How to move to

Quantitative Risk Analysis

for

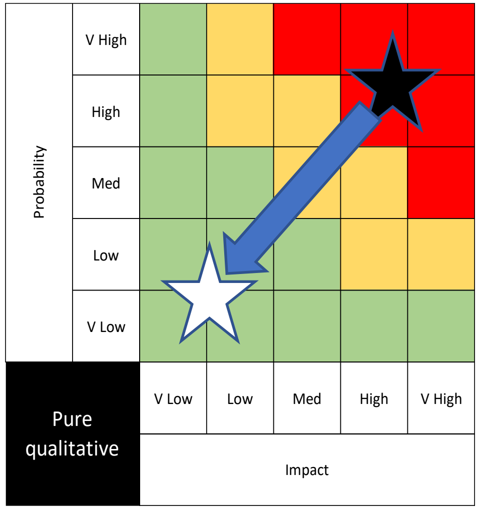
Enterprise Risk Management

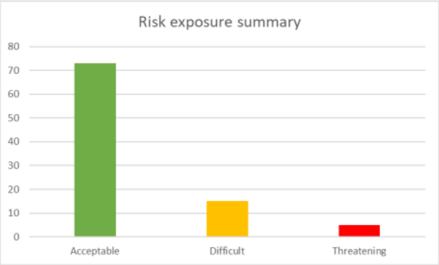
www.vosesoftware.com

GRC/ERM/IRM v risk management

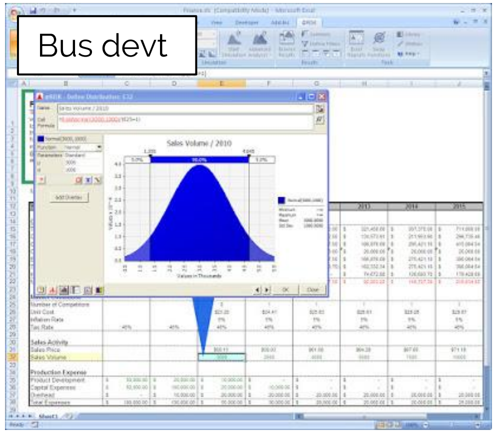
vose
Putting numbers around risk

Risk Managers with GRC system

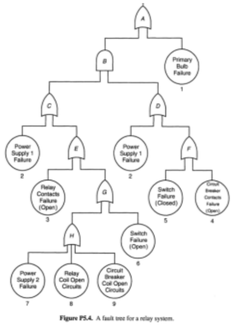


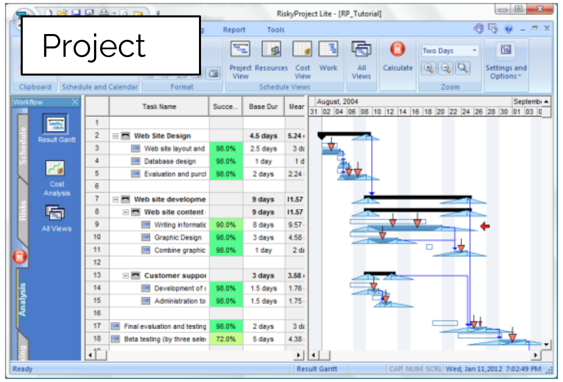


Everyone else



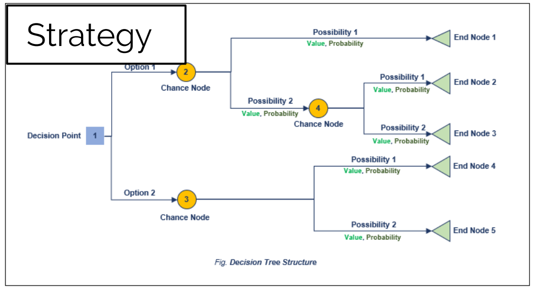
Engineers

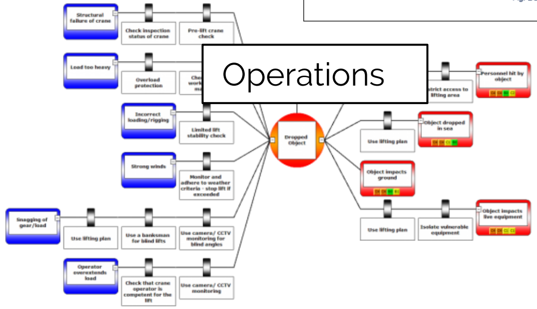


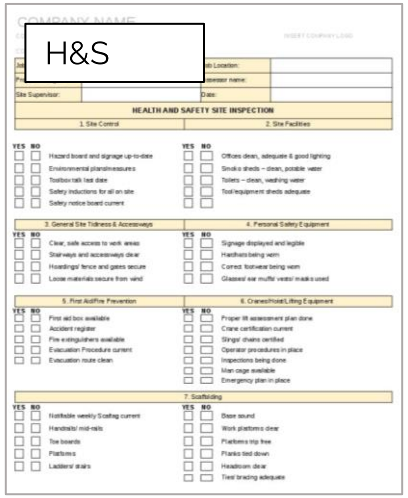


Treasury

$$
\begin{aligned}
C(S,t) &= N(d_1)S - N(d_2)Ke^{-r(T-t)}\\
d_1 &= \frac{1}{\sigma\sqrt{T-t}}\left[\ln\left(\frac{S}{K}\right)+\left(r+\frac{\sigma^2}{2}\right)(T-t)\right]\\
d_2 &= \frac{1}{\sigma\sqrt{T-t}}\left[\ln\left(\frac{S}{K}\right)+\left(r-\frac{\sigma^2}{2}\right)(T-t)\right]\\
&= d_1-\sigma\sqrt{T-t}
\end{aligned}
$$




Operations
Structural failure of crane
Check inspection status of crane
Pre-lift crane check
Load too heavy
Overload protection
Incorrect loading/rigging
Limited lift stability check
Strong winds
Monitor and adhere to weather criteria - stop lift if exceeded
Snagging of gear/load
Use lifting plan
Use a banksman for blind lifts
Use camera/ CCTV monitoring for blind angles
Operator overextends load
Check that crane operator is competent for the lift
Use camera/ CCTV monitoring
Dropped Object
Personnel hit by object
Restrict access to lifting area
Object dropped in sea
Use lifting plan
Object impacts ground
Object impacts live equipment
Use lifting plan
Isolate vulnerable equipment



COMPANY NAME

INSERT COMPANY LOGO

Job		Job Location:	
Pr		Inspector name:	
Site Supervisor:		Date:	

HEALTH AND SAFETY SITE INSPECTION

1. Site Control

YES	NO	
□	□	Hazard board and signage up-to-date
□	□	Environmental plans/measures
□	□	Toolbox talk last date
□	□	Safety inductions for all on site
□	□	Safety notice board current

2. Site Facilities

YES	NO	
□	□	Offices clean, adequate & good lighting
□	□	Smoko sheds – clean, potable water
□	□	Toilets – clean, washing water
□	□	Tool/equipment sheds adequate
□	□	

3. General Site Tidiness & Accessways

YES	NO	
□	□	Clear, safe access to work areas
□	□	Stairways and accessways clear
□	□	Hoardings/ fence and gates secure
□	□	Loose materials secure from wind

4. Personal Safety Equipment

YES	NO	
□	□	Signage displayed and legible
□	□	Hardhats being worn
□	□	Correct footwear being worn
□	□	Glasses/ ear muffs/ vests/ masks used

5. First Aid/Fire Prevention

YES	NO	
□	□	First aid box available
□	□	Accident register
□	□	Fire extinguishers available
□	□	Evacuation Procedure current
□	□	Evacuation route clean

6. Cranes/Hoist/Lifting Equipment

YES	NO	
□	□	Proper lift assessment plan done
□	□	Crane certification current
□	□	Slings/ chains certified
□	□	Operator procedures in place
□	□	Inspections being done
□	□	Man cage available
□	□	Emergency plan in place

7. Scaffolding

YES	NO	
□	□	Notifiable weekly Scaffag current
□	□	Handrails/ mid-rails
□	□	Toe boards
□	□	Platforms
□	□	Ladders/ stairs

YES	NO	
□	□	Base sound
□	□	Work platforms clear
□	□	Platforms trip free
□	□	Planks tied down
□	□	Headroom clear
□	□	Ties/ bracing adequate

GRC v ERM/IRM

Governance, Risk and Compliance v Enterprise/Integrated Risk Management

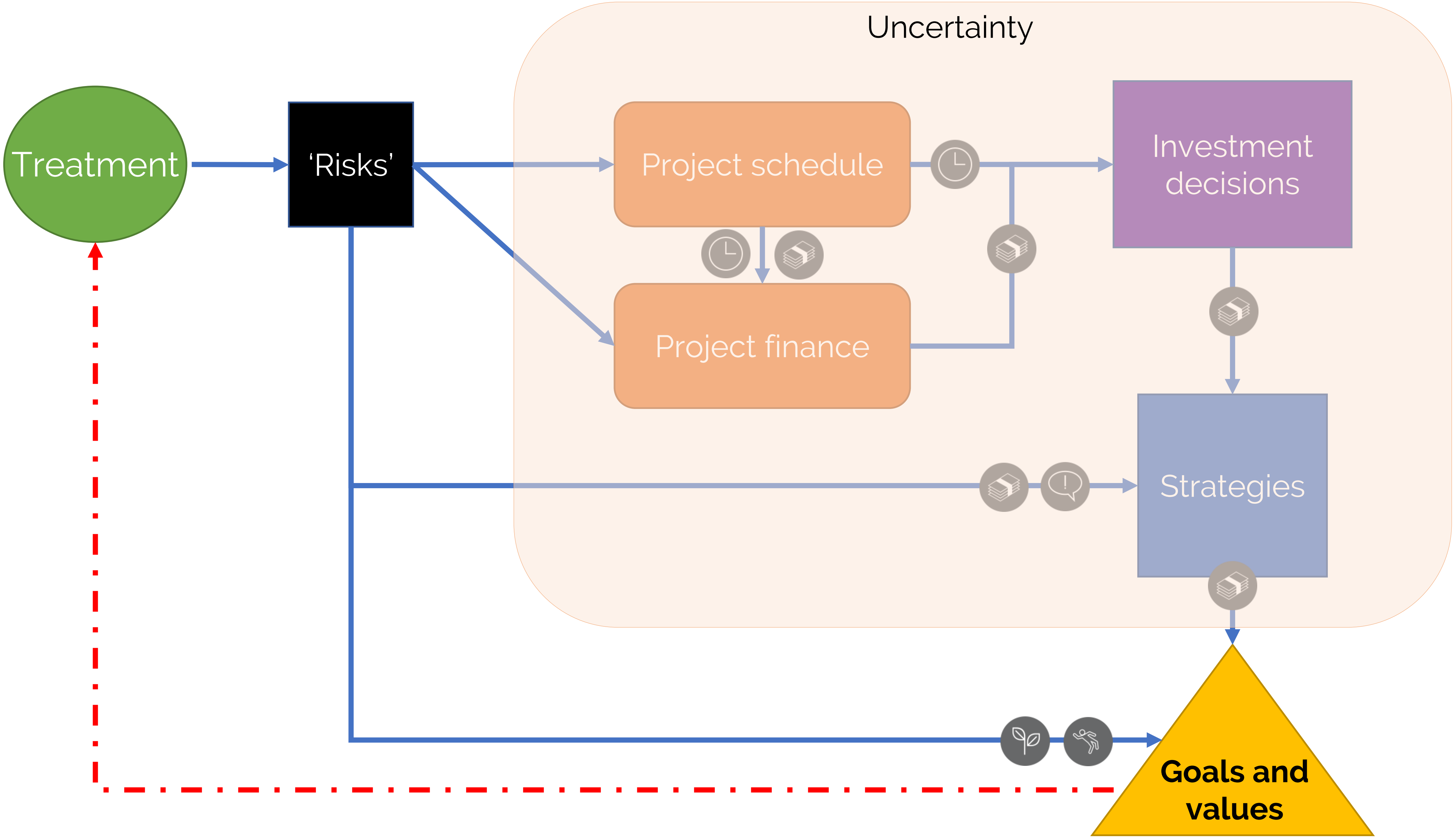
Risk Managers with GRC system

“Our organisation is not yet mature enough to go quantitative”

Everyone else with their methods

“Management doesn’t listen to us”

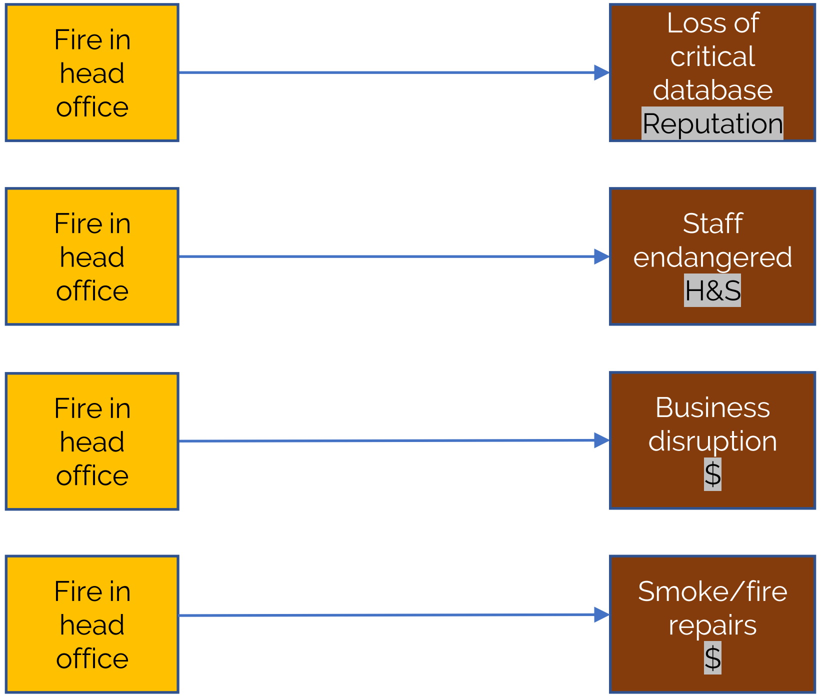
The end goal – build and preserve



A richer way to describe risks

www.vosesoftware.com

Typical risk register approach



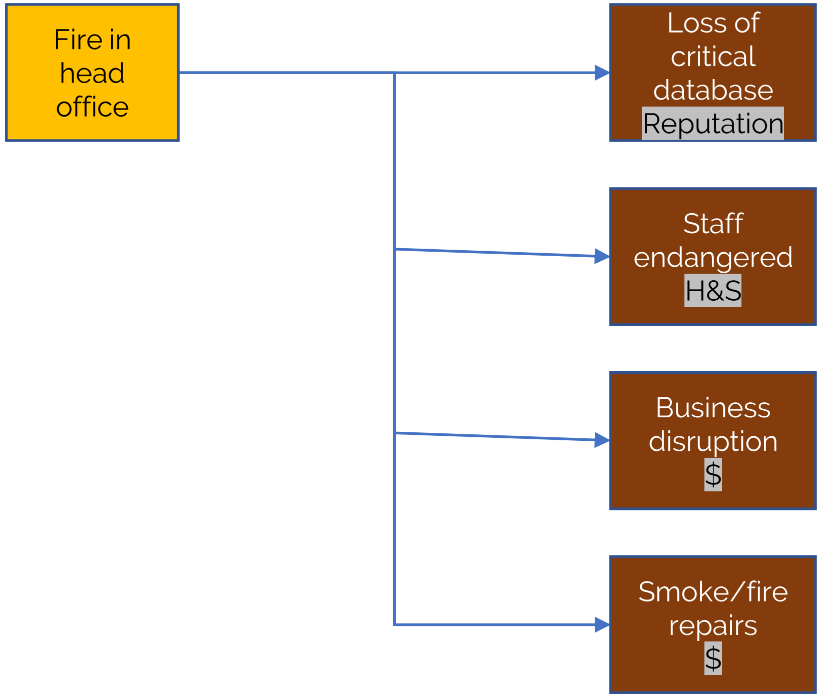
Fire in head office → Loss of critical database Reputation

Fire in head office → Staff endangered H&S

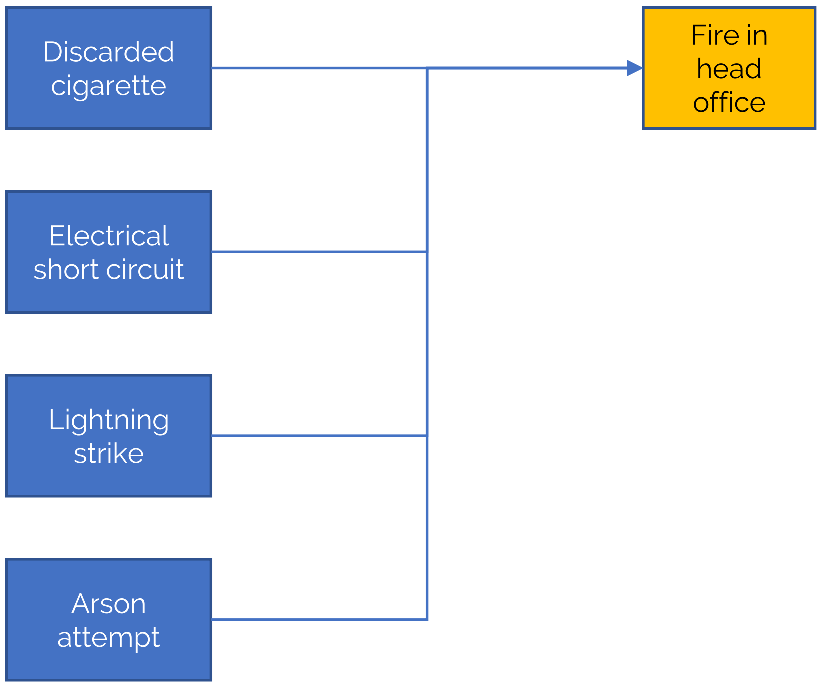
Fire in head office → Business disruption $

Fire in head office → Smoke/fire repairs $

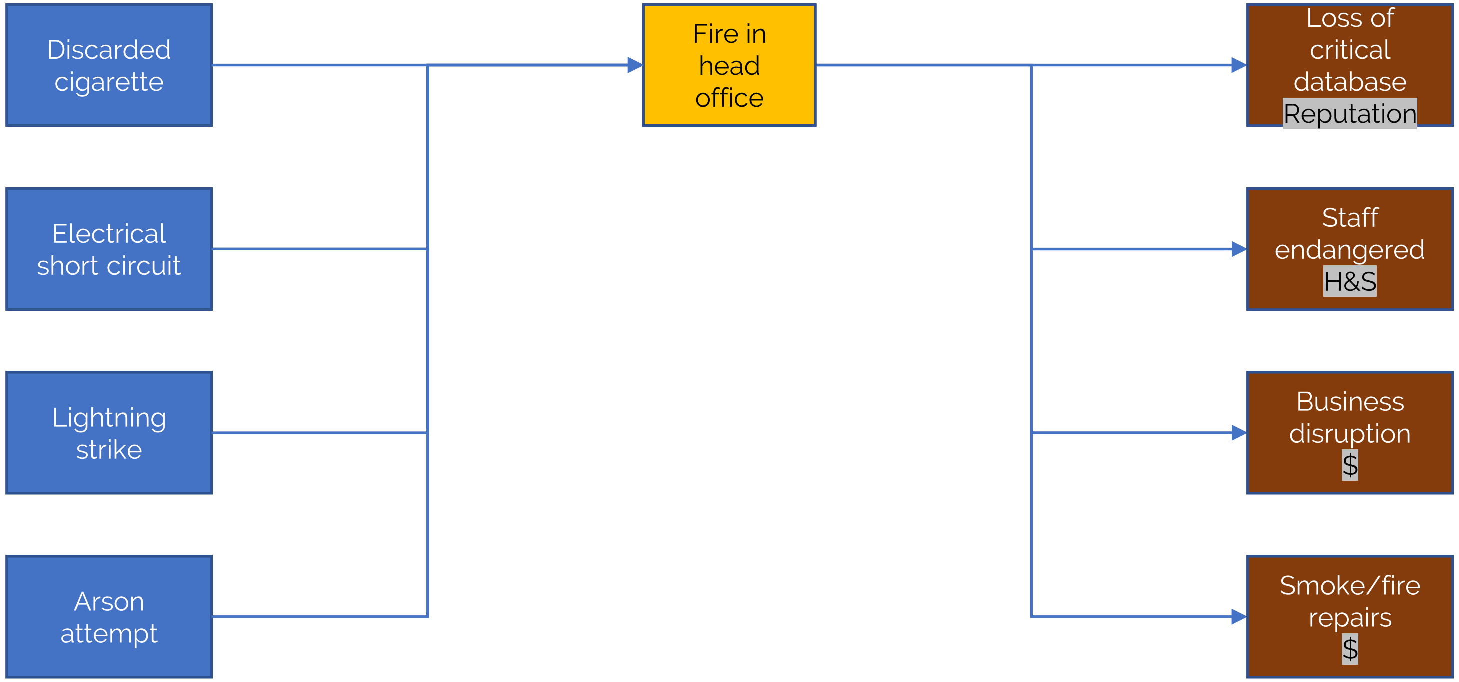
Which is just …



And why might it happen?



The problem we have to manage



Discarded cigarette

Electrical short circuit

Lightning strike

Arson attempt

Fire in head office

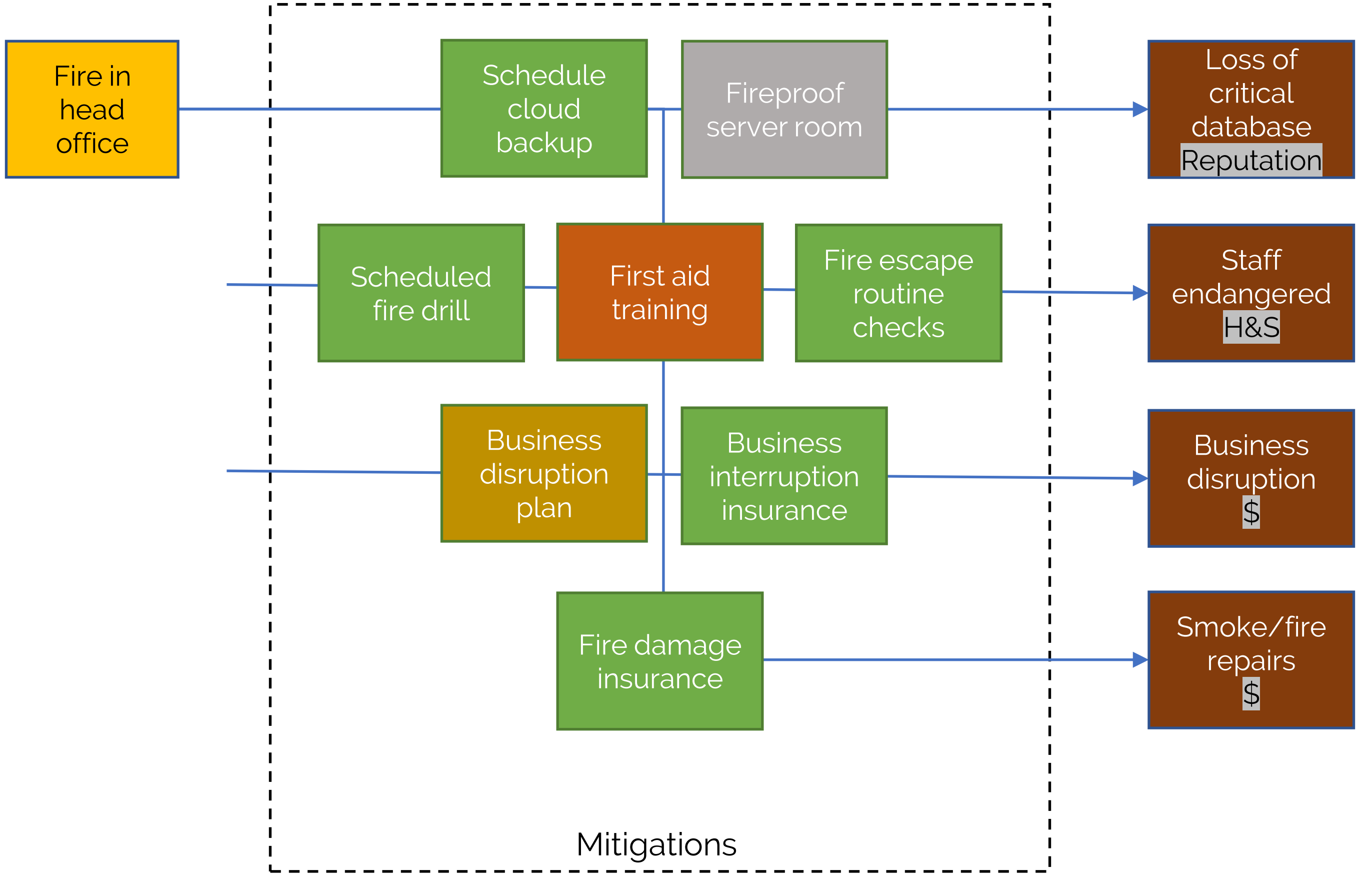
Loss of critical database
Reputation

Staff endangered
H&S

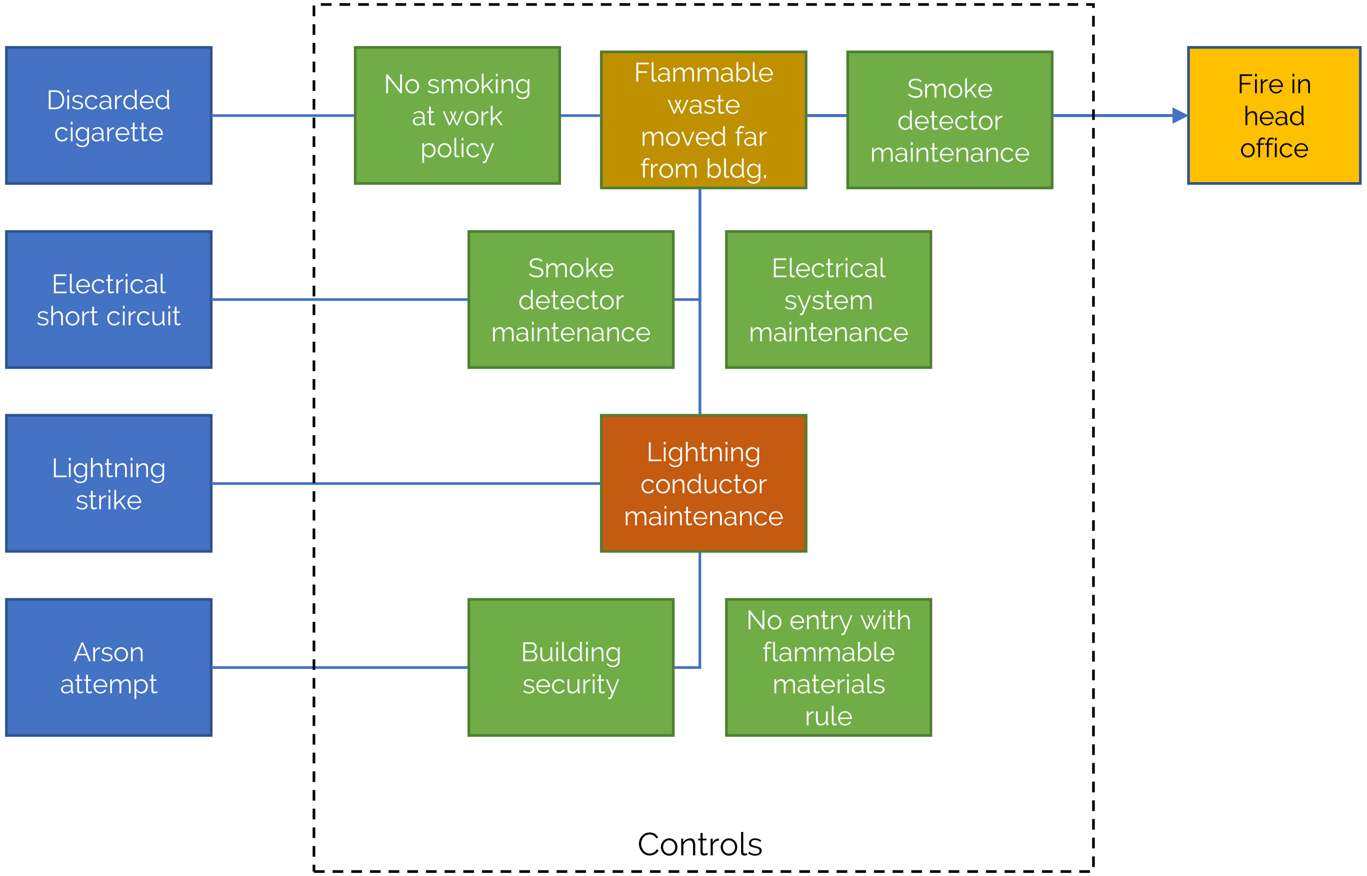
Business disruption
$

Smoke/fire repairs
$

How can we manage the impact?

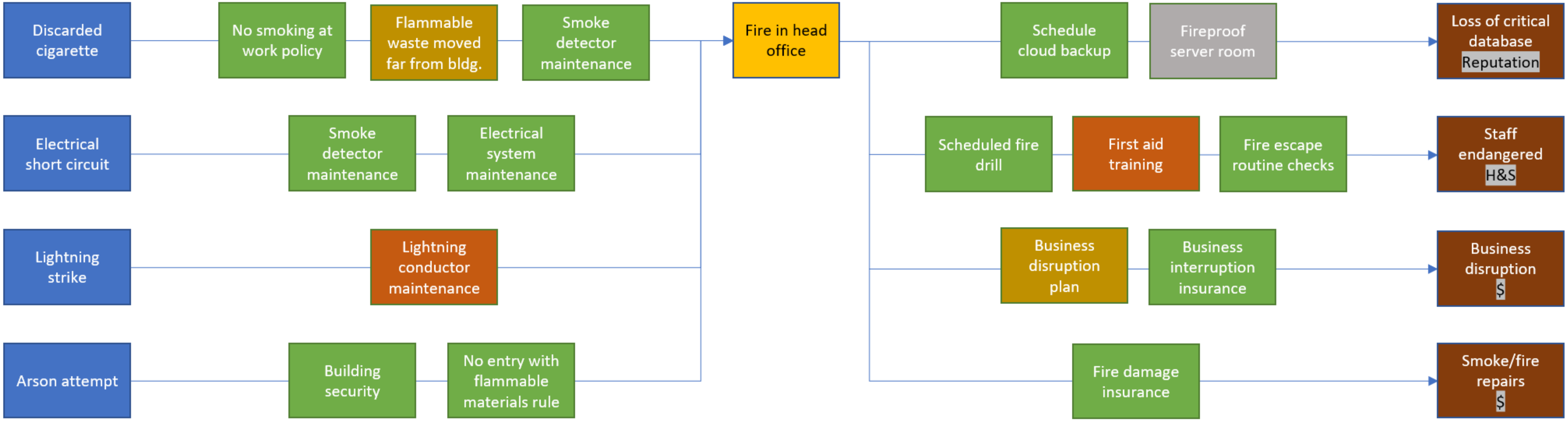


How can we stop it happening?

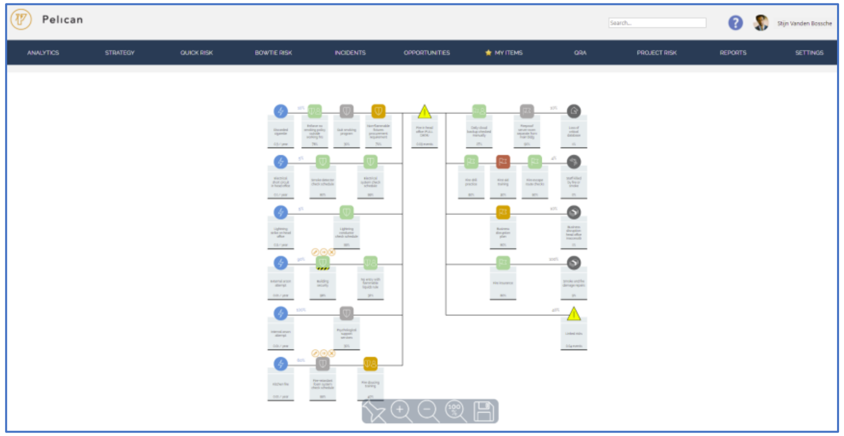

Discarded cigarette
Electrical short circuit
Lightning strike
Arson attempt
No smoking at work policy
Flammable waste moved far from bldg.
Smoke detector maintenance
Smoke detector maintenance
Electrical system maintenance
Lightning conductor maintenance
Building security
No entry with flammable materials rule
Controls
Fire in head office

The overall strategy

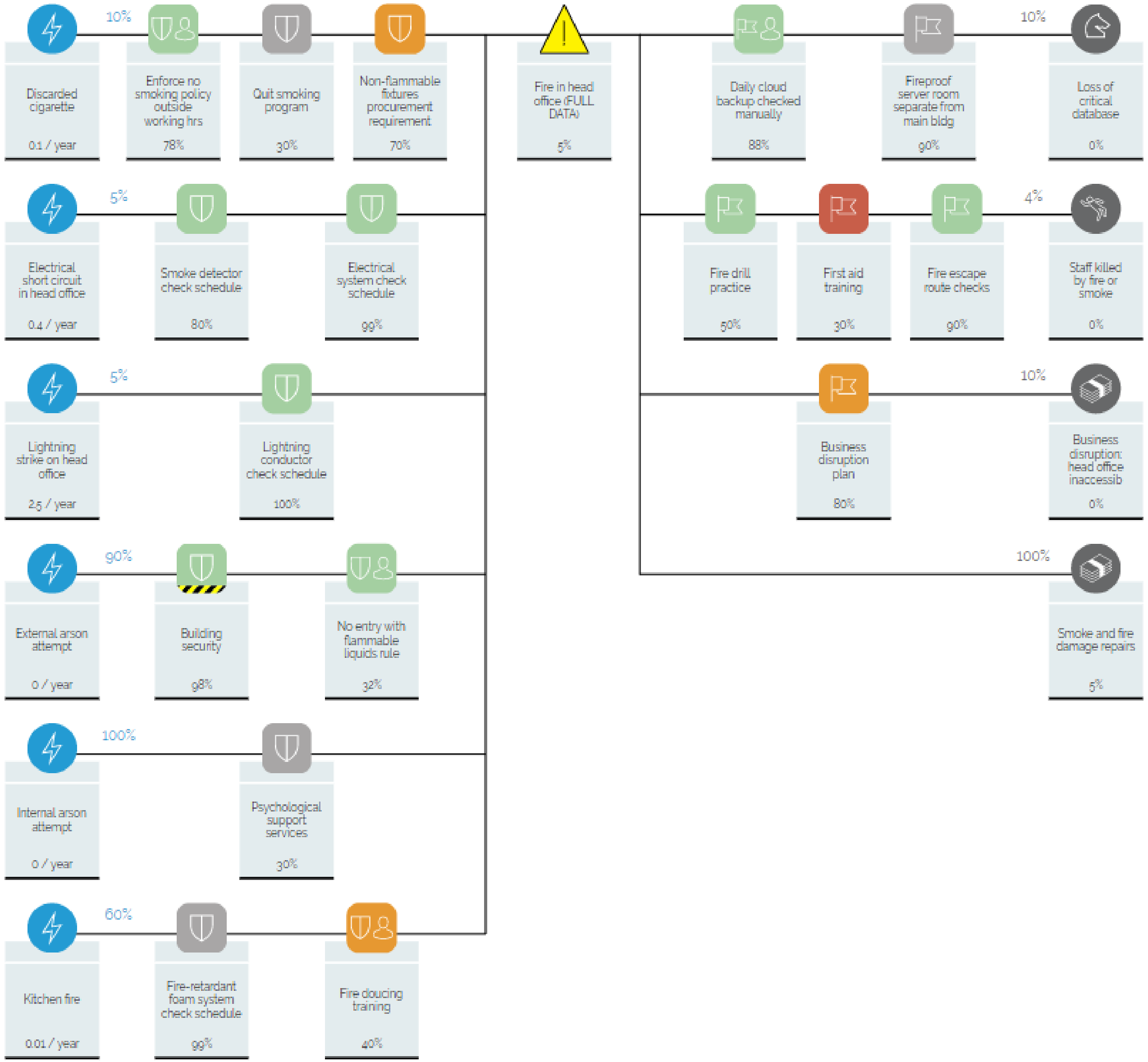
vose
Putting numbers around risk



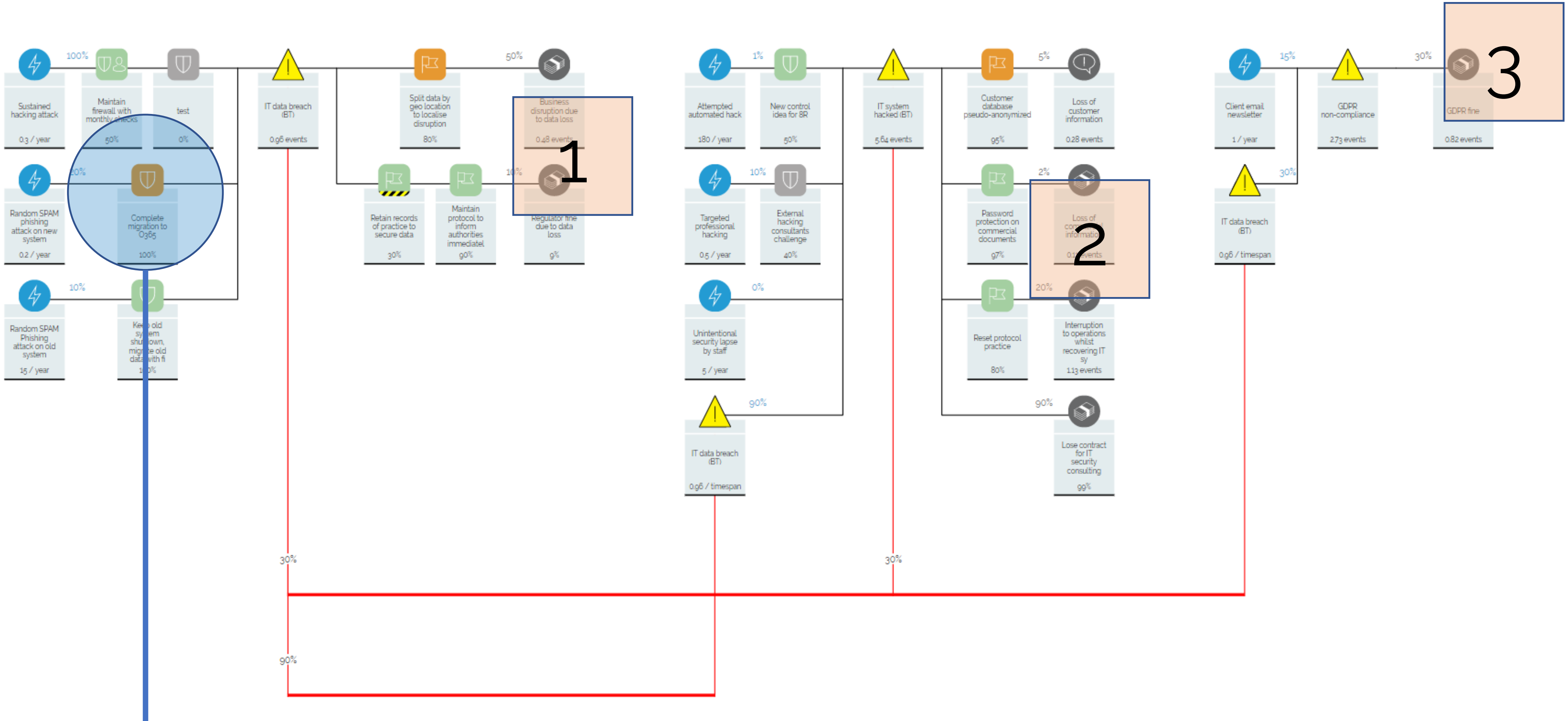
Putting numbers in



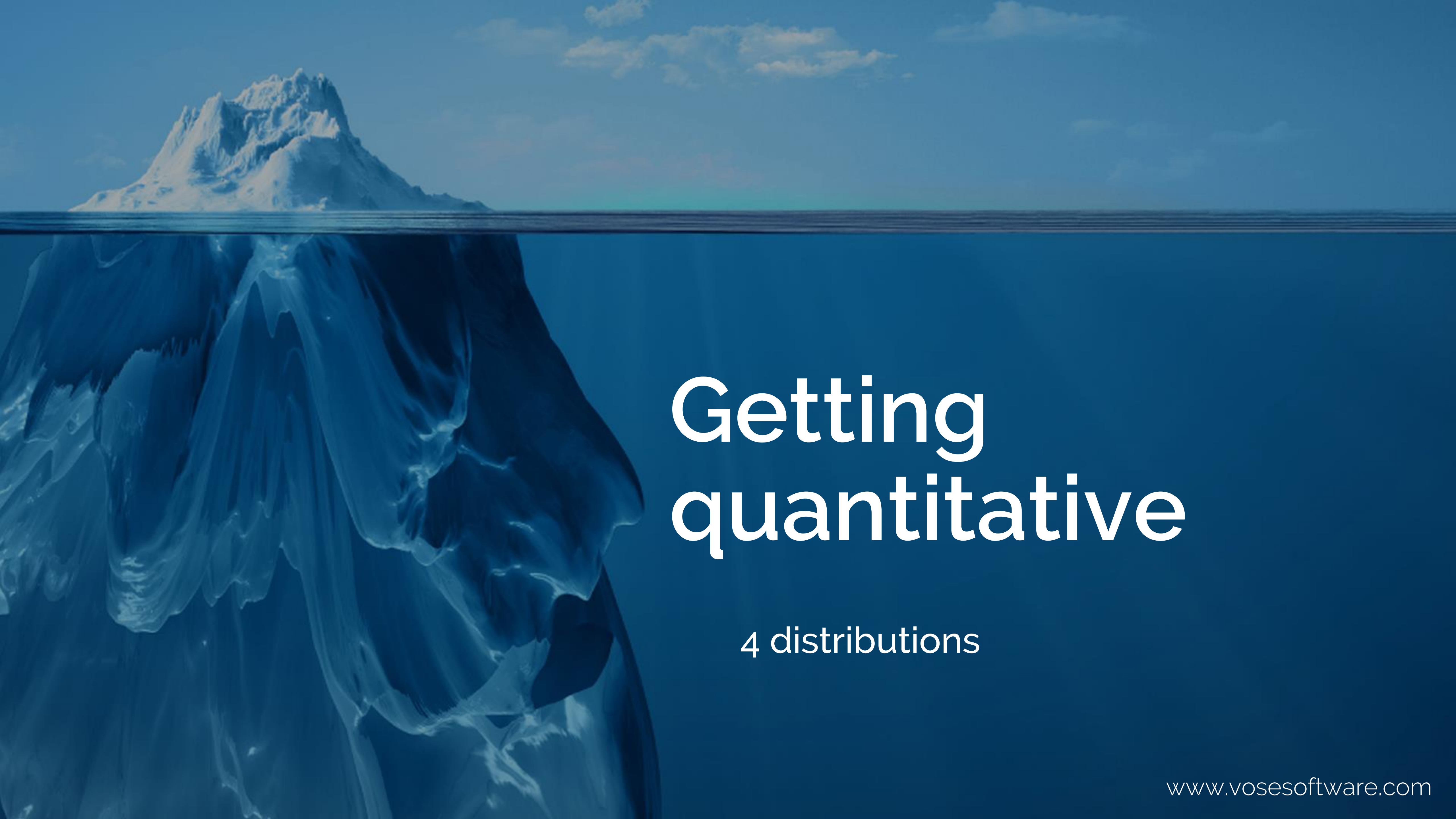
Pelican ERM system
www.vosesoftware.com


10%
Discarded cigarette
0.1 / year
Enforce no smoking policy outside working hrs
78%
Quit smoking program
30%
Non-flammable fixtures procurement requirement
70%
5%
Electrical short circuit in head office
0.4 / year
Smoke detector check schedule
80%
Electrical system check schedule
99%
5%
Lightning strike on head office
2.5 / year
Lightning conductor check schedule
100%
90%
External arson attempt
0 / year
Building security
98%
No entry with flammable liquids rule
32%
100%
Internal arson attempt
0 / year
Psychological support services
30%
60%
Kitchen fire
0.01 / year
Fire-retardant foam system check schedule
99%
Fire doucing training
40%
Fire in head office (FULL DATA)
5%
Daily cloud backup checked manually
88%
Fireproof server room separate from main bldg
90%
10%
Loss of critical database
0%
Fire drill practice
50%
First aid training
30%
Fire escape route checks
90%
4%
Staff killed by fire or smoke
0%
Business disruption plan
80%
10%
Business disruption: head office inaccessib
0%
100%
Smoke and fire damage repairs
5%

Risks are often interconnected


Sustained hacking attack
0.3 / year
100%
Maintain firewall with monthly checks
50%
test
0%
IT data breach (BT)
0.96 events
Split data by geo location to localise disruption
80%
50%
Business disruption due to data loss
0.48 events
1
Random SPAM phishing attack on new system
0.2 / year
20%
Complete migration to O365
100%
Retain records of practice to secure data
30%
Maintain protocol to inform authorities immediatel
90%
10%
Regulator fine due to data loss
9%
Random SPAM Phishing attack on old system
15 / year
10%
Keep old system shutdown, migrate old data with fi
100%
Attempted automated hack
180 / year
1%
New control idea for 8R
50%
IT system hacked (BT)
5.64 events
Customer database pseudo-anonymized
95%
5%
Loss of customer information
0.28 events
Targeted professional hacking
0.5 / year
10%
External hacking consultants challenge
40%
Password protection on commercial documents
97%
2%
Loss of commercial information
0.1 events
2
Unintentional security lapse by staff
5 / year
0%
Reset protocol practice
80%
20%
Interruption to operations whilst recovering IT sy
1.13 events
IT data breach (BT)
0.96 / timespan
90%
90%
Lose contract for IT security consulting
99%
Client email newsletter
1 / year
15%
GDPR non-compliance
2.73 events
30%
GDPR fine
0.82 events
3
IT data breach (BT)
0.96 / timespan
30%
30%
30%
90%

This control has not been checked in time. That jeopardises the management of three risks

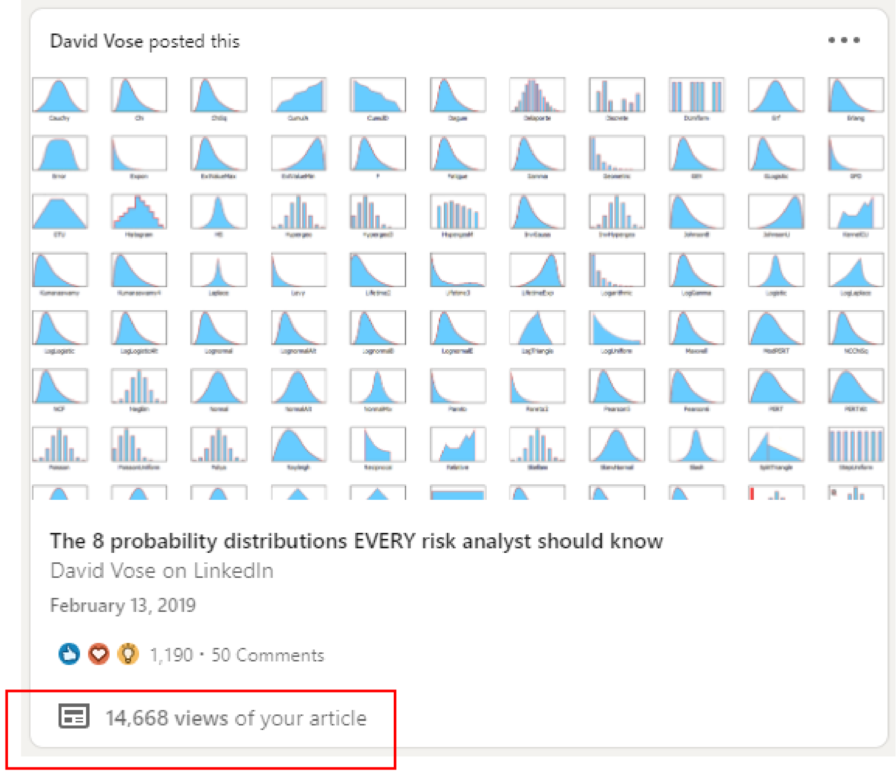


Getting quantitative

4 distributions

If you’re on LinkedIn …

More about the distributions



David Vose posted this

The 8 probability distributions EVERY risk analyst should know

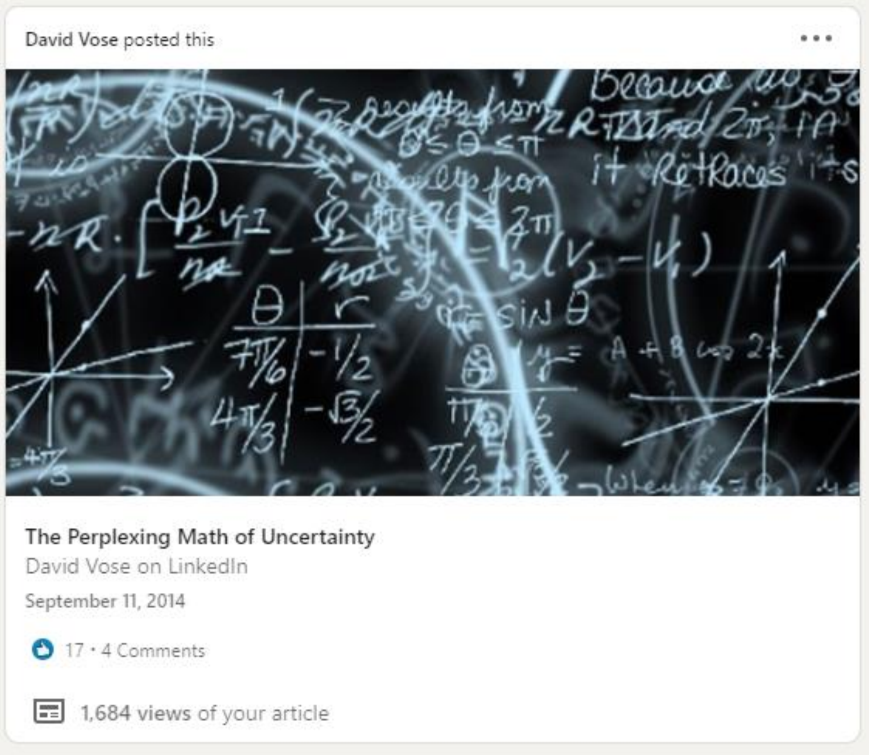
David Vose on LinkedIn

February 13, 2019

1,190 · 50 Comments

14,668 views of your article

Avoid common modelling mistakes



David Vose posted this

The Perplexing Math of Uncertainty

David Vose on LinkedIn

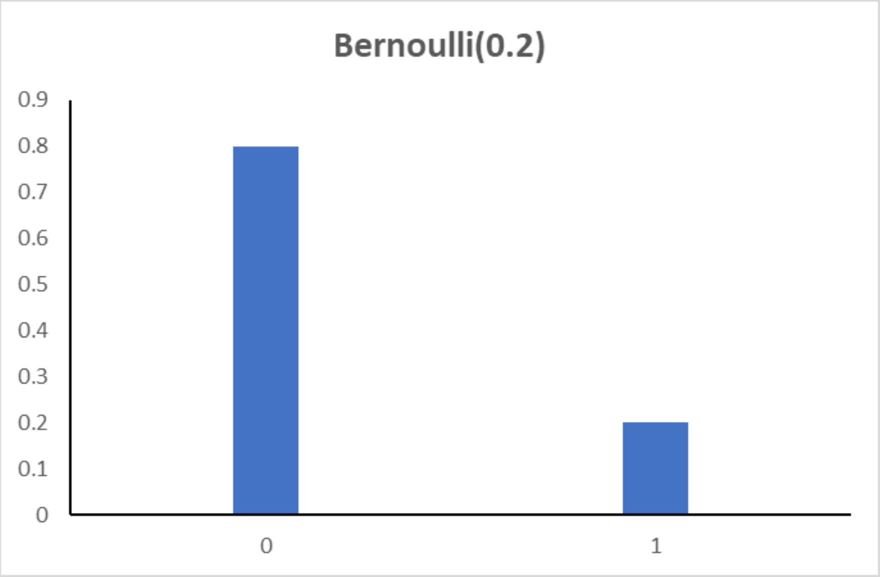
September 11, 2014

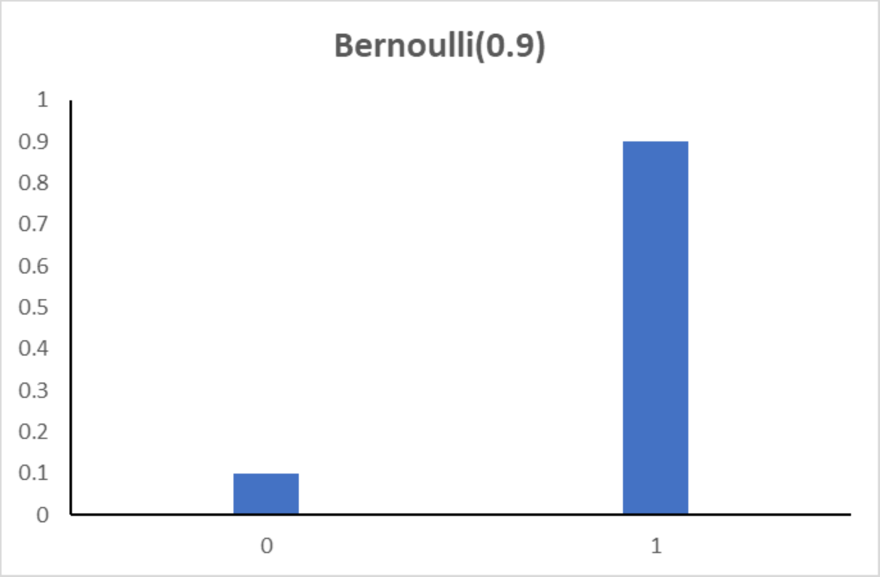
17 · 4 Comments

1,684 views of your article

Bernoulli distribution - essential

Risks that can only occur once





1 = it happened

0 = it didn't happen

Parameter = P(it happened)

Bernoulli(0.2)*10

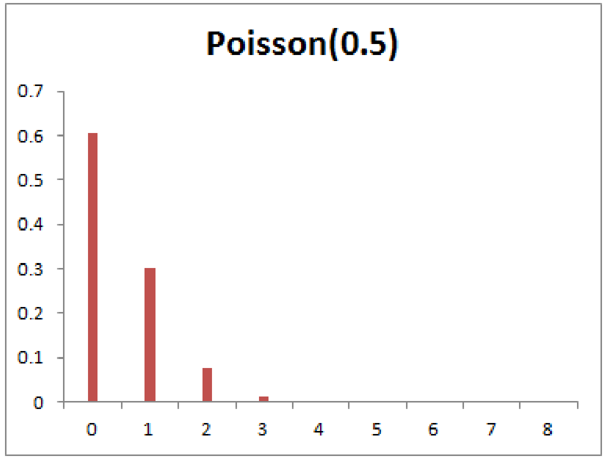
IF(x>2, Bernoulli(0.8), 0)

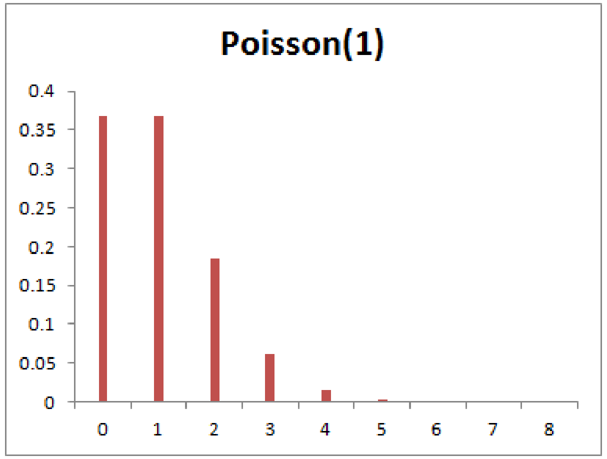
Bernoulli(IF(x=1,p,q))

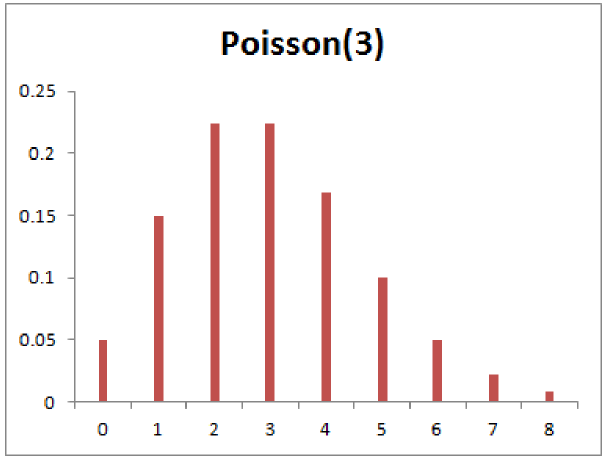
Jacob Bernoulli

Poisson distribution - essential

Risks that can occur multiple times


Poisson(0.5)


Poisson(1)


Poisson(3)

Parameter λ = average # events in period

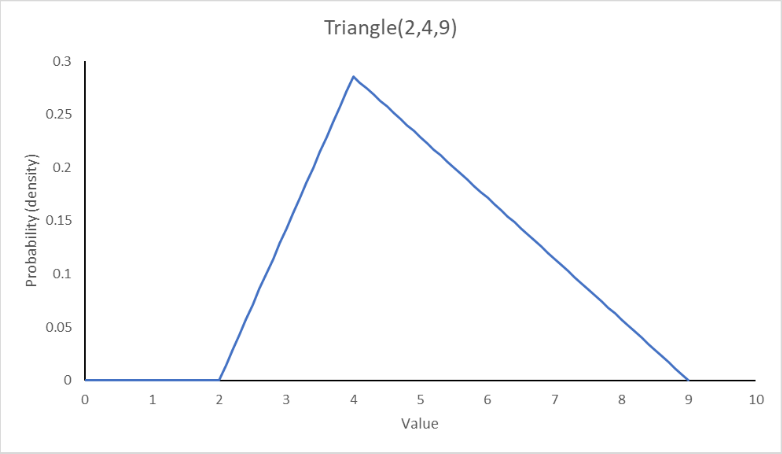
Simple to use:

- μ events per year, t years: $\lambda = \mu t$
- μ events per year, probability p event -> consequence: $\lambda = \mu p$
- P(0) = EXP(- λ), P(>0) = 1-EXP(- λ)

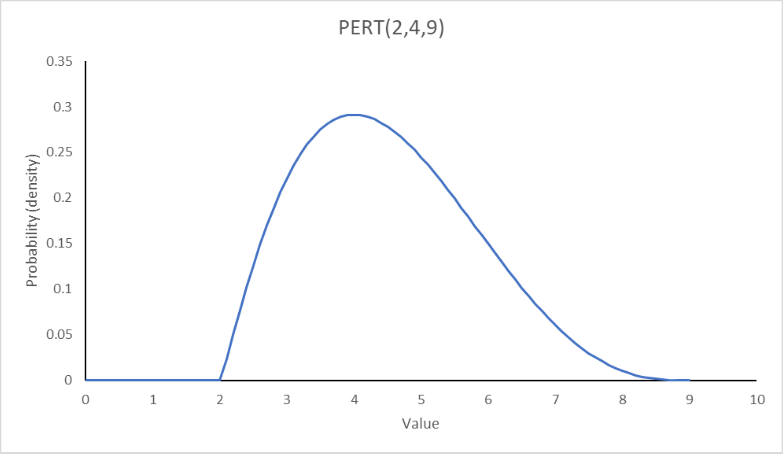
Siméon Poisson

Three-point estimates - essential

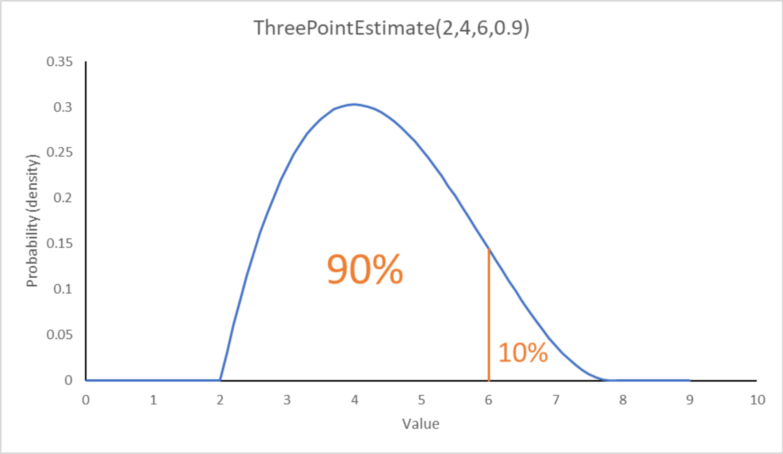
How large an impact might be



Crude



Bit better



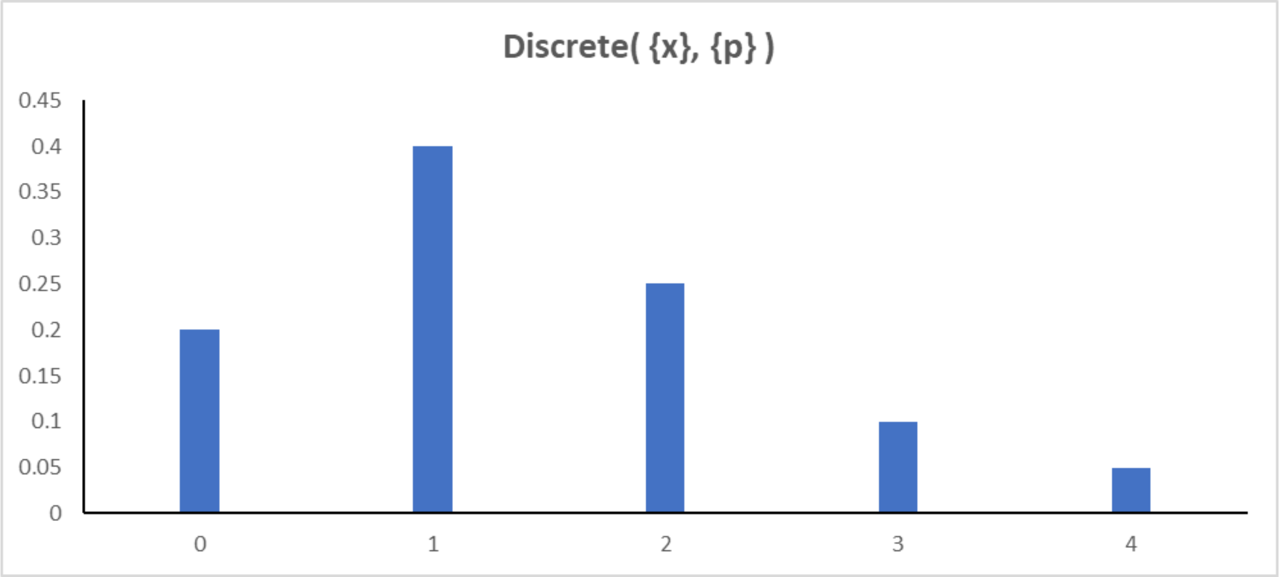
Best

Better than a single value!

What are the:

- Minimum possible value - *usually well known*
- The most likely value - *also usually well known*
- ‘Maximum’ value – *harder to say, P90 is more intuitive*

Discrete distribution - useful

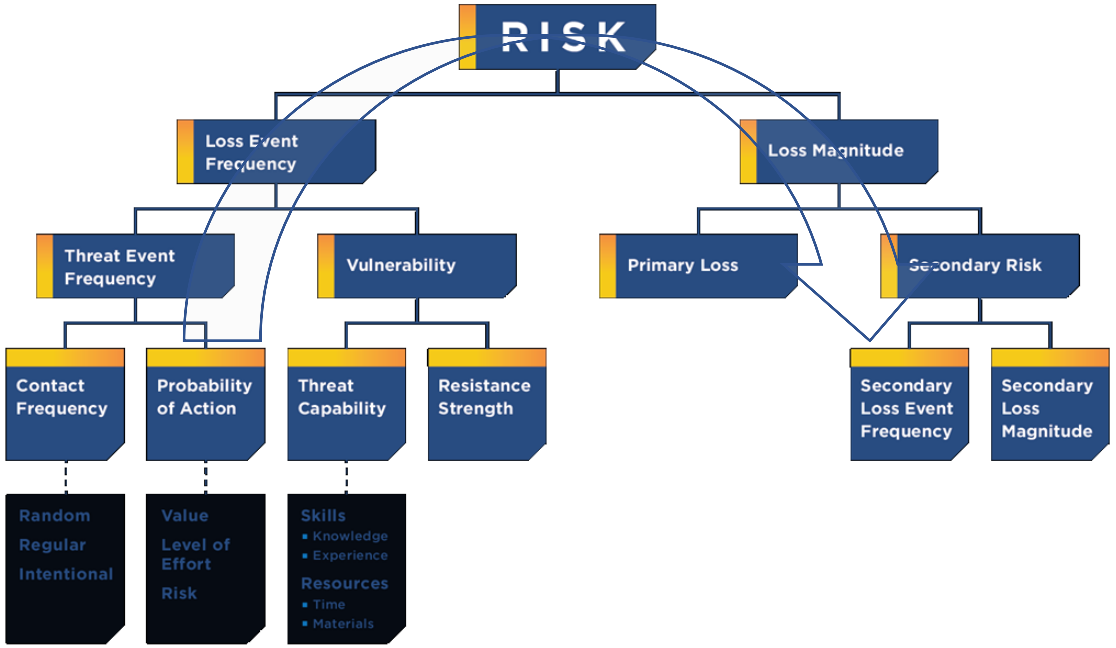


Use for mutually exclusive scenarios, combining expert estimates and discrete variables (like how many bridges)

Cyber risk

FAIR model is a very simple bowtie

FAIR



RISK

Loss Event Frequency

Loss Magnitude

Threat Event Frequency

Vulnerability

Primary Loss

Secondary Risk

Contact Frequency

Probability of Action

Threat Capability

Resistance Strength

Secondary Loss Event Frequency

Secondary Loss Magnitude

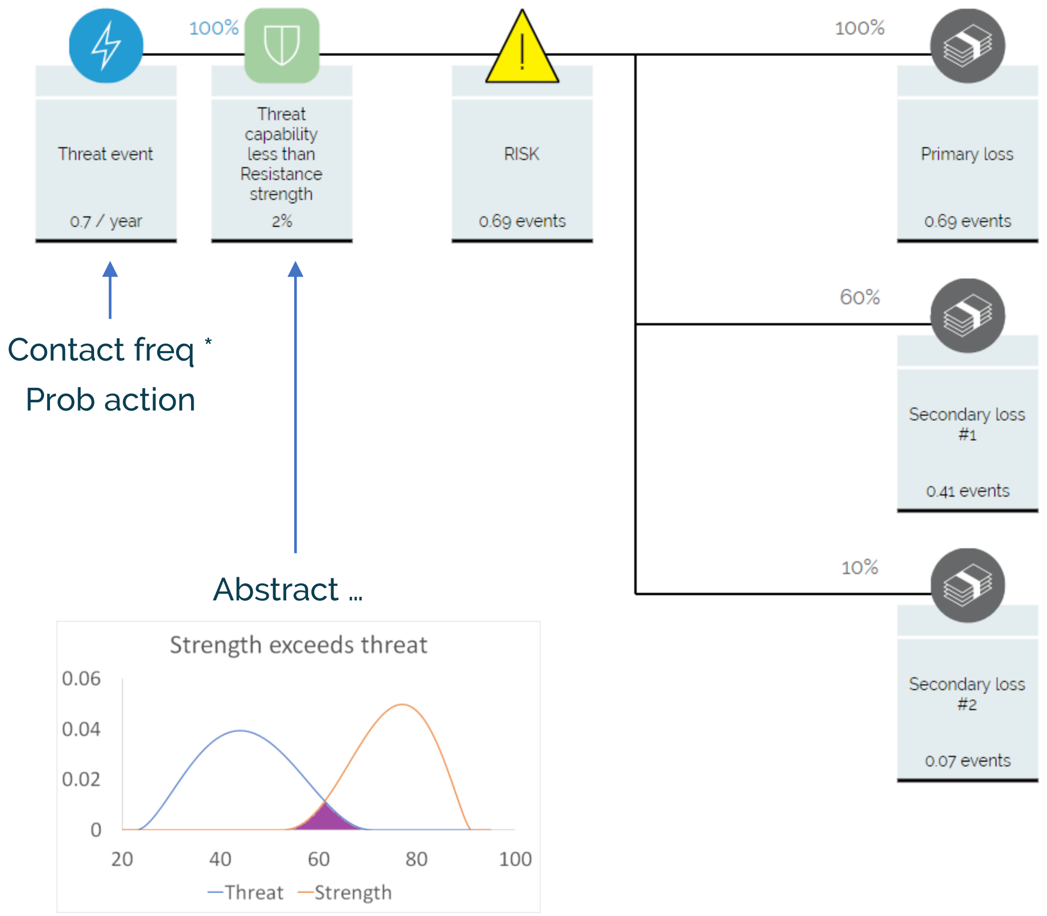
Random
Regular
Intentional

Value
Level of Effort
Risk

Skills
- Knowledge
- Experience

Resources
- Time
- Materials

Equivalent bowtie



100%

Threat event
0.7 / year

Threat capability less than Resistance strength
2%

RISK
0.69 events

100%

Primary loss
0.69 events

60%

Secondary loss #1
0.41 events

10%

Secondary loss #2
0.07 events

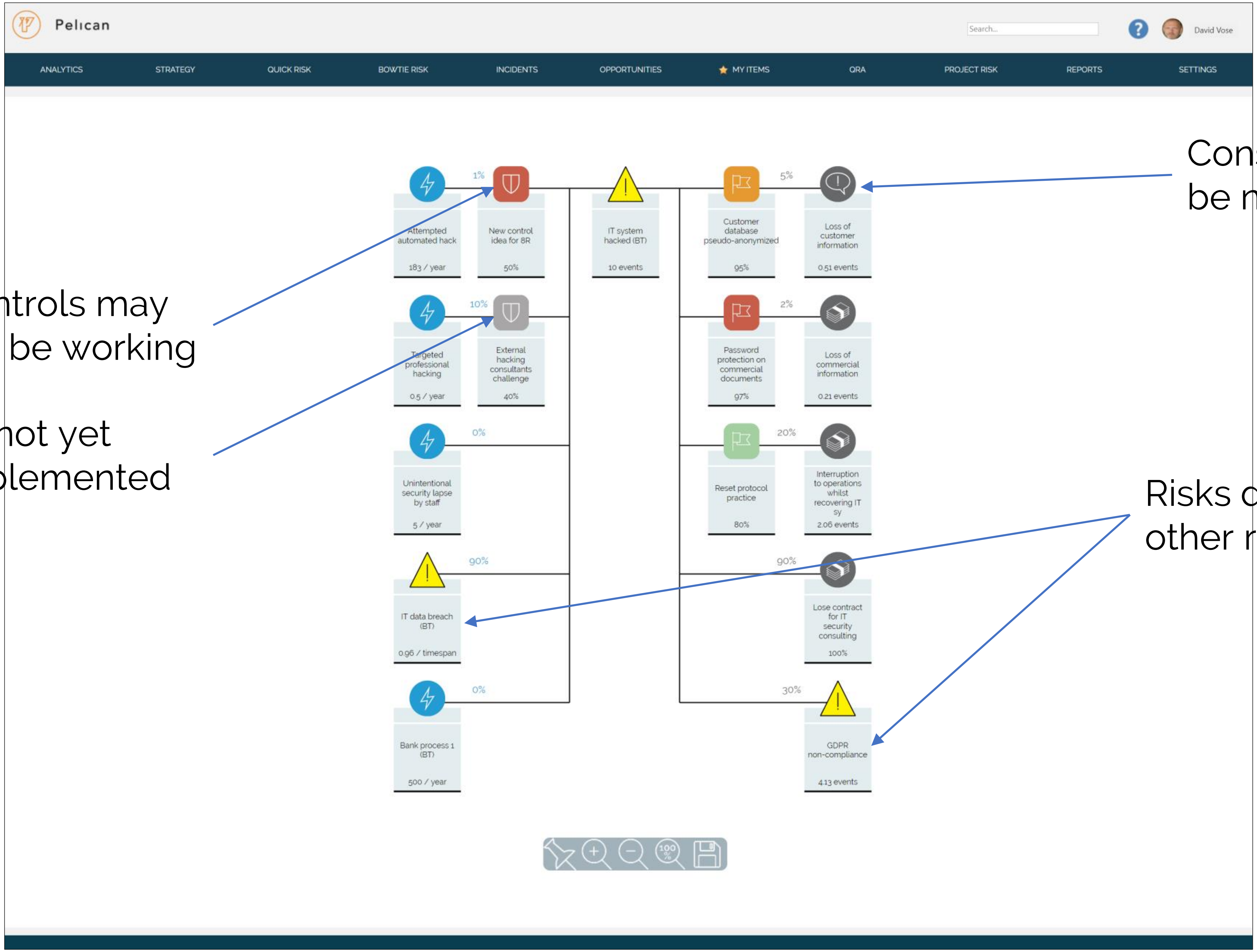
Contact freq *
Prob action

Abstract ...

Strength exceeds threat

$$p = \int_{min}^{max} f_T(x)\,(1 - F_S(x))dx$$

Full cybersecurity analysis



Controls may not be working

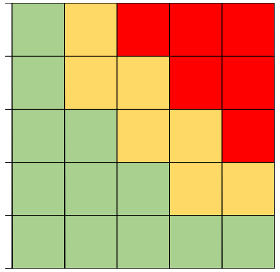
Or not yet implemented

Consequences can be non-financial

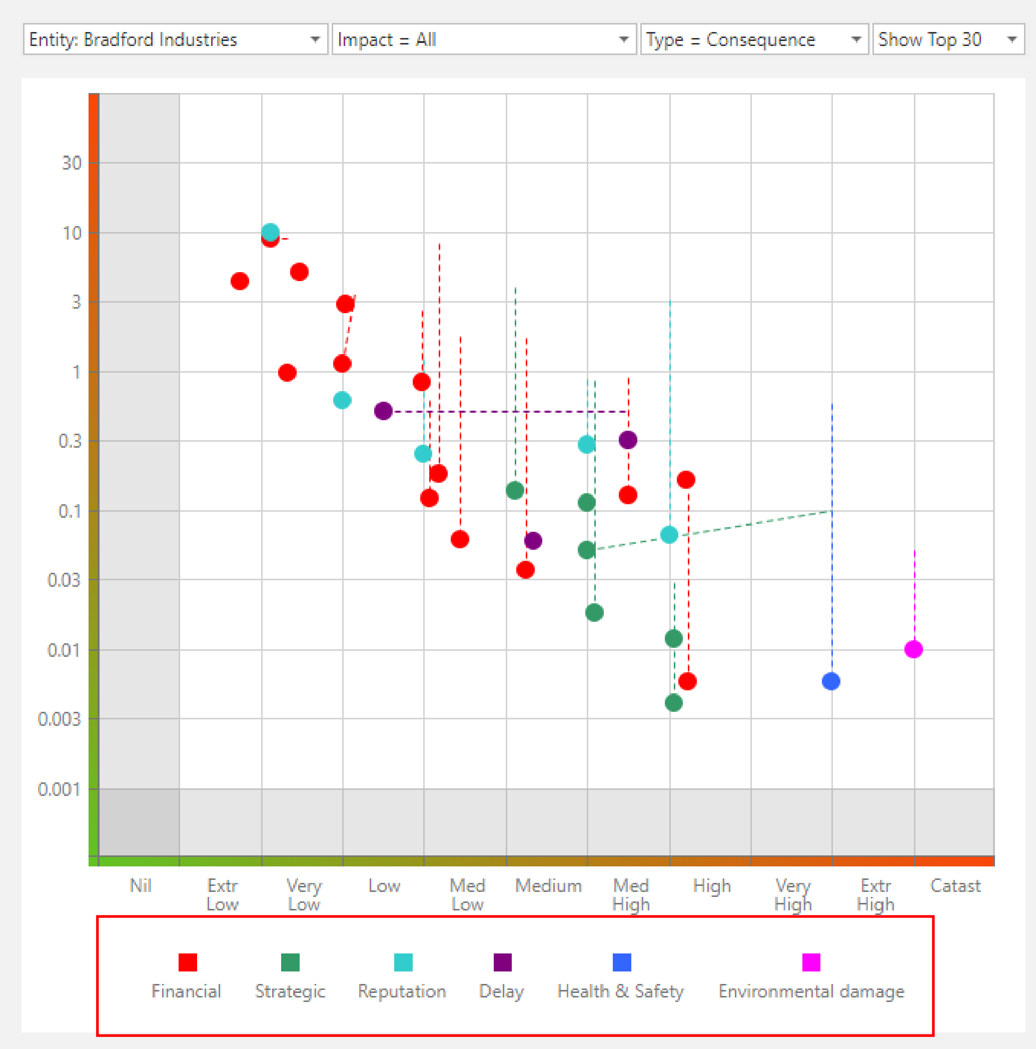
Risks drive other risks

An enterprise view of risk

Out with the old …



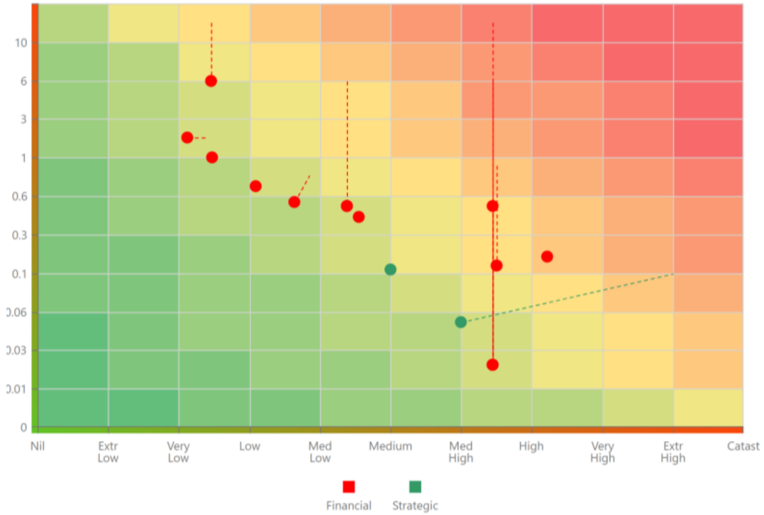
Individual risk overview



Entity: Bradford Industries | Impact = All | Type = Consequence | Show Top 30

- Consistent framework
- Scaled to entity
- Imposes corporate ethical standards

- Let's one see, for example, the value of a cyber-security control against a H&S control

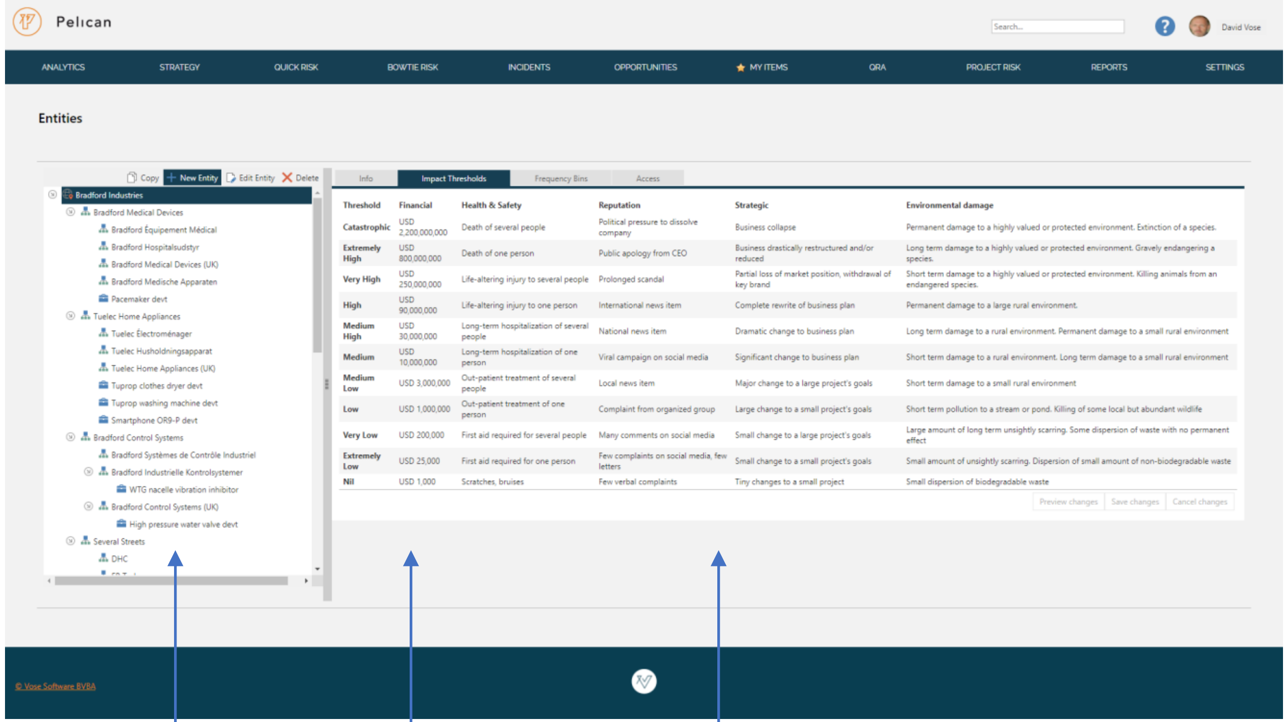


Multi Attribute Utility

🟩 + 🟩 = 🟨

🟩 + 🟩 = 🟩

?



Entities

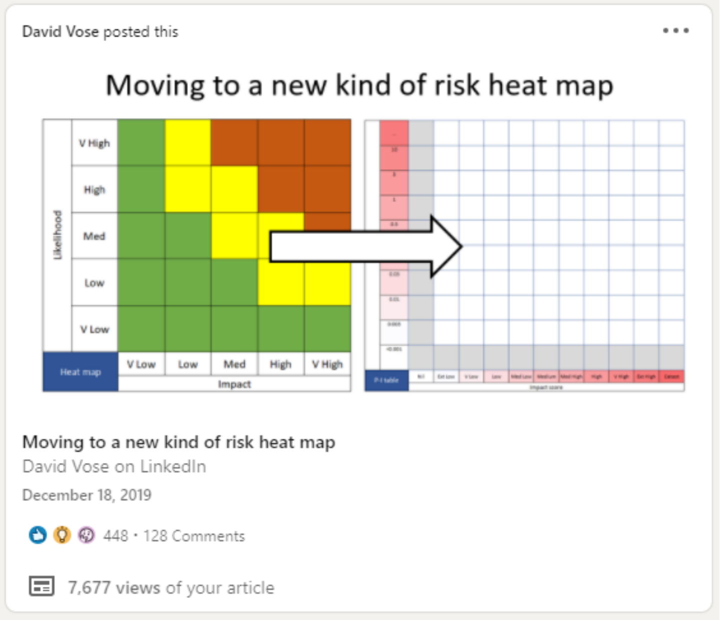
- Bradford Industries
  - Bradford Medical Devices
    - Bradford Équipement Médical
    - Bradford Hospitalsudstyr
    - Bradford Medical Devices (UK)
    - Bradford Medische Apparaten
    - Pacemaker devt
  - Tuelec Home Appliances
    - Tuelec Électroménager
    - Tuelec Husholdningsapparat
    - Tuelec Home Appliances (UK)
    - Tuprop clothes dryer devt
    - Tuprop washing machine devt
    - Smartphone OR9-P devt
  - Bradford Control Systems
    - Bradford Systèmes de Contrôle Industriel
    - Bradford Industrielle Kontrolsystemer
      - WTG nacelle vibration inhibitor
    - Bradford Control Systems (UK)
      - High pressure water valve devt
  - Several Streets
    - DHC

Threshold	Financial	Health & Safety	Reputation	Strategic	Environmental damage
Catastrophic	USD 2,200,000,000	Death of several people	Political pressure to dissolve company	Business collapse	Permanent damage to a highly valued or protected environment. Extinction of a species.
Extremely High	USD 800,000,000	Death of one person	Public apology from CEO	Business drastically restructured and/or reduced	Long term damage to a highly valued or protected environment. Gravely endangering a species.
Very High	USD 250,000,000	Life-altering injury to several people	Prolonged scandal	Partial loss of market position, withdrawal of key brand	Short term damage to a highly valued or protected environment. Killing animals from an endangered species.
High	USD 90,000,000	Life-altering injury to one person	International news item	Complete rewrite of business plan	Permanent damage to a large rural environment.
Medium High	USD 30,000,000	Long-term hospitalization of several people	National news item	Dramatic change to business plan	Long term damage to a rural environment. Permanent damage to a small rural environment
Medium	USD 10,000,000	Long-term hospitalization of one person	Viral campaign on social media	Significant change to business plan	Short term damage to a rural environment. Long term damage to a small rural environment
Medium Low	USD 3,000,000	Out-patient treatment of several people	Local news item	Major change to a large project's goals	Short term damage to a small rural environment
Low	USD 1,000,000	Out-patient treatment of one person	Complaint from organized group	Large change to a small project's goals	Short term pollution to a stream or pond. Killing of some local but abundant wildlife
Very Low	USD 200,000	First aid required for several people	Many comments on social media	Small change to a large project's goals	Large amount of long term unsightly scarring. Some dispersion of waste with no permanent effect
Extremely Low	USD 25,000	First aid required for one person	Few complaints on social media, few letters	Small change to a small project's goals	Small amount of unsightly scarring. Dispersion of small amount of non-biodegradable waste
Nil	USD 1,000	Scratches, bruises	Few verbal complaints	Tiny changes to a small project	Small dispersion of biodegradable waste

Entity structure

$

Qualitative and quantitative



David Vose posted this

Moving to a new kind of risk heat map

Moving to a new kind of risk heat map

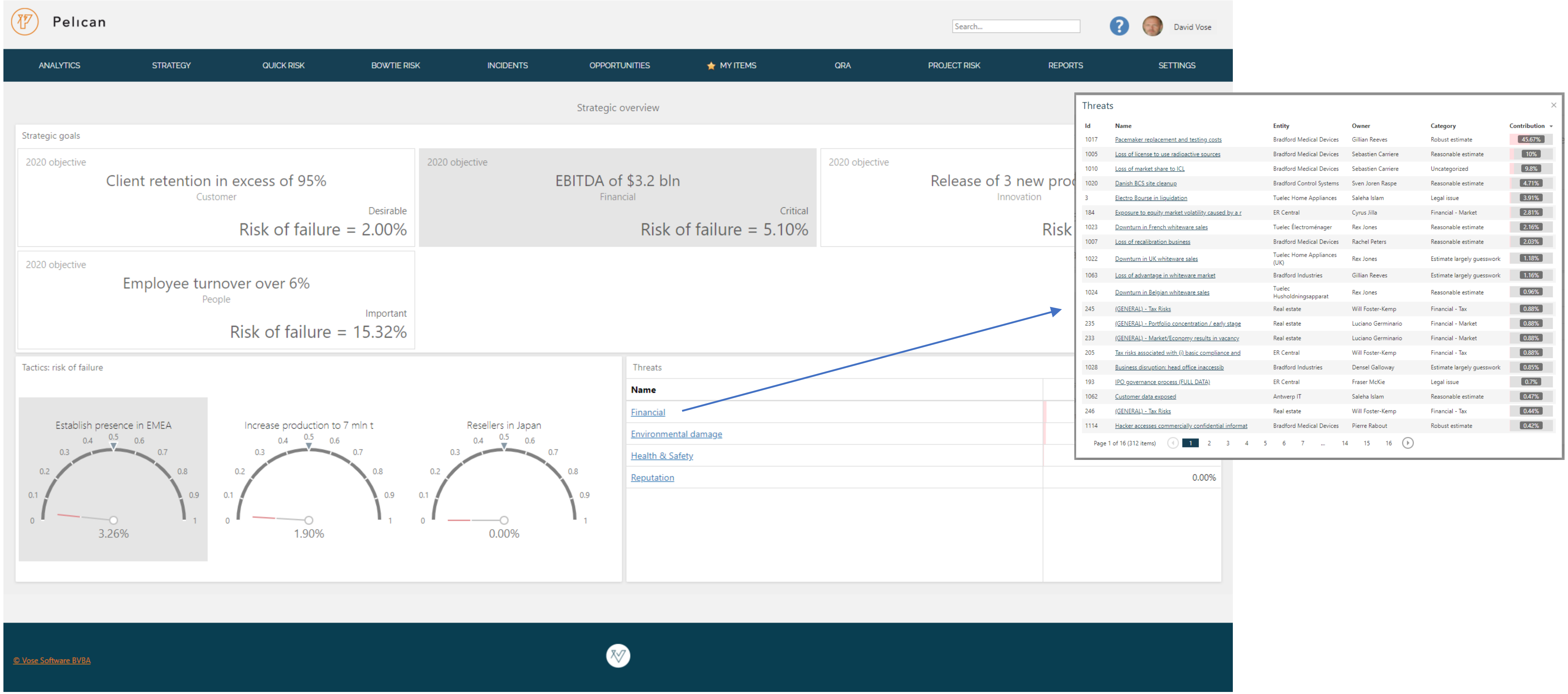
David Vose on LinkedIn

December 18, 2019

448 · 128 Comments

7,677 views of your article

Strategic risk



Pelican

Search...

David Vose

ANALYTICS | STRATEGY | QUICK RISK | BOWTIE RISK | INCIDENTS | OPPORTUNITIES | ★ MY ITEMS | QRA | PROJECT RISK | REPORTS | SETTINGS

Strategic overview

Strategic goals

2020 objective
Client retention in excess of 95%
Customer
Desirable
Risk of failure = 2.00%

2020 objective
EBITDA of $3.2 bln
Financial
Critical
Risk of failure = 5.10%

2020 objective
Release of 3 new prod
Innovation
Risk

2020 objective
Employee turnover over 6%
People
Important
Risk of failure = 15.32%

Tactics: risk of failure

Threats

Name	
Financial	
Environmental damage	
Health & Safety	
Reputation	0.00%

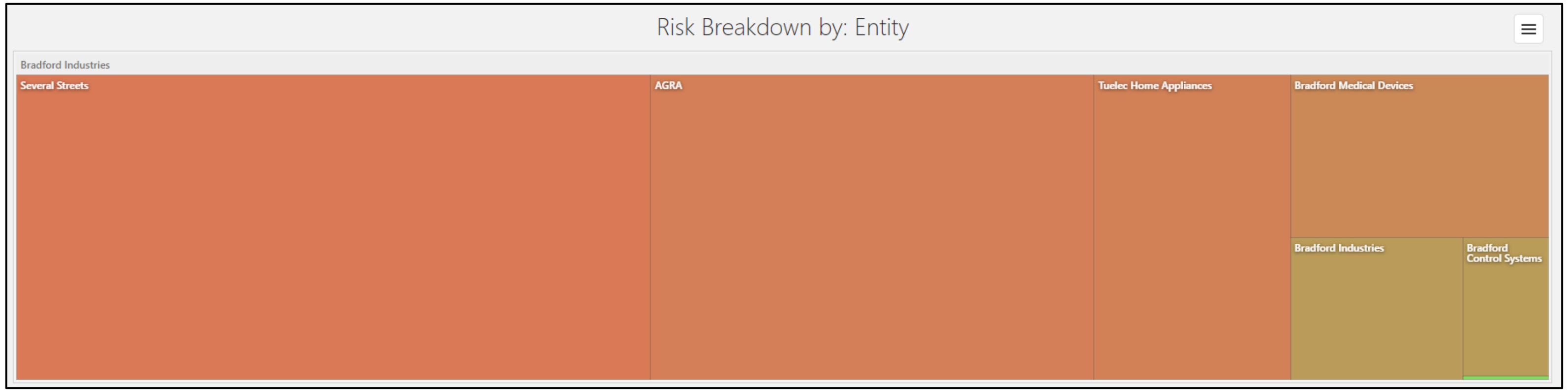
Threats

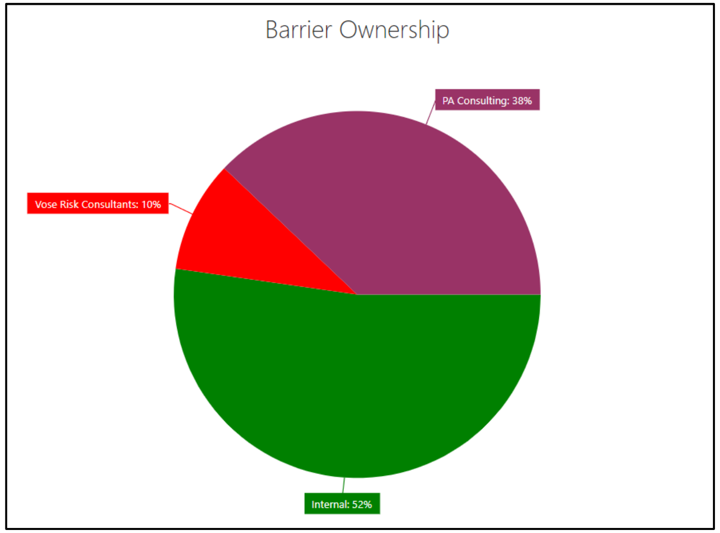
Id	Name	Entity	Owner	Category	Contribution
1017	Pacemaker replacement and testing costs	Bradford Medical Devices	Gillian Reeves	Robust estimate	45.67%
1005	Loss of license to use radioactive sources	Bradford Medical Devices	Sebastien Carriere	Reasonable estimate	10%
1010	Loss of market share to ICL	Bradford Medical Devices	Sebastien Carriere	Uncategorized	9.8%
1020	Danish BCS site cleanup	Bradford Control Systems	Sven Joren Raspe	Reasonable estimate	4.71%
3	Electro Bourse in liquidation	Tuelec Home Appliances	Saleha Islam	Legal issue	3.91%
184	Exposure to equity market volatility caused by a r	ER Central	Cyrus Jilla	Financial - Market	2.81%
1023	Downturn in French whiteware sales	Tuelec Électroménager	Rex Jones	Reasonable estimate	2.16%
1007	Loss of recalibration business	Bradford Medical Devices	Rachel Peters	Reasonable estimate	2.03%
1022	Downturn in UK whiteware sales	Tuelec Home Appliances (UK)	Rex Jones	Estimate largely guesswork	1.18%
1063	Loss of advantage in whiteware market	Bradford Industries	Gillian Reeves	Estimate largely guesswork	1.16%
1024	Downturn in Belgian whiteware sales	Tuelec Husholdningsapparat	Rex Jones	Reasonable estimate	0.96%
245	(GENERAL) - Tax Risks	Real estate	Will Foster-Kemp	Financial - Tax	0.88%
235	(GENERAL) - Portfolio concentration / early stage	Real estate	Luciano Germinario	Financial - Market	0.88%
233	(GENERAL) - Market/Economy results in vacancy	Real estate	Luciano Germinario	Financial - Market	0.88%
205	Tax risks associated with (i) basic compliance and	ER Central	Will Foster-Kemp	Financial - Tax	0.88%
1028	Business disruption: head office inaccessib	Bradford Industries	Densel Galloway	Estimate largely guesswork	0.85%
193	IPO governance process (FULL DATA)	ER Central	Fraser McKie	Legal issue	0.7%
1062	Customer data exposed	Antwerp IT	Saleha Islam	Reasonable estimate	0.47%
246	(GENERAL) - Tax Risks	Real estate	Will Foster-Kemp	Financial - Tax	0.44%
1114	Hacker accesses commercially confidential informat	Bradford Medical Devices	Pierre Rabout	Robust estimate	0.42%

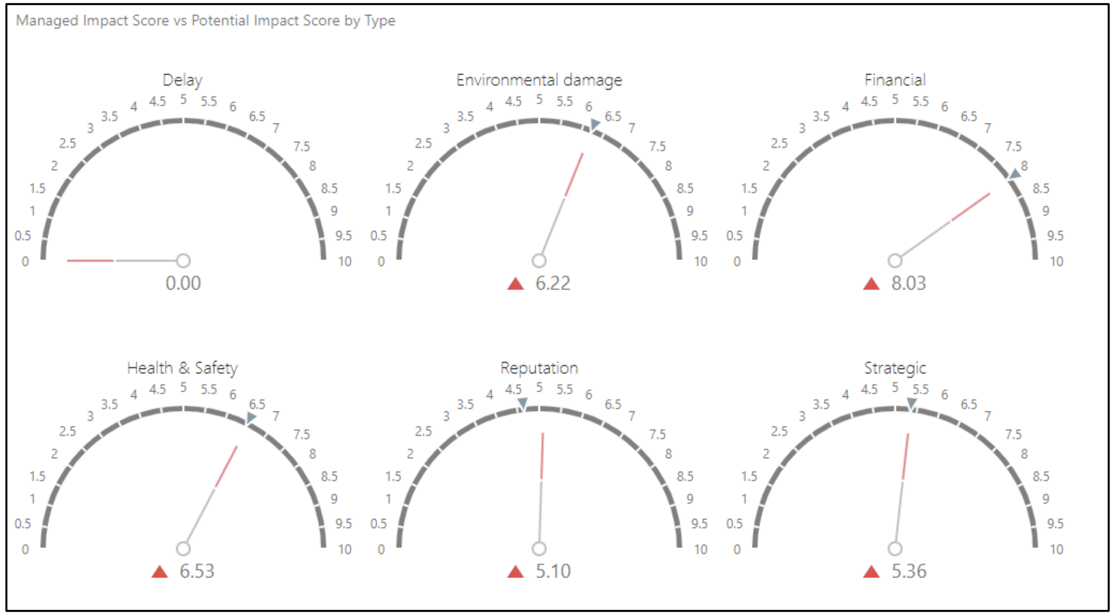
Page 1 of 16 (312 items) 1 2 3 4 5 6 7 ... 14 15 16

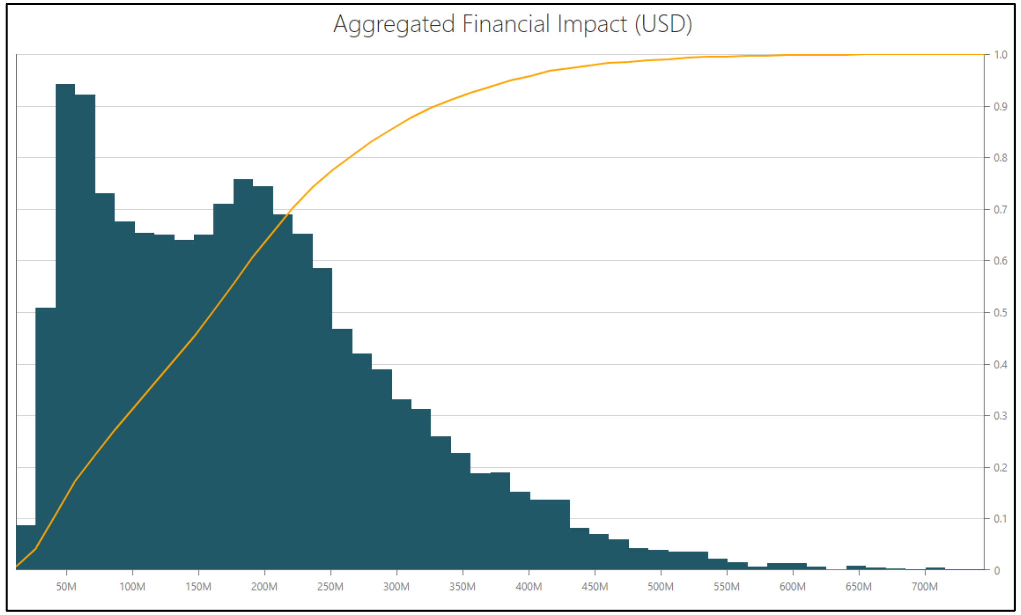
© Vose Software BVBA

Monitoring


Risk Breakdown by: Entity


Barrier Ownership


Managed Impact Score vs Potential Impact Score by Type


Aggregated Financial Impact (USD)

Thank you

Questions?