Modern Security Risk

CISO Mentor

Phil Huggins, Director, CISO Mentor Ltd

Common Security Practices: Analysis

Lists of Risks

Overlaps

Gaps

Assumes independence

Category Labels

Imprecise

Unreliable

Range compression

Single Likelihood Estimates

Implies precision

Hides uncertainty

Worst Case Estimates

Aggregation of risks unbelievable

Likely to be in the tail of the risk

Probability X Impact

Doesn’t reflect reality

Common Security Practice: Presentation

Risk Matrix

Throws away data
Does not allow aggregation
Often uses log scales
Saw-tooth tolerance

How bad is a yellow risk?
How many yellows are a red worth?
Is a thousand green risks acceptable?

>75%	Very high	🟩	🟨	🟥	🟥	🟥
50% - 75%	High	🟩	🟨	🟨	🟥	🟥
25% - 50%	Medium	🟩	🟩	🟨	🟨	🟥
5% - 25%	Low	🟩	🟩	🟩	🟨	🟨
<5%	Very Low	🟩	🟩	🟩	🟩	🟩
		Very Low	Low	Medium	High	Very High
		<£10K	£10K - £50K	£50K - £200K	£200K - £1M	>£1M

Levels of Uncertainty in Risk

Level 0

- Identification of Hazard
- Failure Mode Identification

Level 1

- Worst Case
- Cybergeddon

Level 2

- Plausible Upper Bound
- What is a reasonable worst case?

Level 3

- Best Estimate
- Central Value
- Mean / Median
- No Long Tails

Level 4

- Probabilistic Analysis
- Single Risk Curve

Level 5

- Probabilistic Analysis
- Multiple Risk Curves

From: M Elisabeth Pate-Cornell, 1996, Uncertainties in Risk Management: Six Levels of Treatment

Modern Risk Practices: Calibrated Estimation

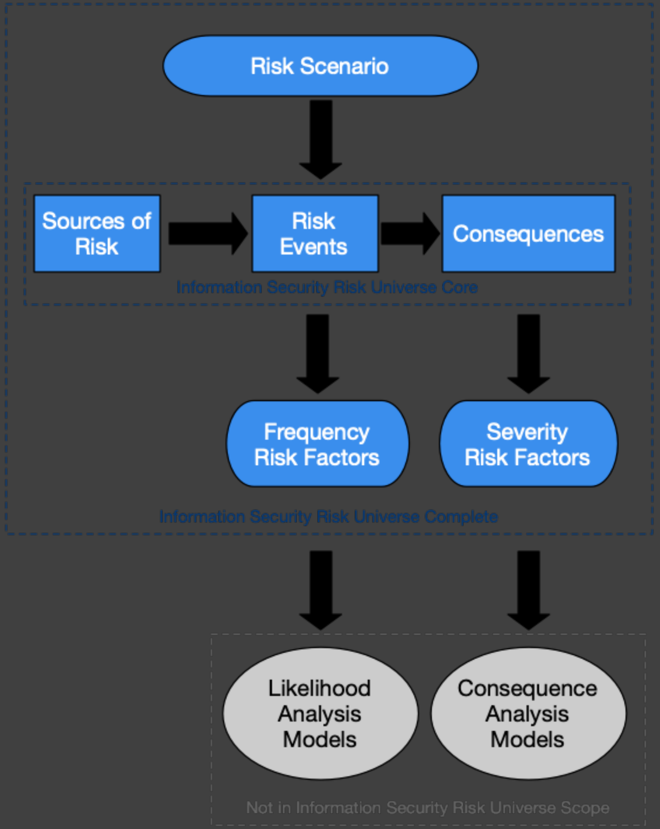
Accuracy (Calibration) beats precision (Discrimination). Both are good to have.

Expert estimates are by nature subjective, uncertain and biased, there are ways to counter this:

- Measuring internal & external base-rate data to indicate risk factors
  - *Lots of data available but discrimination and analysis required.*
- Internal & external expert estimation
- Panel-based estimation
- Delphi technique
- Risk calibration training for experts
  - *90% confidence interval, avoid anchoring*
  - *General knowledge tests*
- Brier Scores for annual feedback

Modern Risk Practices: Risk Universe

There is a risk that <**source**> causes <**event**> that causes <**consequence**>.



Risk Scenario

Sources of Risk → Risk Events → Consequences

Information Security Risk Universe Core

Frequency Risk Factors

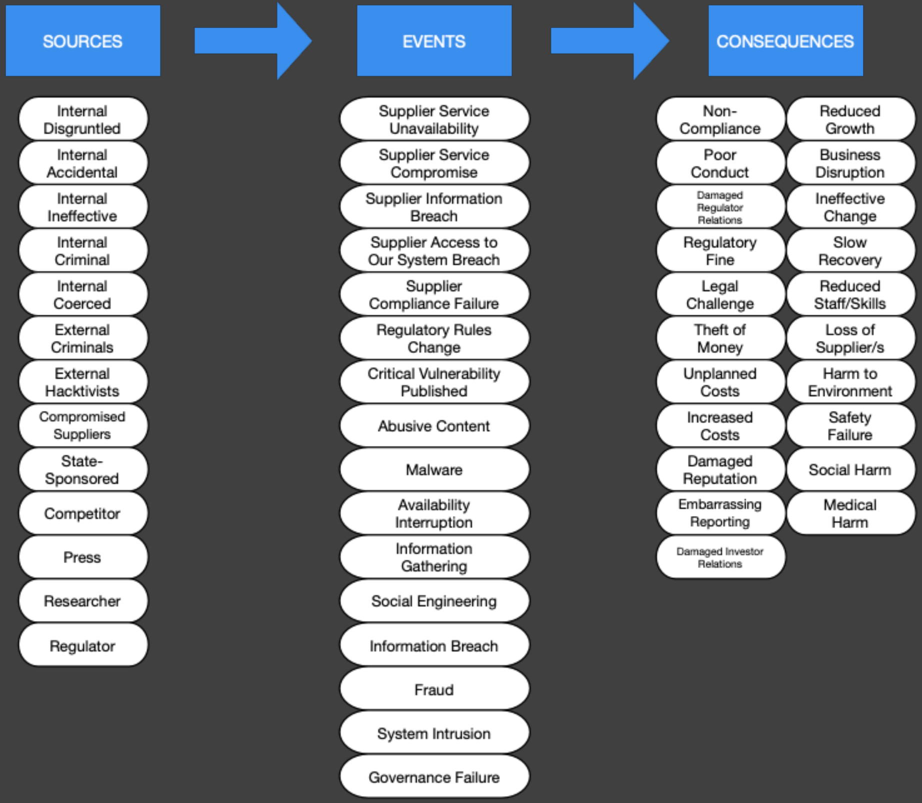
Severity Risk Factors

Information Security Risk Universe Complete

Likelihood Analysis Models

Consequence Analysis Models

Not in Information Security Risk Universe Scope



SOURCES → EVENTS → CONSEQUENCES

SOURCES
- Internal Disgruntled
- Internal Accidental
- Internal Ineffective
- Internal Criminal
- Internal Coerced
- External Criminals
- External Hacktivists
- Compromised Suppliers
- State-Sponsored
- Competitor
- Press
- Researcher
- Regulator

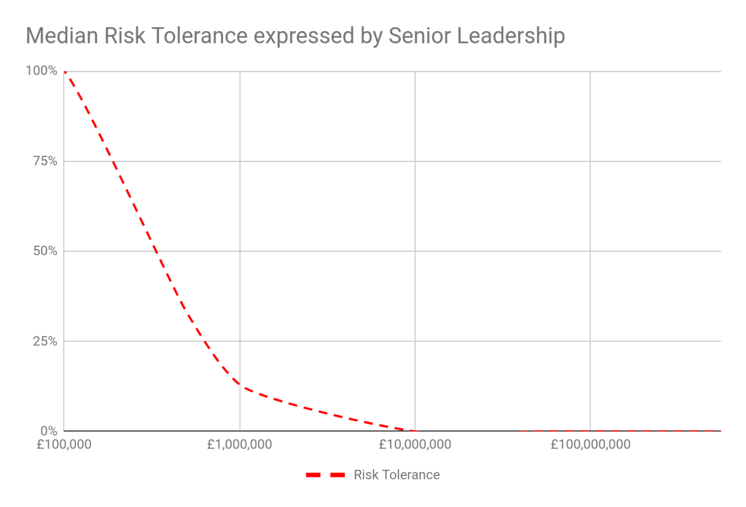
EVENTS
- Supplier Service Unavailability
- Supplier Service Compromise
- Supplier Information Breach
- Supplier Access to Our System Breach
- Supplier Compliance Failure
- Regulatory Rules Change
- Critical Vulnerability Published
- Abusive Content
- Malware
- Availability Interruption
- Information Gathering
- Social Engineering
- Information Breach
- Fraud
- System Intrusion
- Governance Failure

CONSEQUENCES
- Non-Compliance
- Poor Conduct
- Damaged Regulator Relations
- Regulatory Fine
- Legal Challenge
- Theft of Money
- Unplanned Costs
- Increased Costs
- Damaged Reputation
- Embarrassing Reporting
- Damaged Investor Relations
- Reduced Growth
- Business Disruption
- Ineffective Change
- Slow Recovery
- Reduced Staff/Skills
- Loss of Supplier/s
- Harm to Environment
- Safety Failure
- Social Harm
- Medical Harm

From: Open Information Security Risk Universe https://github.com/oracuk/oisru

CISO Mentor Ltd

Modern Risk Practices: Tolerance Curve



Avoid forcing stakeholders to do maths in their head.

Avoid qualitative descriptors, they are interpreted differently by different people.

Median value handles overly risk hungry executives, weighting executive scores by ownership also appropriate.

Expected Rate of Occurrence / Frequency	Monthly Likelihood	Annual Likelihood
Once a month	100.00%	12 x 100%
Once a quarter	33.33%	4 x 100%
Once every six months	16.67%	2 x 100%
Once a year	8.33%	100%
Once every two years	4.17%	50%
Once every three years	2.78%	33.33%
Once every five years	1.67%	20.00%
Once every ten years	0.83%	10.00%
Once every fifteen years	0.55%	6.66%%

CISO Mentor Ltd

Modern Risk Practices: Quantitative Analysis

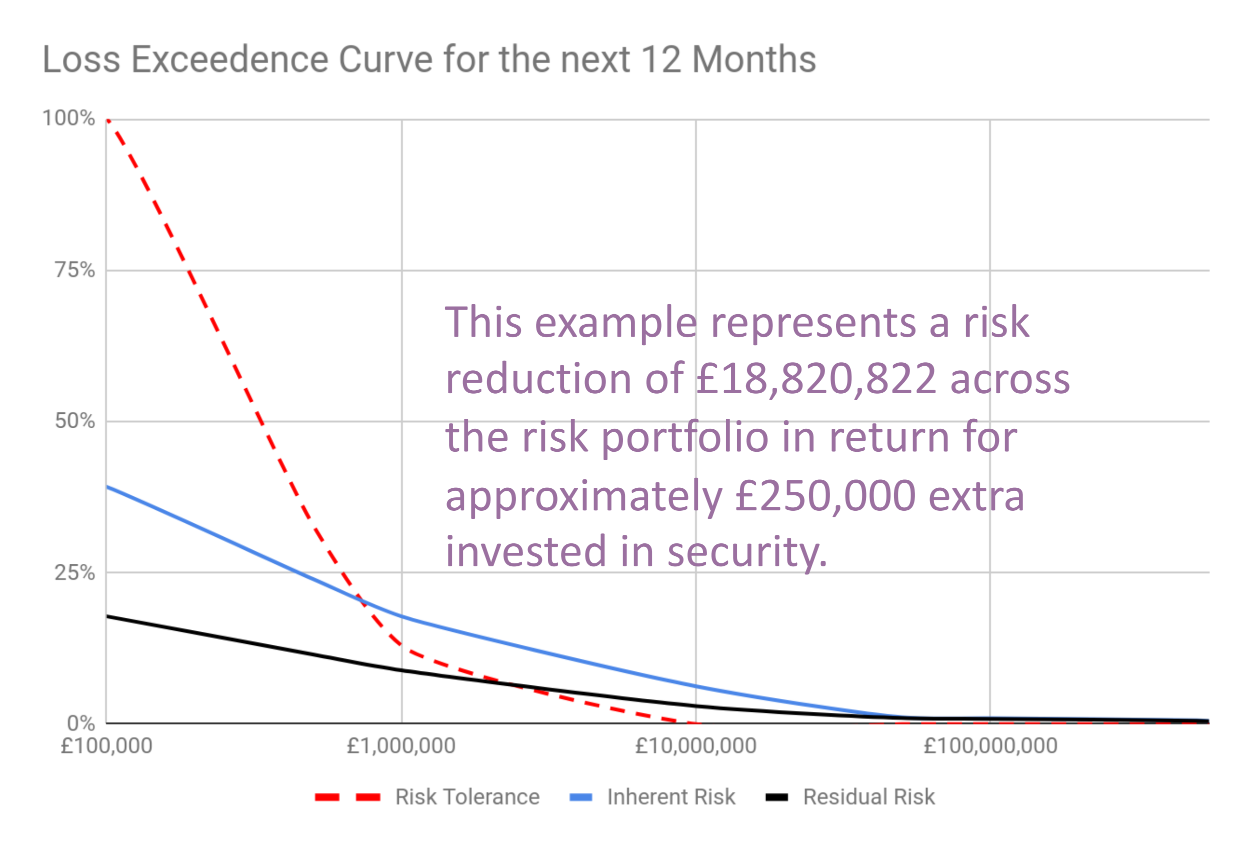
Likelihood, minimal harm and maximal harm estimates.

Standard Monte Carlo simulation run tens of thousands of times and combined.

Lognormal distribution for harm.

Simulate both risks individually and as a portfolio of risk.

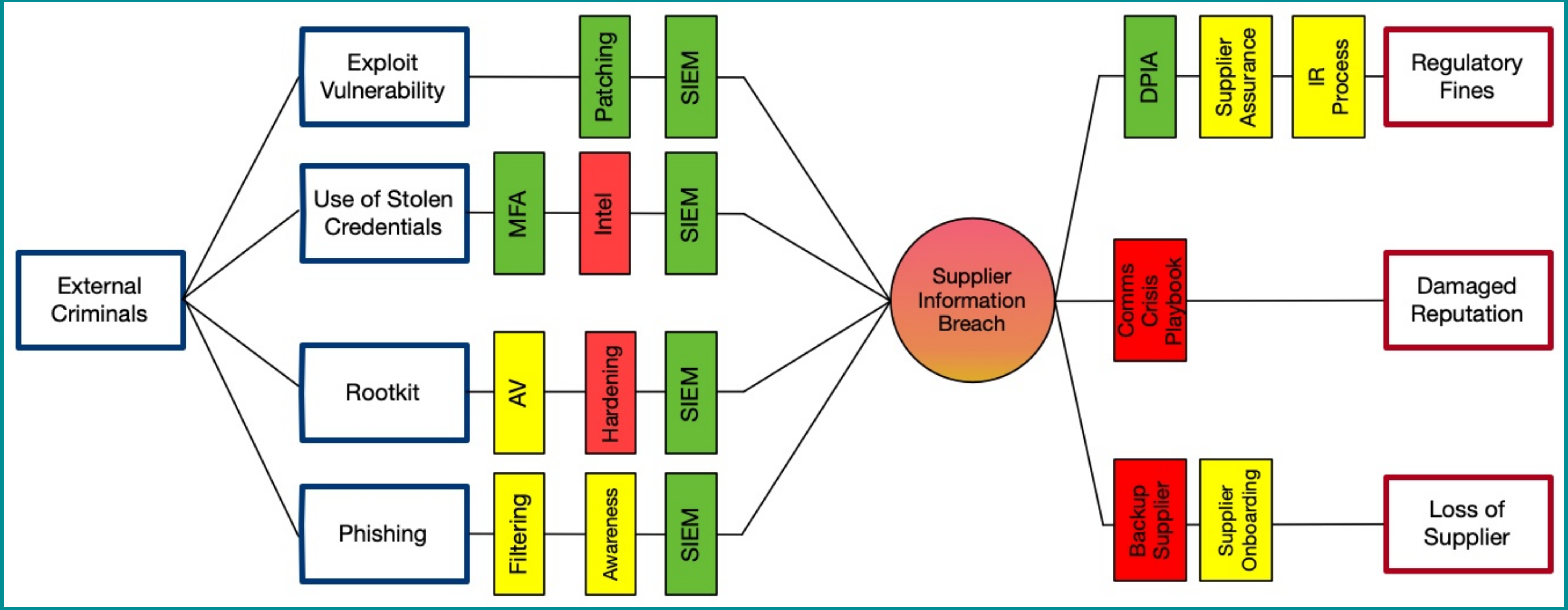
Aggregate the risk exposure for board consideration.


Loss Exceedence Curve for the next 12 Months

This example represents a risk reduction of £18,820,822 across the risk portfolio in return for approximately £250,000 extra invested in security.

CISO Mentor Ltd

Modern Risk Practices: Bow-Tie Diagram



Further Reading

Books:

How to Measure Anything in Cybersecurity Risk, Hubbard & Seiersen

Measuring and Managing Information Risk: A FAIR Approach, Freund & Jones

Uncertain Judgements: Eliciting Experts' Probabilities, O'Hagan

Risk Assessment and Decision Analysis with Bayesian Networks, Fenton & Neil

Groups:

Society of Information Risk Analysts (SIRA)

FAIR Institute

Cyentia Institute

Standards:

ISO 31010 - Risk Management - Risk Assessment Techniques

Sites:

https://magoo.github.io/simple-risk/

http://blog.blackswansecurity.com/category/risk/

Papers:

A New Approach for Managing Operational Risk, Society of Actuaries

Information Risk Insights Study (IRIS 20/20), Cyentia Institute

Three influential risk foundation papers from the 80s and 90s: Are they still state-of-the-art? Terje Aven

Uncertainties in Risk Management: Six Levels of Treatment, M Elisabeth Pate-Cornell

The risk concept—historical and recent development trends, Terje Aven

What's Wrong with Risk Matrices?, Louis Anthony (Tony)Cox Jr

Estimation of losses due to cyber risk for financial institutions, Antoine Bouveret

Hype and heavy tails: A closer look at data breaches, Edwards, Hofmeyr & Forrest

Delphi, Norman C. Dalkey

Judgemental Decomposition: When does it work? MacGregor & Armstrong

Lessons learned from the real world application of the Bow-tie method, Risktec

Supporting on-going capture and sharing of digital event data, CRO Forum

Reference Incident Classification Taxonomy: Task Force Status and Way Forward, ENISA

Quantitative Techniques in Information Risk Analysis, ISF

Thank you

Phil Huggins, Director, CISO Mentor Ltd
phil@cisomentor.com
www.cisomentor.com

CISO Mentor