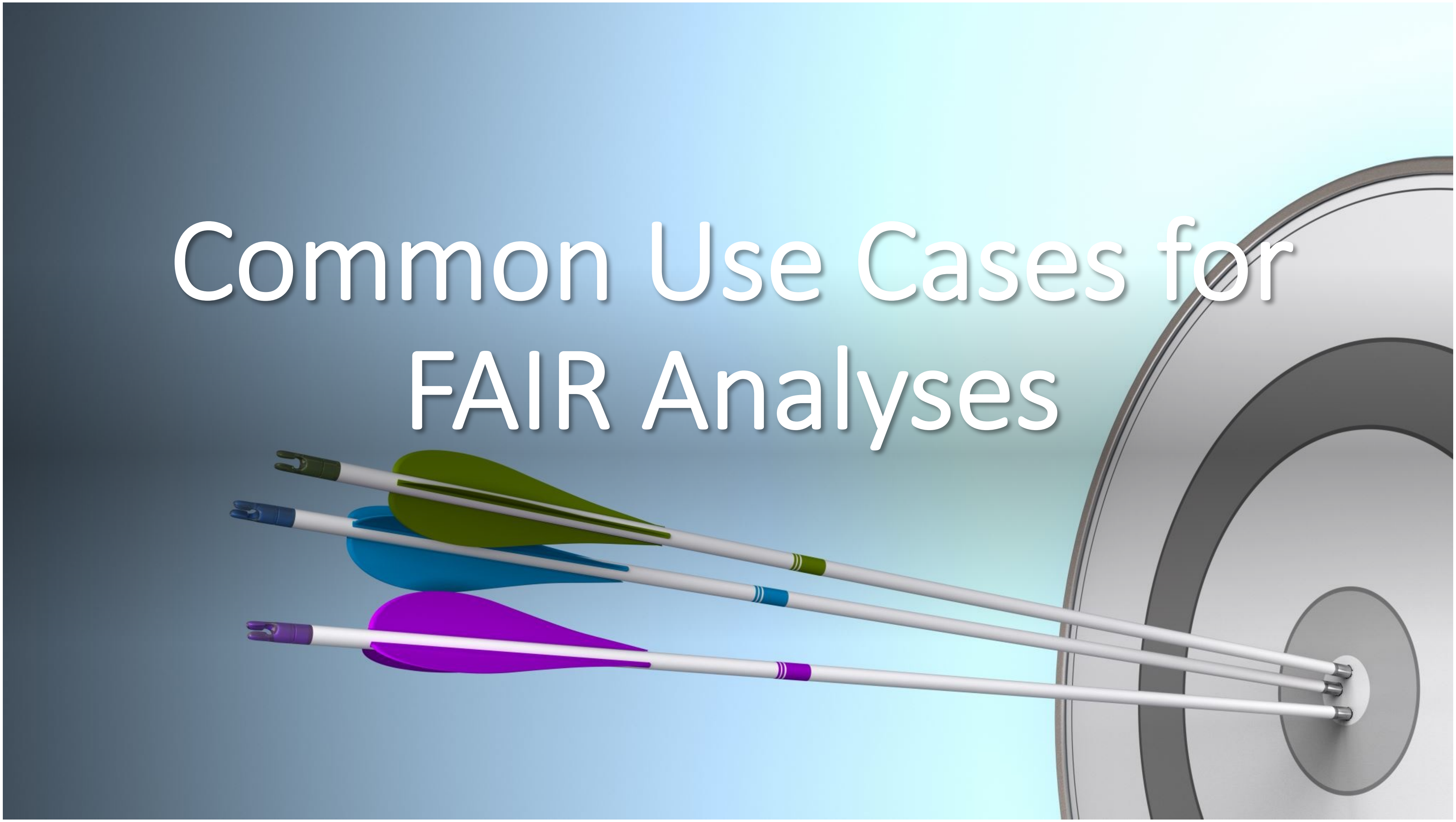
Common Use Cases for FAIR Analyses



Tony Martin-Vegue

Twitter: @tdmv
LinkedIn: linkedin.com/in/tonymartinvegue/
Blog: tonym-v.com
Email: tony.martinvegue@gmail.com

Work

- Quant risk team at Netflix (*opinions are my own*)
- IT & InfoSec: 20+ years; technology risk for 11
- On the board of the Society of Information Risk Analysts (SIRA) and co-Chair of the SF Bay Chapter of the FAIR Institute

Walk-On Song

- "Problem Child" by AC/DC

Something you don't know about me

- I've swum from Alcatraz to San Francisco 10 times

Agenda

Where do I get my data?

- Quantitative versus qualitative data
- Subjective versus objective data
- Gathering external data
- Gathering internal data
- Utilizing SME estimates

Common use cases

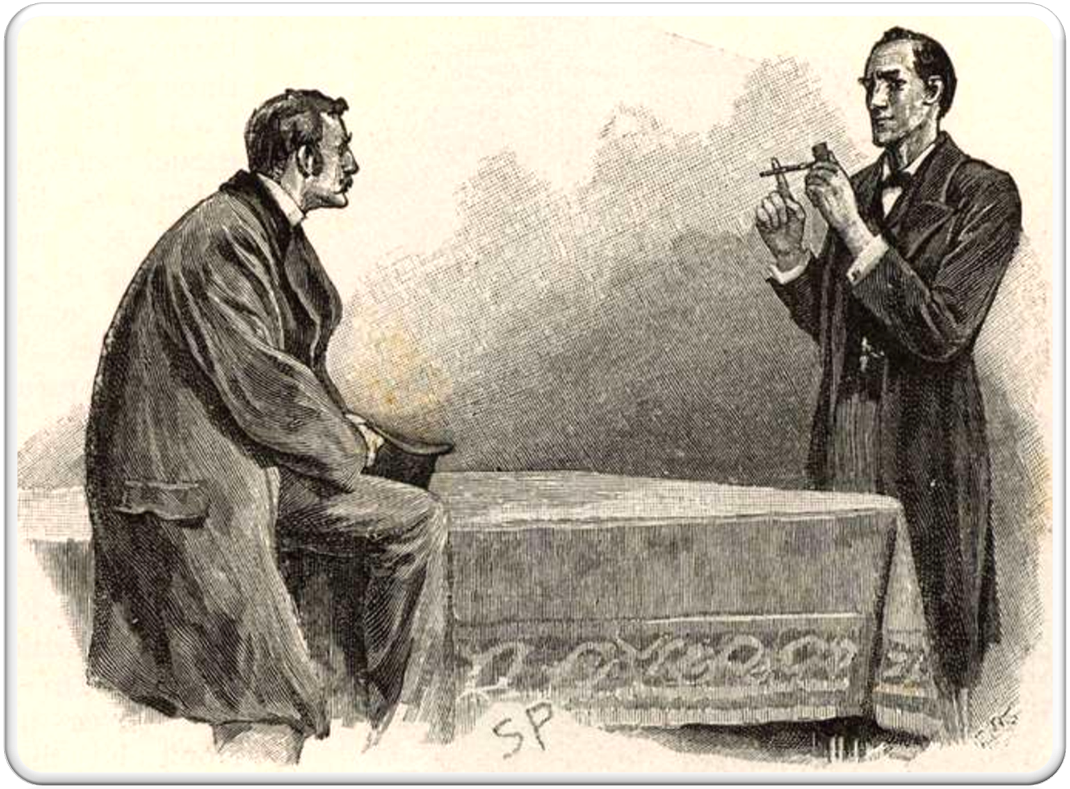
- FAIR and risk appetite / tolerance
- FAIR for optimized risk mitigation
- FAIR for insurance analysis
- FAIR to… increase risk?

Q&A

Where do I get my data?

“It is a capital mistake to theorize before one has data.”

Sir Arthur Conan Doyle (Sherlock Holmes)



Qualitative –vs- Quantitative

Qualitative

- Descriptive
- Adjectives
- Arbitrary rankings
- Opinions, feelings

Examples:

- High, medium, low
- Red, yellow, green
- Fast, not fast, slow

Quantitative

- Numerical data
- Counting
- Ratios
- Measurements

Examples:

- 3 chairs at the table
- He’s between 5’ and 5’ 6” tall
- It rained 5 times in SF last month

Subjective –vs- Objective

Subjective

- Personal opinions
- Feelings
- Judgement

Examples:

- That risk feels high
- Incidents will increase by 10% next year

Objective

- Observations
- Measurements

Examples:

- It’s 70- degrees today
- We had one reportable data breach last year

Objective, subjective, quantitative, qualitative

	Qualitative Data	Quantitative
Subjective	High, medium low Interviews Reports that describe a risk	Expert estimation of future incident counts Ponemon Cost of a Data Breach Report
Objective	Incident reports Grouping data with adjective (e.g fastest car in a race)	Incident counts How much an incident cost Verizon DBIR & Cyentia IRIS 2020

Objective, subjective, quantitative, qualitative

	Qualitative Data	Quantitative
Danger Subjective	High, medium low Interviews Reports that describe a risk	Expert estimation of future incident counts Ponemon Cost of a Data Breach Report
Objective	Incident reports Grouping data with adjective (e.g fastest car in a race)	Incident counts How much an incident cost Verizon DBIR & Cyentia IRIS 2020

Objective, subjective, quantitative, qualitative

	Qualitative Data	**Quantitative**
Subjective	High, medium low Interviews Reports that describe a risk	Expert estimation of future incident counts Ponemon Cost of a Data Breach Report
Objective	Incident reports Grouping data with adjective (e.g fastest car in a race)	Incident counts How much an incident cost Verizon DBIR & Cyentia IRIS 2020

Objective, subjective, quantitative, qualitative

	Qualitative Data	**Quantitative**
Subjective	High, medium low Interviews Reports that describe a risk	Expert estimation of future incident counts Ponemon Cost of a Data Breach Report
Objective	Incident reports Grouping data with adjective (e.g fastest car in a race)	Incident counts How much an incident cost Verizon DBIR & Cyentia IRIS 2020

Objective, subjective, quantitative, qualitative

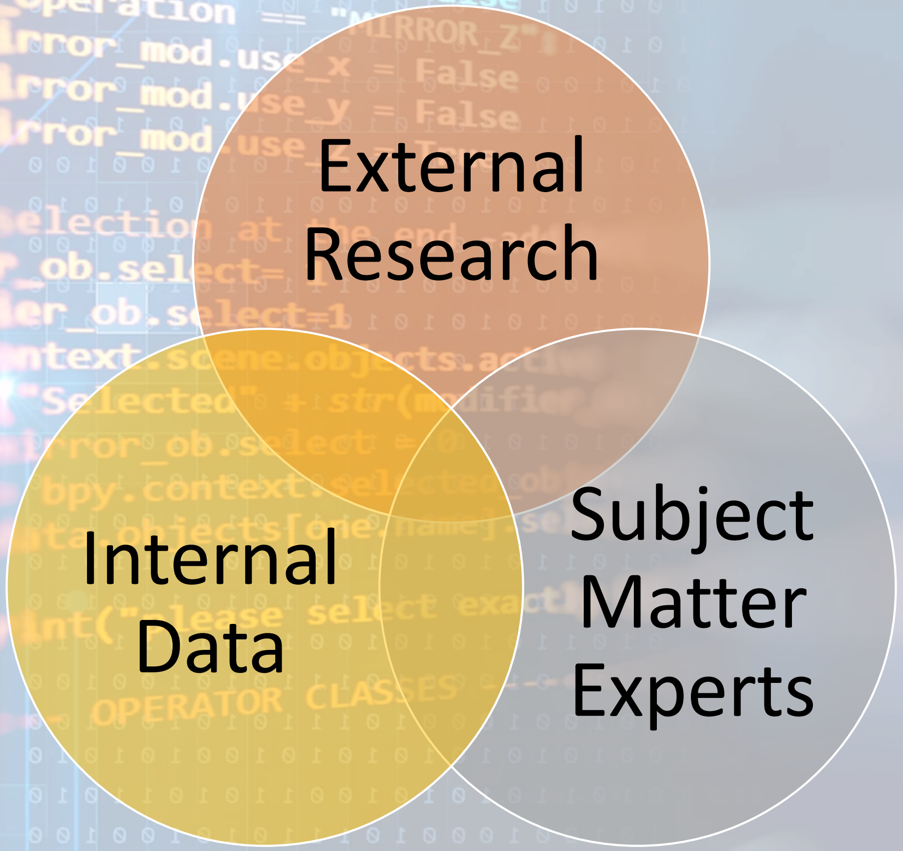
	Qualitative Data	Quantitative
Subjective	High, medium low Interviews Reports that describe a risk	Expert estimation of future incident counts Ponemon Cost of a Data Breach Report
Objective	Incident reports Grouping data with adjective (e.g fastest car in a race)	Incident counts How much an incident cost Verizon DBIR & Cyentia IRIS 2020

Objective, subjective, quantitative, qualitative

	Qualitative Data	Quantitative
Subjective	High, medium low Interviews Reports that describe a risk	Expert estimation of future incident counts Ponemon Cost of a Data Breach Report
Objective	Incident reports Grouping data with adjective (e.g. fastest car in a rac	Incident counts How much an incident cost Verizon DBIR & Cyentia IRIS 2020

Good Zone

Where we get our data



External Research

Internal Data

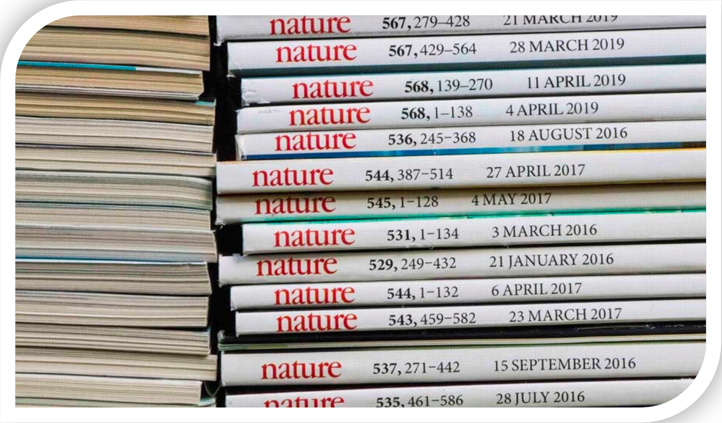
Subject Matter Experts

COMEDIAS DE TIRSO DE MOLINA
240
248
256
JOSE MARIA DE PEREDA OBRAS COMPLETAS II
JOSE MARIA DE PEREDA OBRAS COMPLETAS I
CALDERÓN DE LA BARCA OBRAS
EL EPIGRAMA ESPAÑOL
Santos de Carrión Proverbios Morales
El teatro español Medieval y del Renacimiento
JUAN VALERA OBRAS COMPLETAS
249
50 DON QUIJOTE DE LA MANCHA
PAGAZARRI AL NERVION
241
257
Alejo Carpentier La consagración de la primavera
Luis S. Granjel
OBRAS COMPLETAS DE PEREZ LUGIN
Jorge Guillén Y OTROS POEMAS
PICARESCA ESPAÑOLA TOMO I
PICARESCA ESPAÑOLA TOMO II
PICARESCA ESPAÑOLA TOMO III
PICARESCA ESPAÑOLA TOMO IV
250
Alberto Insua OBRAS SELECTAS
MARIANO J. DE LARRA «FIGARO»
242
258

External Research

Some External Research Sources

Journal / Academic papers



Where to find

- Sci Hub
- Directory of Open Access Journals
- Science Open

How to Use

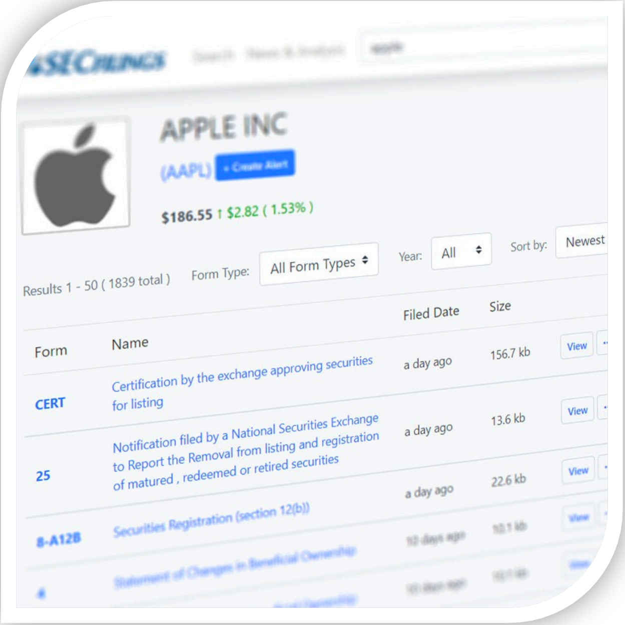
- Mostly techniques, research on risk
- Some trends on emerging risk or impact studies

Pro Tip

- If you feel stuck on a concept, look at how other disciplines have solved the same problem – information / cyber risk is not unique

Some External Research Sources

SEC Filings


SECFilings

APPLE INC

(AAPL) + Create Alert

$186.55 ↑ $2.82 (1.53%)

Results 1 - 50 (1839 total) Form Type: All Form Types Year: All Sort by: Newest

Form	Name	Filed Date	Size	
CERT	Certification by the exchange approving securities for listing	a day ago	156.7 kb	View
25	Notification filed by a National Securities Exchange to Report the Removal from listing and registration of matured , redeemed or retired securities	a day ago	13.6 kb	View
8-A12B	Securities Registration (section 12(b))	a day ago	22.6 kb	View
4	Statement of Changes in Beneficial Ownership	10 days ago	10.1 kb	View

Where to find

- [SEC's EDGAR search](), or
- Company's website

How to Use

- Public companies are required to file a 10-K annual report with the SEC; usually contain a treasure trove of information following a data breach or major incident
- Find a company that had a similar incident that you are assessing risk for. Look for a 10-K for the following year.

Pro Tip

- Companies will usually disclose how are are responding to an incident, sometimes with costs, and can help informs the magnitude portion of an assessment

Some External Research Sources

Vendor Research / Whitepapers

The State of the Internet
Secureworks
Threat Intelligence Executive Report
Tripwire Enterprise: System, Compliance Policy and File Integrity Monitoring Reports
RIPPLES ACROSS THE RISK SURFACE
KENNA Security
Cyentia
PRIORITIZATION TO PREDICTION
Volume 5: In Search of Assets at Risk
Cyentia
Information Risk Insights Study
IRIS 20 20
Advisen

Where to find

- Company websites and the Cyentia Research Library

How to Use

- Good to reference for trends, emerging risks and incidents at other companies.
- Can help you separate out probable from improbable (Verizon DBIR)
- Cyentia IRIS 2020 and Kenna's EPSS calculator are good for risk analysis

Pro Tip

- Some of the very best and the very worst research comes from vendors
- Beware survey based research

Some External Research Sources

Lists of Incidents

Where to find

- ID Theft Center lists
- Raw DBIR data aka VERIS
- Privacy Rights Clearing House (gone dark?)

How to Use

- Peruse how incidents have unfolded at other companies
- Slice and dice your own data – by sector, technique, effect, actor, etc

Pro Tip

- Under a specific incident definition, there's an almost complete incident list
- Can use sampling to determine probability

Internal Data

Some Internal Data Sources

Internal Incidents

Where to find

- Incident responder teams

How to Use

- Ask for access to incident tickets (e.g. JIRA)
- Look for patterns of incidents, threats, assets, etc.

Pro Tip

- May be able to directly use for forecasts - if we have 10 years of consistent incident reporting and there has been 2 ransomware incidents, it’s reasonable to say that there’s 1 every 5 years or 20% probability

Some Internal Data Sources

Other

Where to find

- Event logs, system telemetry, vuln scans, pen tests

How to Use

- Most useful in the scoping and scenario building process

Pro Tip

- Don’t get bogged down when easier data sources are sufficient

Subject Matter Experts

Subject Matter Experts

Expert Judgement

Where to find

- Subject matter experts within your company;

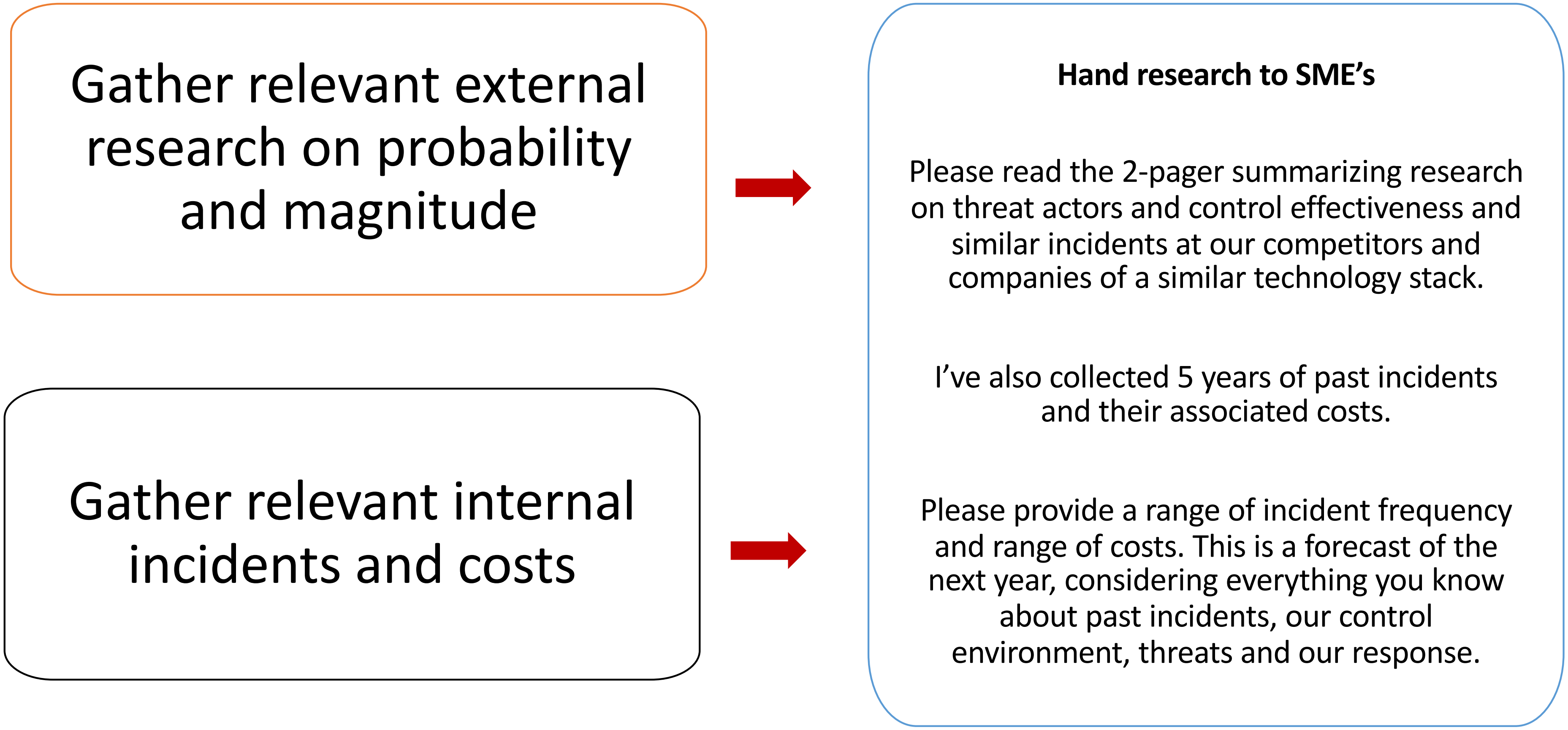
How to Use

- Interview SMEs in structured or unstructured settings to collect probability and magnitude estimates.

Pro Tips

- Excellent supplement to missing, incomplete or expensive data
- Use in analysis that require conjecture, hypothetical questions
- Subject to bias

Bringing it all together



Gather relevant external research on probability and magnitude

Gather relevant internal incidents and costs

Hand research to SME's

Please read the 2-pager summarizing research on threat actors and control effectiveness and similar incidents at our competitors and companies of a similar technology stack.

I've also collected 5 years of past incidents and their associated costs.

Please provide a range of incident frequency and range of costs. This is a forecast of the next year, considering everything you know about past incidents, our control environment, threats and our response.

Uses cases for FAIR

What kinds of analyses can I perform?

FAIR unlocks many more decisions over qualitative risk

Typical qualitative risk register

Risk Description	Likelihood	Impact	Risk
Weak admin password on SQL server	**High**	**High**	**High**
30 Windows servers out of patch compliance	**Medium**	**High**	**High**
Data breach	**Very High**	**Very High**	**Very High**
Server room lock is broken	**Low**	**High**	**Medium**

Decisions with FAIR analysis

Risk ranking / prioritization

- List of projects; which one to do first?

Insurance analysis

- What are the gaps in my cyber insurance coverage?
- Should I self-insure against this risk?

Add or remove a control

- Measure the baseline of risk
- Measure forecasted risk after changing a control

Project ROI

- How much does this project cost?
- If/when implemented, by how much will risk exposure change?

Emerging risk analysis

- Oddball, exotic risks that keeps someone up at night

M&A activity

- Changes in overall risk if a company acquires a company (third-party, data breach)

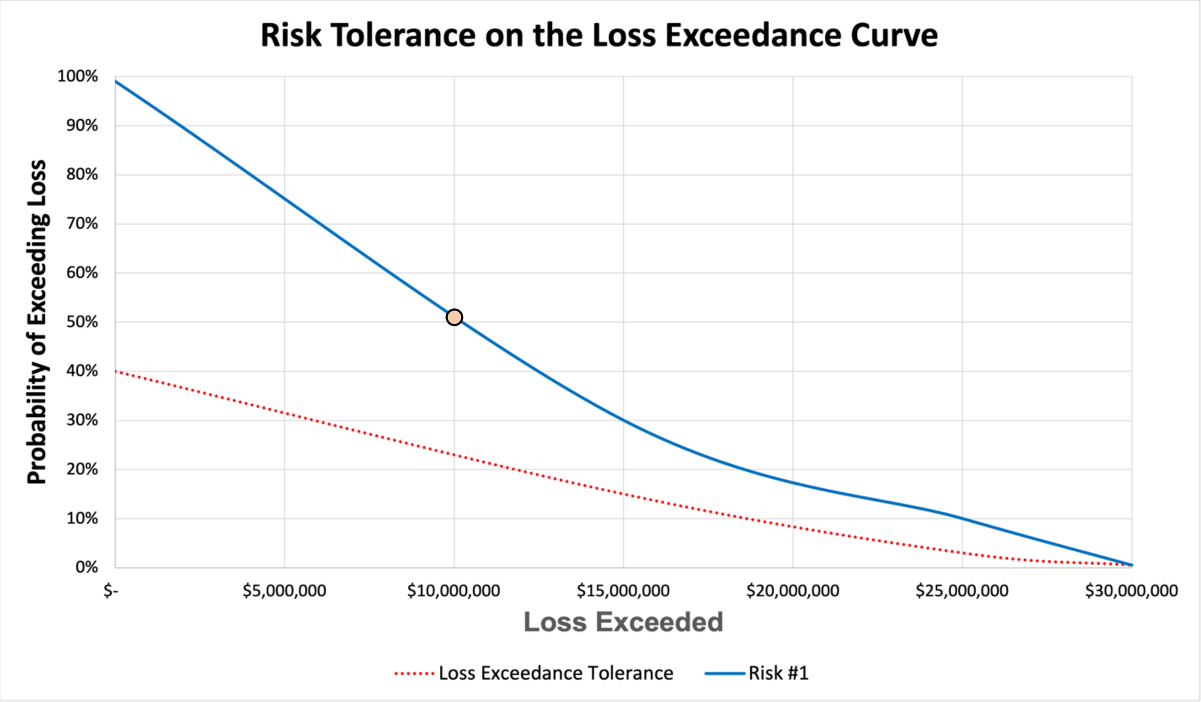
FAIR and Risk Tolerance

Managing Risk on the Loss Exceedance Curve

Uses a numerical range to articulate risk tolerance

Allows deeper conversations about risk

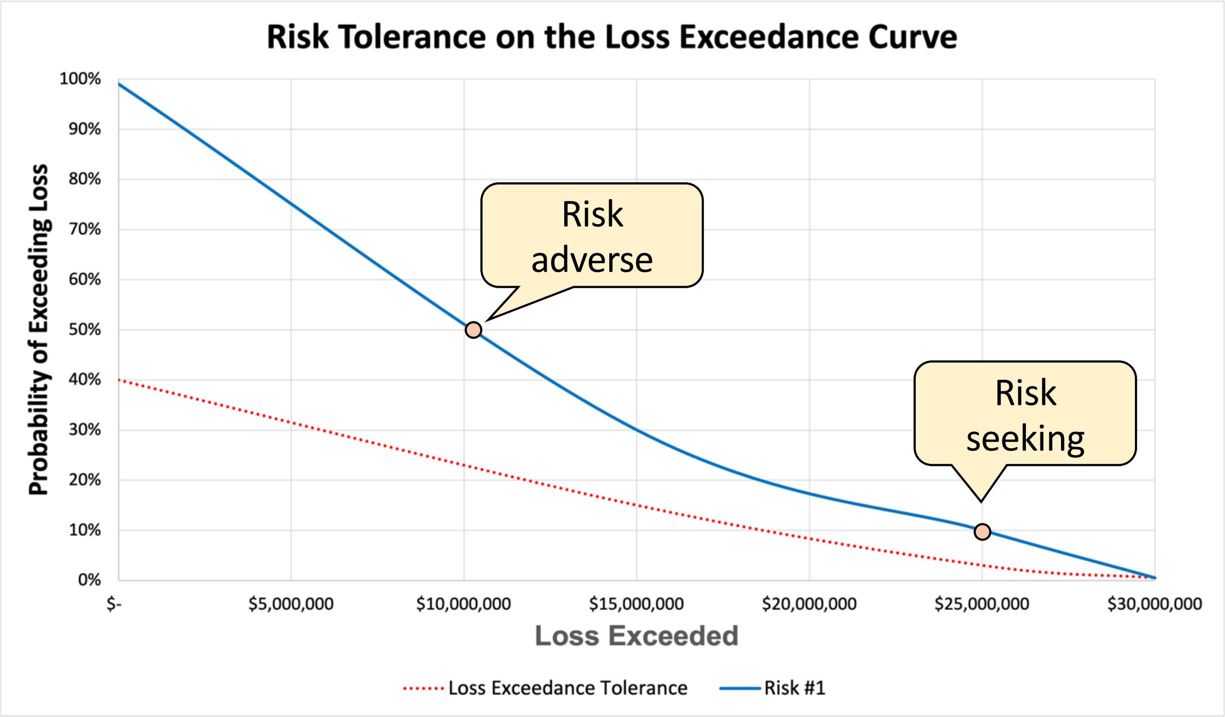
Management can decide where on the curve to manage to



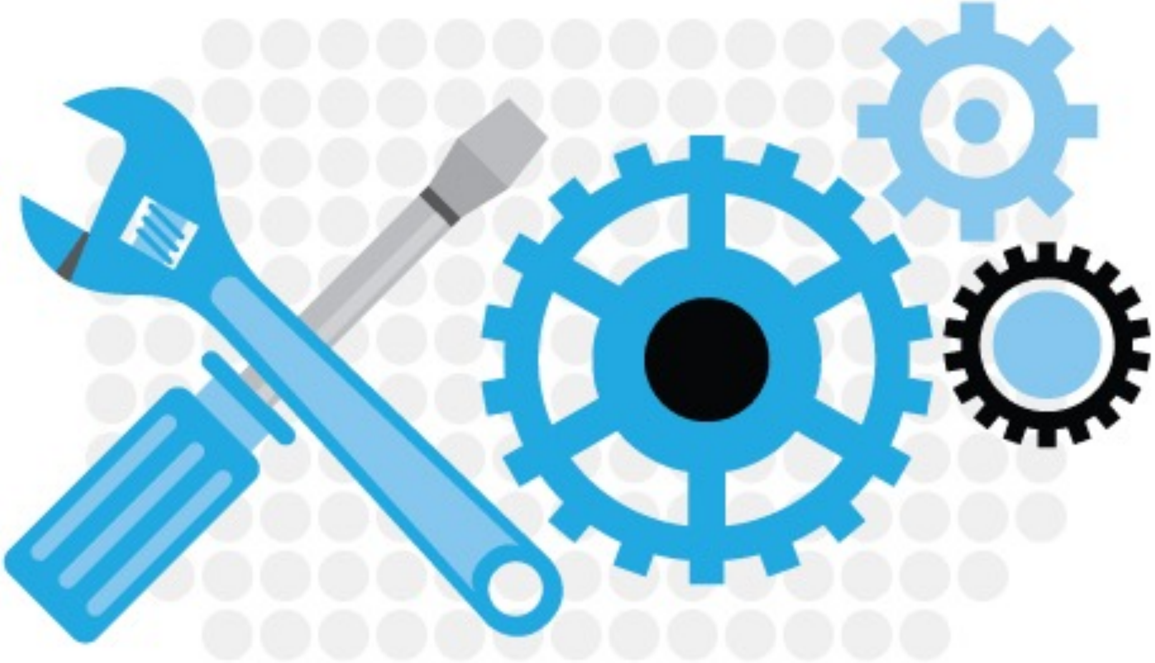
Managing Risk on the Loss Exceedance Curve

Risk adverse orgs: may want to manage a wide range of outcomes; can't won't tolerate losses ≥ $10m

Risk seeking orgs: hold into capital for other projects; focus on mitigating extreme losses



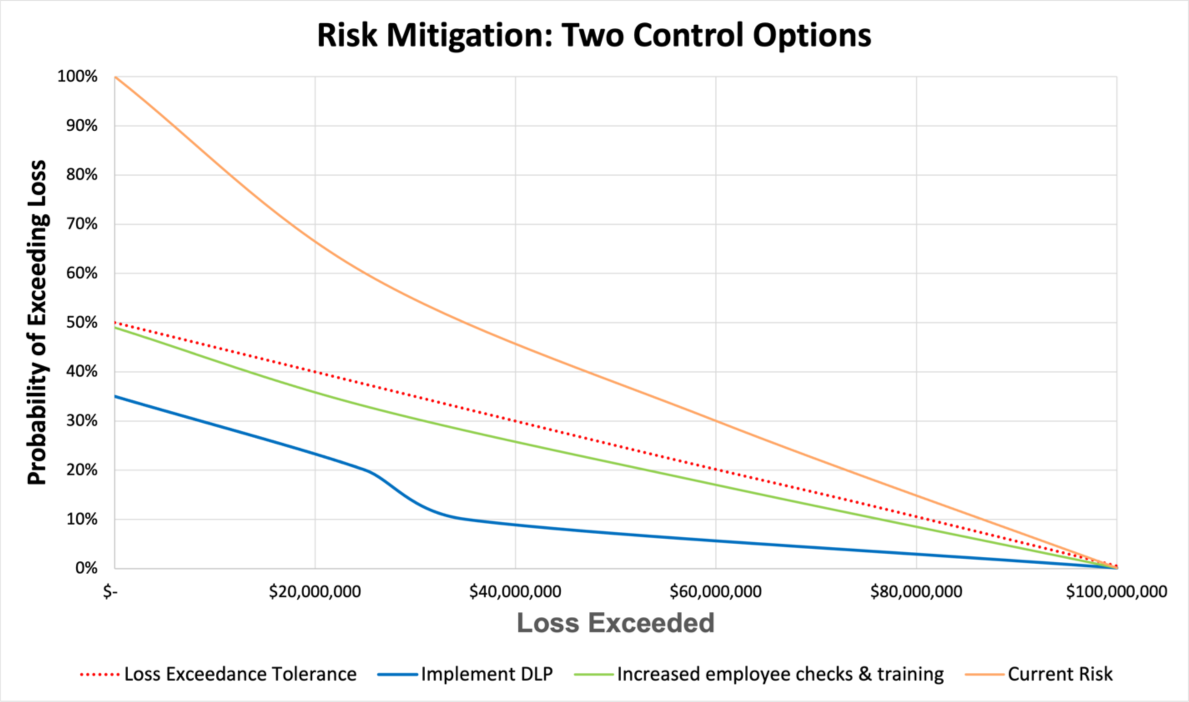
Using FAIR for optimized risk mitigation



Risk Mitigation

3 risk analyses

- Baseline of current risk
- Projected risk reduction with DLP
- Projected risk reduction with employee checks & training

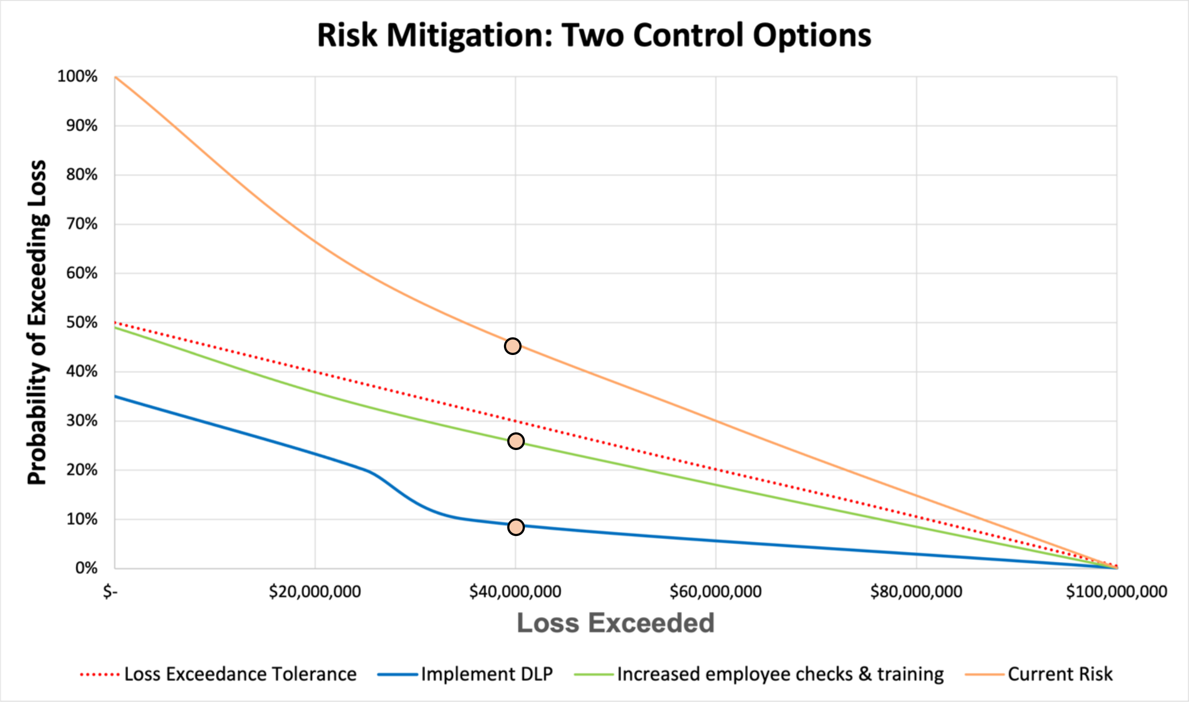


Risk Mitigation

“Where will our money go?”

Tired: “It will move a red to a green…”

Wired: $1m in investment buys down $45m in risk



FAIR for insurance analysis

Misconception that all loss forms are covered

Funny Math

$80m in data breach risk
- $50m cyber insurance

$30m residual risk

Risk Transfer Gap Analysis

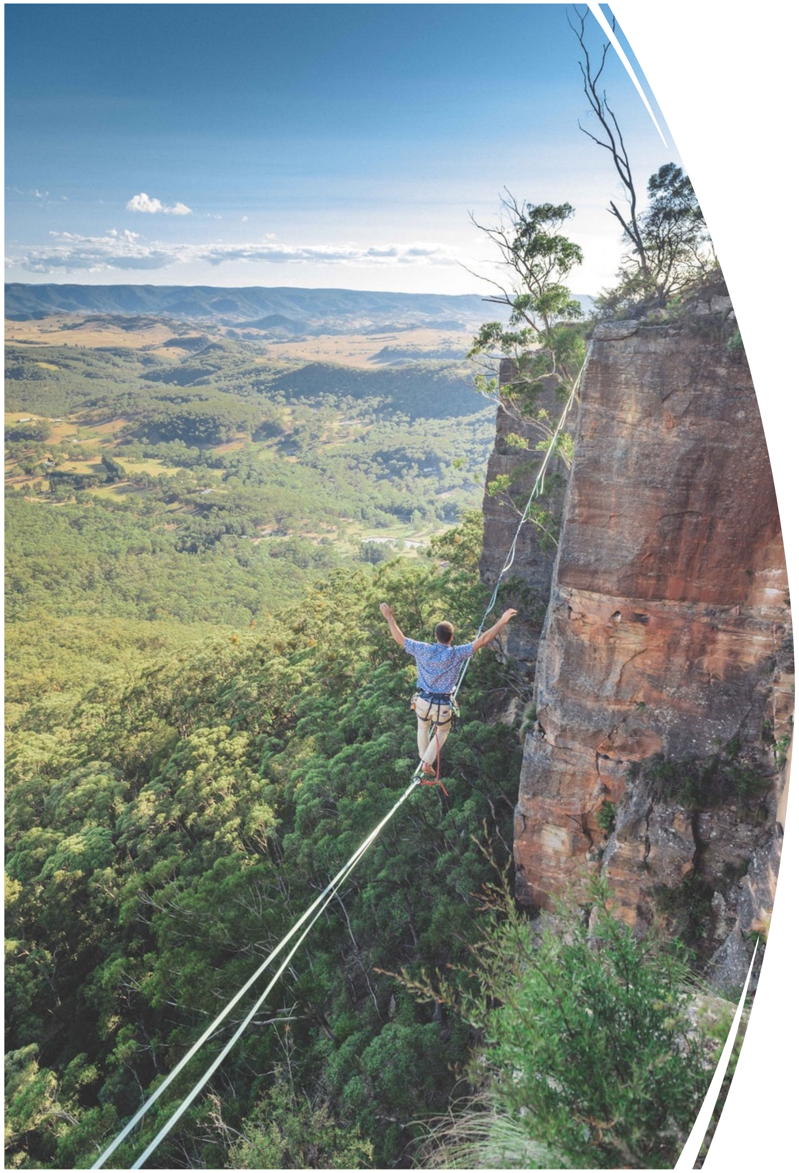
Open your insurance policy or master service agreement

Line by line, determine if a loss is covered

Source: OpenFAIR's 6 Forms of Loss : Risk Taxonomy (O-RT), Version 2.0

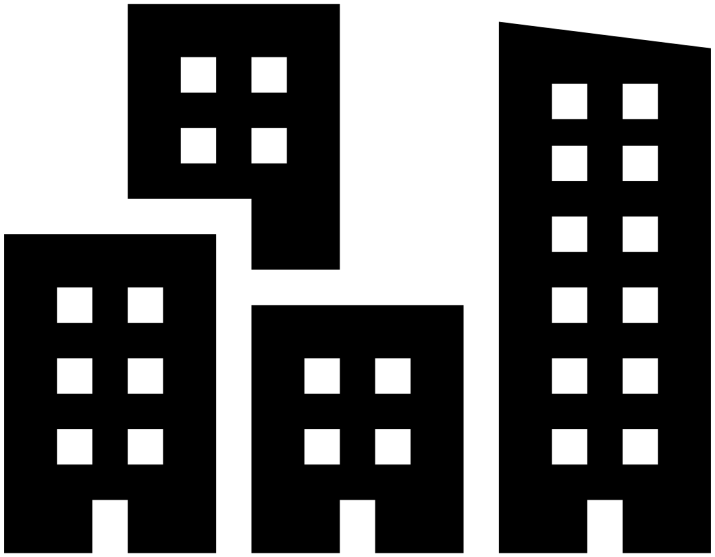
Example: SaaS outage | MSA covers $100k

Form of Loss	Loss	Current Risk	Coverage
Productivity	Lost revenue	$2m - $5m	
	Lost wages	N/A	
Response	Incident response team	$40k-100k	$20k
	Forensics	$250k-$350k	
	Management meetings	$100k-$200k	
	Customer notification	N/A	
	Credit monitoring	N/A	
Replacement	Repair/replace capital assets	N/A	$20k
Competitive Advantage	Loss of intellectual property	N/A	
	Loss of trade secrets	N/A	
	Loss of merger and acquisition information	N/A	
	Loss of market conditions information	N/A	
Fines and Judgment	Regulatory fines	N/A	
	Class action lawsuits	N/A	
	Bail	N/A	
Reputation	Reduced market share (lost customers)	N/A	
	Decreased projected sales growth	N/A	
	Reduced stock price	N/A	
	Increased cost of capital	N/A	



FAIR to... increase risk?

Increase risk: example



The organization has a security control implemented to reduce security incidents

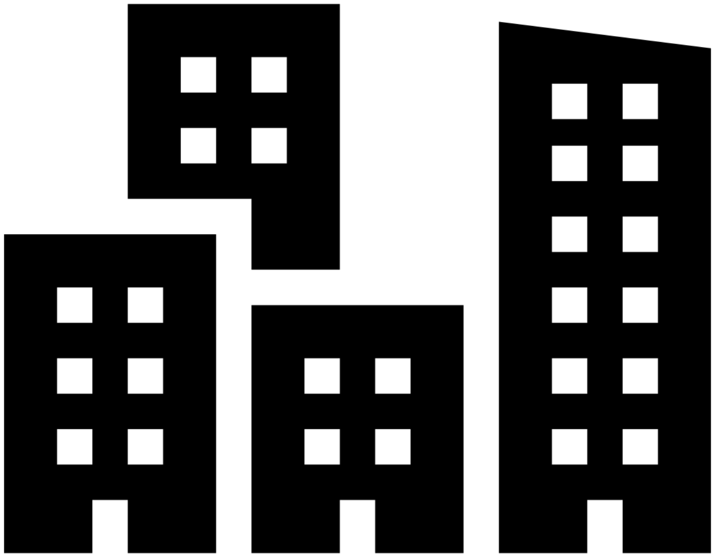
Causes a good deal of user friction

Some productivity loss due to the control

Is not free: annual cost of $15m (SaaS subscription, maintenance, internal staffing)

Risk team: how does removing the control affect our risk exposure?

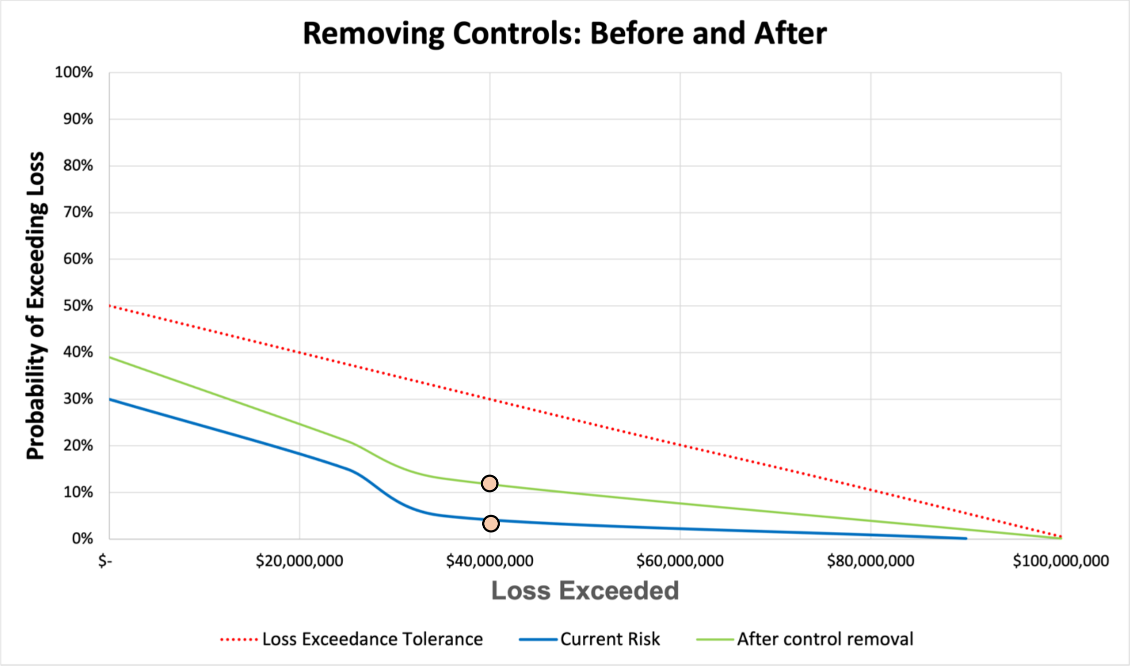
Increase risk: example



Perform 2 analyses

- Current risk
- Forecast risk if controls are removed

Increase risk: example



Conclusions

Current risk is below our tolerance, so we have room to maneuver

The probability of losses exceeding $40m goes from 5% to 12%

This change will net $15m in savings annually

If we need more data to make a decision, we can price out productivity gains from the change

Final Thoughts

- Consider FAIR at least for your huge existential risks – big strategic unlock
- Subjective data (human judgement) isn't bad
- FAIR allows for different kinds of decisions in cyber security
- Use the data you have