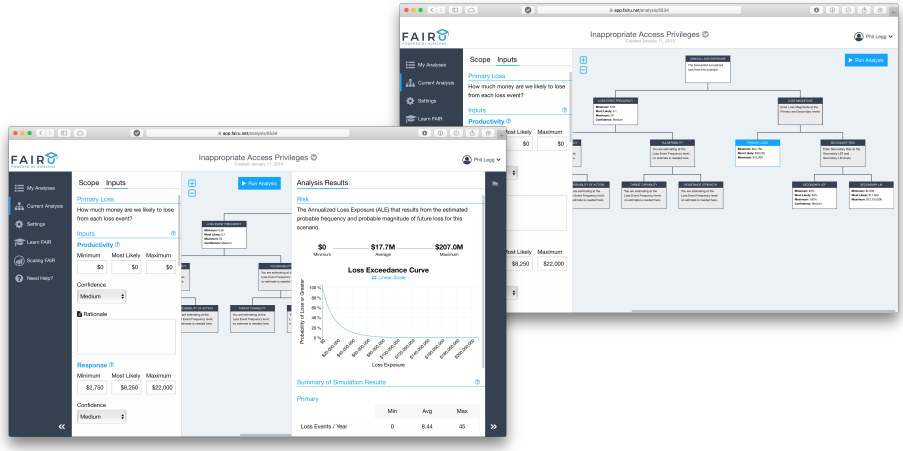
- If we do this many times (e.g., 10000 times), can we generalize the result - this is what is known as a *monte carlo simulation*.
  - *used by casinos to assess the true return of a game, e.g. Roulette*

Performing Risk Analysis

- We can easily create our own simulation tool for conducting a FAIR analysis using Python (or even Excel!)
  - Show link to Jupyter Notebook example

- Commercial Products:
  - E.g. RiskLens

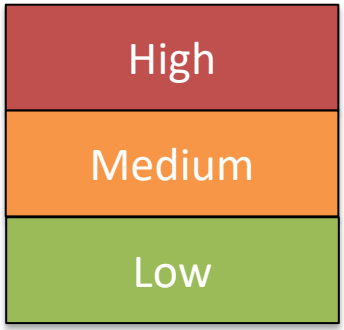
- FAIR-U Online Tool available:
  - https://www.fairinstitute.org/fair-u

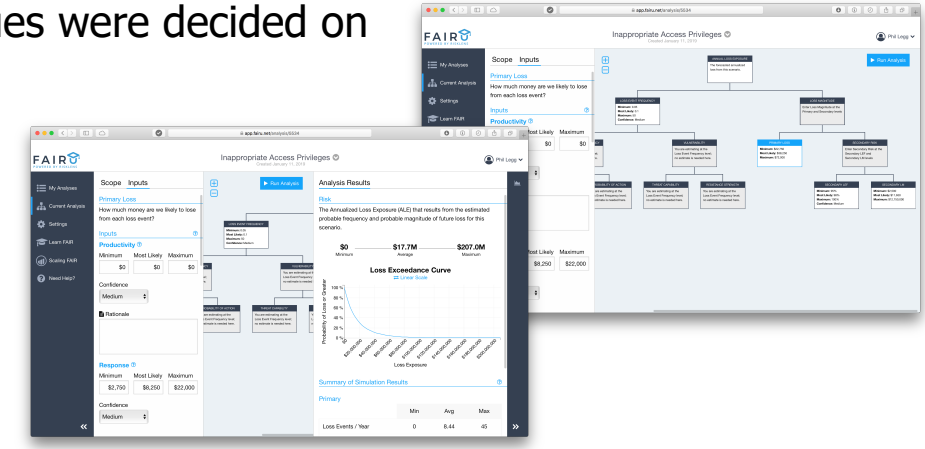


UWE Bristol University of the West of England

Interpreting Risk Analysis

- *"Providing a qualitative interpretation of an analysis is not the same thing as doing a qualitative analysis"*
  - We can easily interpret quantitative results in a qualitative form by simply deciding our bounds
  - This can help C-level understand the key details, whilst also giving justification for how the values were decided on



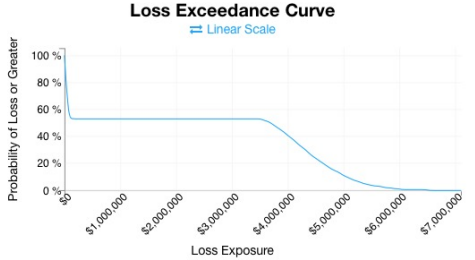


Interpreting Risk Analysis

- The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

Analysis Results

$0	$2.4M	$7.0M
Minimum	Average	Maximum



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	0.54	1
Loss Magnitude	$4.0k	$47.9k	$184.4k

Secondary

	Min	Avg	Max
Loss Events / Year	0	0.53	1
Loss Magnitude	$3.4M	$4.5M	$7.0M

Vulnerability 42.42%

UWE Bristol | University of the West of England

Risk Analysis Examples

Inappropriate Access Privileges

Inappropriate Access Privileges

- *"During a recent audit, it was discovered there were active accounts in a customer service application with inappropriate access privileges. These access were for employees who still worked in the organization but whose job responsibilities no longer required access to this information. Internal audit labeled this a high risk finding"*

- **Asset at Risk:** Account privileges permit access to the entire customer database, comprising of 50000 people. This information includes name, address, DOB. No banking, credit, or other financial information

Inappropriate Access Privileges

- **Tcoms**: *Privileged insiders, non-privileged insiders, cyber criminals.*
- **Threat types:**
  - *Malicious, or*
  - *snooping*

Table 8.1 The Scope Table for Level of Risks Associated with Inappropriate Access Privileges

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Snooping	Confidentiality
Customer PII	Privileged insiders	Malicious	Availability
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Nonpriv insiders	Malicious	Confidentiality
Customer PII	Nonpriv insiders	Malicious	Availability
Customer PII	Nonpriv insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality
Customer PII	Cyber criminals	Malicious	Availability
Customer PII	Cyber criminals	Malicious	Integrity

Inappropriate Access Privileges

- **Can users delete the records?**
  - In our investigation we find they can not – allows us to slim down our scope.

Remember what question we want to answer…

Our next step, then, is to look at the scenarios in our scope table and try to identify one or more scenarios that are likely to be much more (or less) frequent and/or much more (or less) impactful than the others.

Table 8.2 The Slimmed Scope Table

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Snooping	Confidentiality
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Nonpriv insiders	Malicious	Confidentiality
Customer PII	Nonpriv insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality
Customer PII	Cyber criminals	Malicious	Integrity

Inappropriate Access Privileges

- We have refined our scope to those that we consider high risk
  (assessing the level of risk was the question – not the level of all risks)

Table 8.3 The Scope Table with Further Omissions

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Snooping	Confidentiality
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality

Inappropriate Access Privileges

- The most frequent scenario is likely to be snooping
- The most impactful is likely to be the cyber criminals

- *Let's analyse both cases then…*

Table 8.3 The Scope Table with Further Omissions

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Snooping	Confidentiality
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality

Privileged Insider LEF

- Let's start with the left side - What's the Loss Event Frequency?
- We know the value for vulnerability - 100%.
  - Therefore the TEF score is equal the LEF score.

- How to estimate a LEF score? Start with the absurd…
  - Minimum: once every 1000 years, Maximum: a million times a year
  - *Keep in mind – this TEF estimate is constrained to this population of privileged users with inappropriate access, not all privileged users.*
  - *So what is the size of this population?*
  - *15% of access – 30.*
  - *What constitutes an event?*

Privileged Insider LEF

- Let's query the event with HR that prompted this analysis.
- Turns out the 2 people fired were selling this detail – so more than just snooping.

- 2 people in the last 3 years = 0.67 frequency
  - But these were two people who had legitimate access – part of the 170, not the 30!
  - For our population of 30,
  - we take it as 15% percent
  - Min: 0.05, Most likely:0.1, Max: 50

Table 8.4 The Scope Table with the Most Important Scenarios

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Privileged insiders	Malicious	Confidentiality
Customer PII	Privileged insiders	Malicious	Integrity
Customer PII	Cyber criminals	Malicious	Confidentiality

Privileged Insider LEF

- What is the loss magnitude of this event?

- Primary response costs:
- Staff: 50 hours – 400 hours
- Aver hourly rate of $55

- Replacement of staff:
- Costing can be found from HR

Table 8.7 Primary LEF Response and Replacement Estimates

Loss Type	Minimum	Most Likely	Maximum	Confidence
Primary response	$2750	$8250	$22,000	Moderate
Primary replacement	$20,000	$30,000	$50,000	High

Privileged Insider LEF

- Secondary Loss
- Assessed for the 6 categories
  - Only need response, fines, and reputation

Table 8.9 Loss Estimates due to a Customer Information Compromise Analysis

	Minimum	Most Likely	Maximum	Confidence
Notification	$3	$60	$1,500,000	Moderate
Customer support	$0	$20	$500,000	Moderate
Credit monitoring	$0	$50	$1,250,000	Moderate
Meetings	$2500	$6250	$50,000	Moderate
Legal	$0	$5000	$500,000	Moderate
PR	$0	$0	$3,000,000	Moderate

Table 8.12 Secondary Loss Estimates Involving Reputation Damage

Loss Type	Minimum	Most Likely	Maximum	Confidence
Sec response	$2500	$11,500	$7,000,000	Moderate
Sec fines & judgments	$0	$0	$2,000,000	Moderate
Sec reputation	$0	$150	$3,750,000	Moderate

Privileged Insider LEF

- FAIR risk analysis for inappropriate access privileges
- Single Loss Event (SLE) magnitude – just over $4M – this is a worst case outcome

FIGURE 8.2

FAIR risk analysis for inappropriate access privileges.

Privileged Insider LEF

- Max Total Loss Exposure
- $23M!!!

- Driven by 14 for Primary Loss Events Per Year
- (Whilst you may try to remedy once 1 event occurs… do we know in time?)

FIGURE 8.2

FAIR risk analysis for inappropriate access privileges.