RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **RMG1-R07**

What's in your risk assessment?

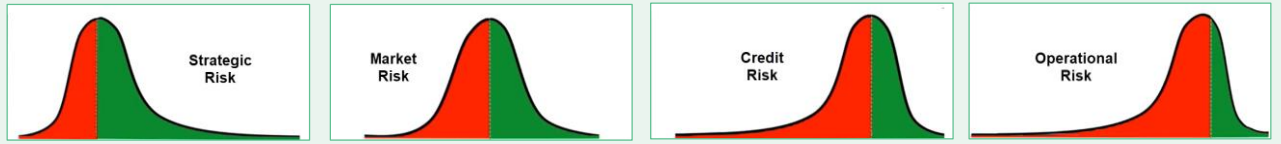
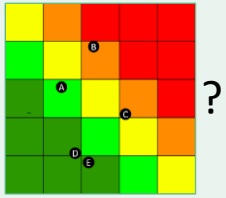
Steve Reznik

Director, Operational Risk Management
ADP

Allison Seidel

Senior Risk Specialist
PNC Bank

Are we aligned?

Risk Assessment Concept	The Board 	The Security Team 
Asset	Digital assets portfolio, corporate brand, reputation	Technology? The perimeter?
Risk		 ?
Threat	Cyber Criminals, Privileged Insiders	Vulnerability?
Control	$ → ROI	Compliance? Audit requirement?
Trade Off	Value / Risk	User experience / Control?
Likelihood	%	Given a long enough timeline…?
Impact	$	H/M/L?
Assessment	Decision	Procedure

Why stay?

- Probabilistic approach to risk assessment
- How to get started
- Case study of value with compliance

Risk Assessment
(Key Terms)

The probable frequency and probable magnitude of future loss associated with a specific event

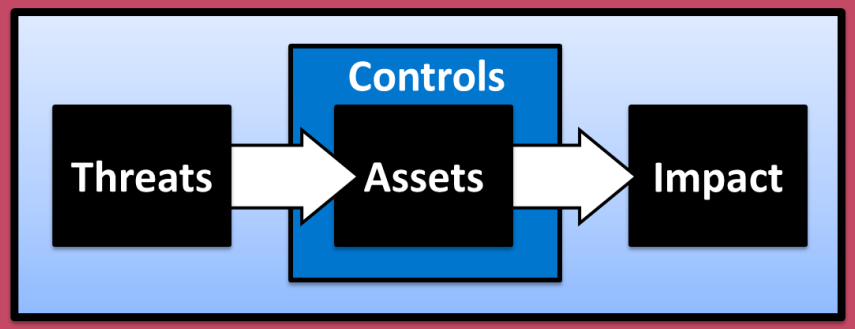
Source: Risk Analysis (O-RA), an Open Group Standard (C13G), October 2013 www.opengroup.org/library/c13g

The act of judging or deciding the amount, value, quality, or importance of something, or the judgment or decision that is made

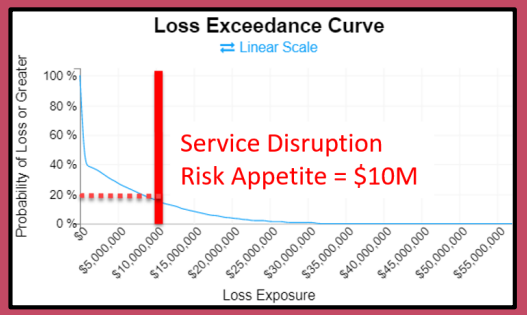
Source: Cambridge Dictionary

Risk Assessment
(Key Questions)

- Identify assets of value and possible loss events that may materialize – "Where/What?"
- Describe the action of a threat onto an asset and the effect (loss event scenario) – "How?"

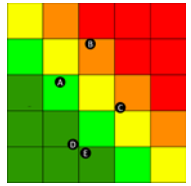


- Gather data and analyze factors of loss event scenarios – "How much?"
- Estimate the effect of changes to certain risk factors – "How much more/less if?"



Where's the risk assessment?

- Expert intuition alone
- Stratification with red-yellow-green or risk score
- Weighted scores
- ISO 31010 consequence/probability matrix
- ERM inherent/residual risk campaign
- Application security testing
- Red team exercise
- Baseline standards compliance review
- Threat modelling
- Maturity assessment
- ISO/IEC Annex B 31 flavors
- NIST 800-30r1
- RCSA



Which ones answer:

- Where/What?
- How?
- How much?
- How much more/less if?

RSAConference2020

Poll Questions

Poll the Audience

- Session ID #RMG1-R07
- Does your risk assessment include industry costs?
  - Yes
  - No
  - Not sure
- https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1931438753

Poll the Audience

- Session ID #RMG1-R07
- Does your risk assessment include probability distributions?
  - Yes
  - No
  - Not sure
- https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1931438753

Poll the Audience

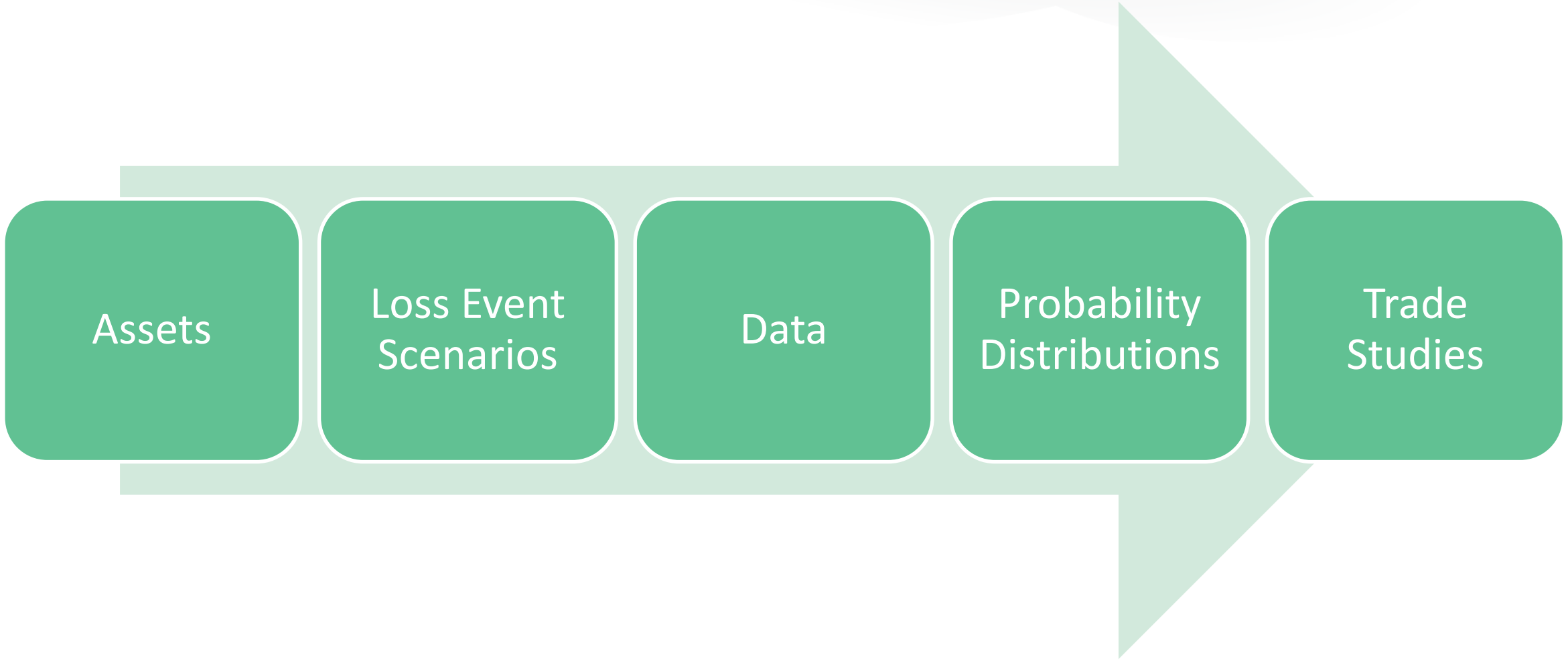
- Session ID #RMG1-R07
- Does your risk assessment include trade studies?
  - Yes
  - No
  - Not sure
- https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1931438753

Polling is over now…please put down your mobile and take me home!

RSAConference2020

How to get started

Quantitative Risk Assessment Flow

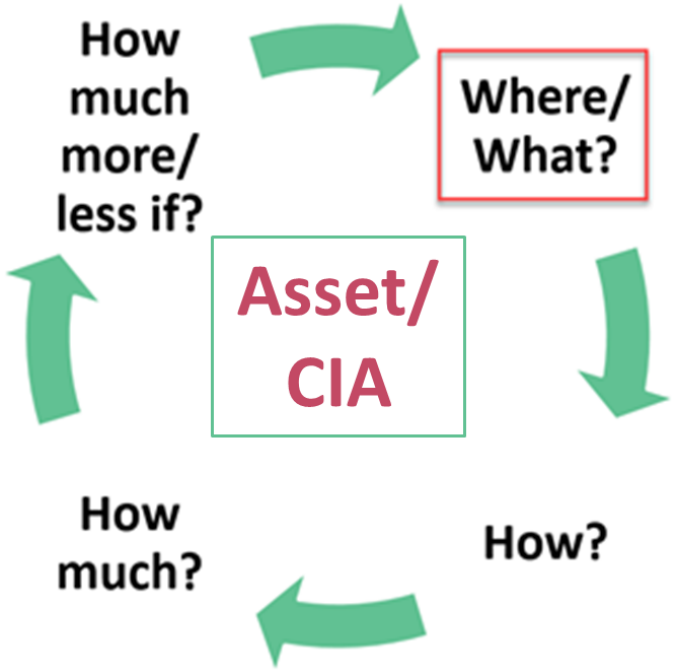


RSAConference2020

Assets

Risk exists where…

- **Value can be lost or diminished**
  - Revenue generators and services
  - Resources with replacement costs / street value
  - Efficiency drivers
- **Liability can materialize**
  - Information confidentiality/integrity/privacy
  - Service availability
  - Personal health & safety
- **Resources can be wasted**

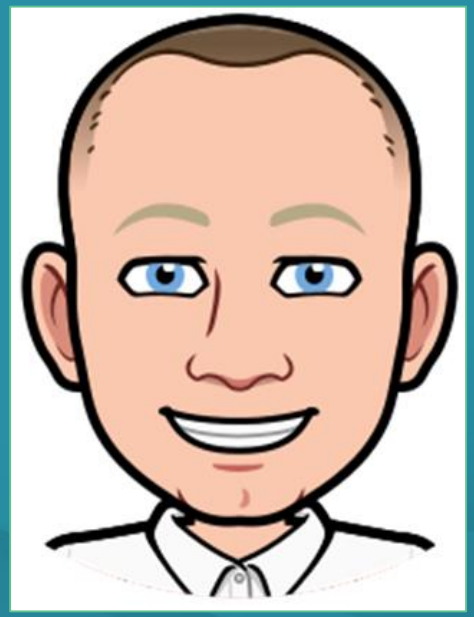


“How much risk is associated with _____?”

- Differentiating process
- Customer information
- Infrastructure
  - Technology
  - Equipment
  - Facility
- Intellectual property
- Third party

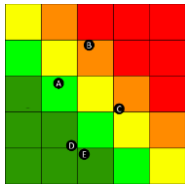
RSAConference2020

Loss event scenarios



Calibration Question

How many humans are attending RSAC 2020?

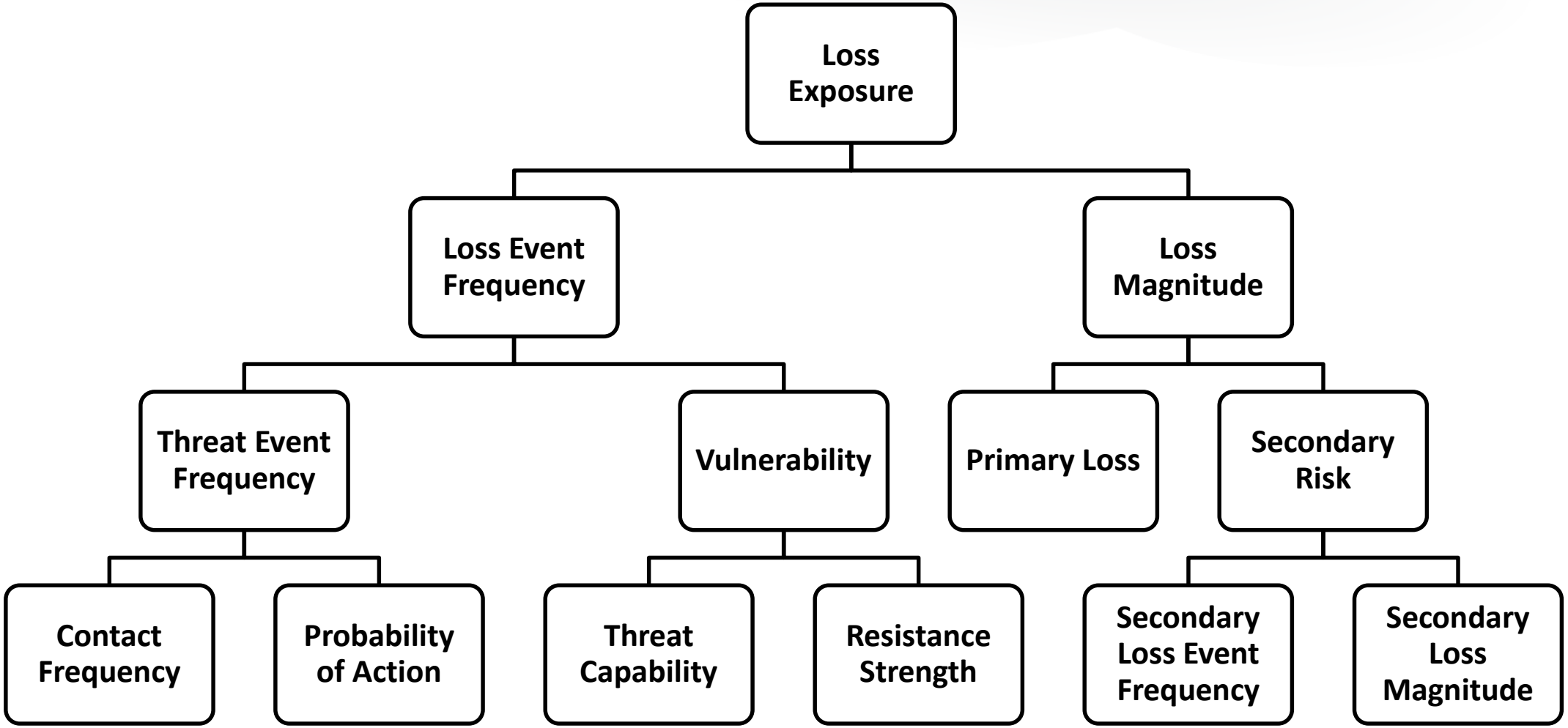
1) A lot
2) More than last year
3) 36,524 
4) 10,000 – 100,000
5) 30,000 – 50,000

CALIBRATION:

- Start with the absurd
- Consider what you DO know
- Decompose the problem
- Identify / challenge your assumptions
- Consider where data may exist
- Seek out SMEs
- Focus on accuracy rather than high precision

Source: FAIR Institute

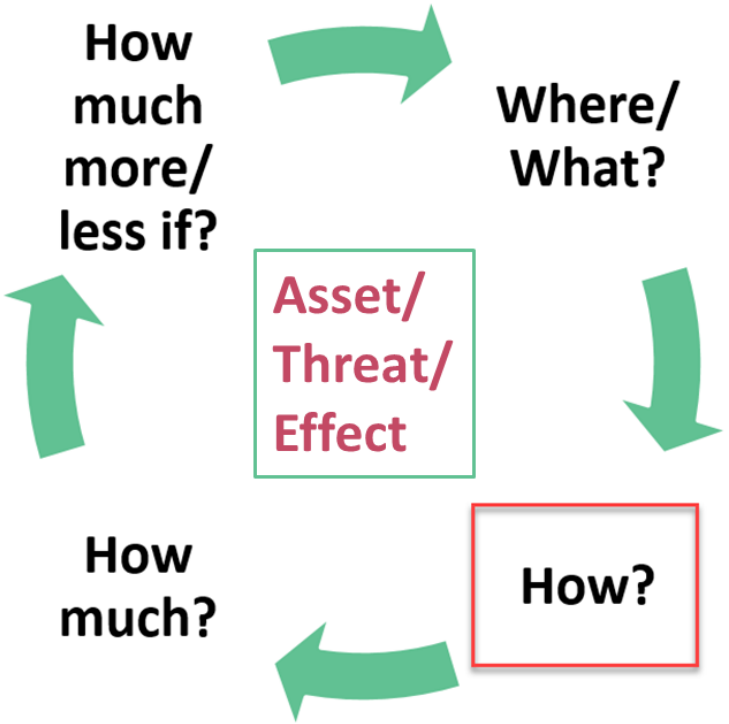
Loss Event Scenario Factors



Getting started with loss event scenarios

Asset + Threat Community + Threat Effect

Frequency	Magnitude
Driving Factors	Driving Factors
-	-
-	-
-	-
Limiting Factors	Limiting Factors
-	-
-	-
-	-



RSAConference2020

Data

What do the experts say about data?

Doug Hubbard

- Your problem is not as unique as you think
- You have more data than you think
- You need less data than you think
- An adequate amount of new data is more accessible than you think

Jack Jones

- Calibration methods enable subject matter experts to provide good estimates
- Many organizations are awash in data from the security technologies that they use
- Many organizations have processes in place that can be useful sources of data

"Attention cyber risk data shoppers…"

Types of Costs

- Notification
- Forensics
- Credit monitoring
- Regulatory
- Legal guidance/ Crisis services
- Recovery
- Lost Income

External Source	Cost	Relevance	Reputation
Advisen	$	Variable based on criteria	Reputable source
FTC		Fines only	Reputable
IBM/ Ponemon	$	Variable	Known issues
NetDiligence	$	Variable	Reputable
SEC		Fines only	Reputable
Tower Street	$	Variable	New
Verizon DBIR		Dated	Reputable
Your insurance company		Minimal	Biased toward active clients

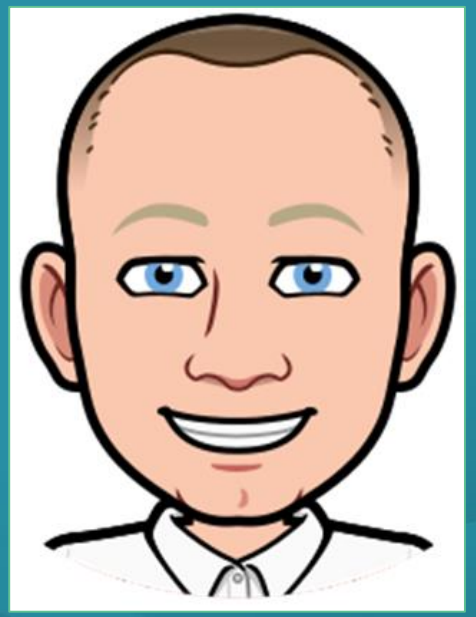
HUMAN ELEMENT

Internal Sources

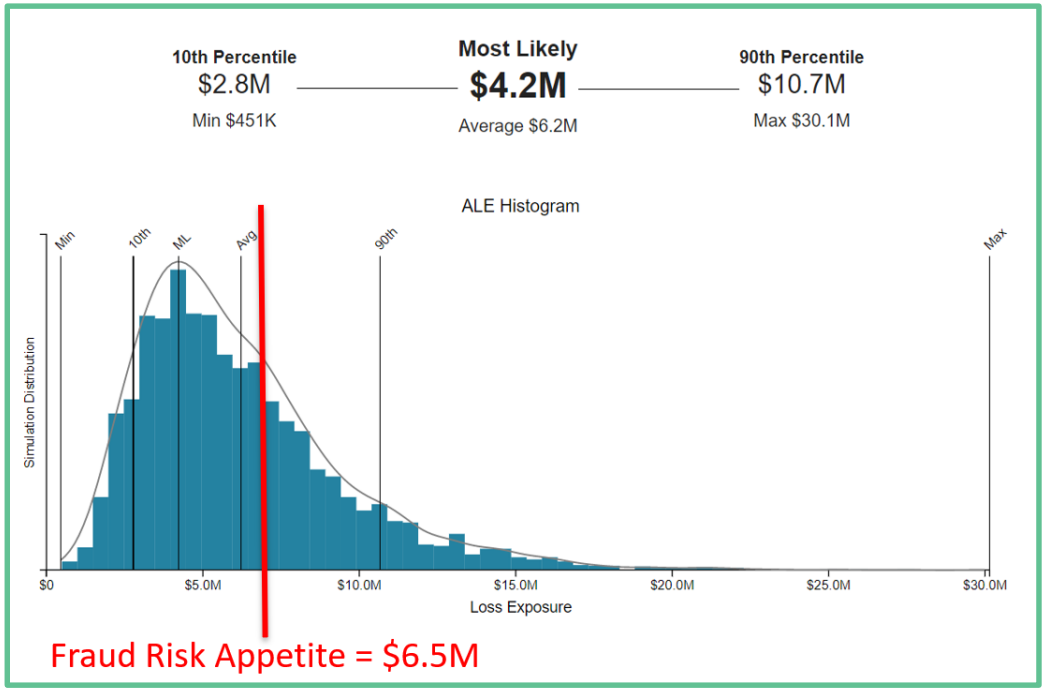
- Insurance group
- Information security
- Corporate communications
- Human resources
- Third party vendor management
- Incident Management
- Fraud
- Business continuity
- Legal
- Other risk groups

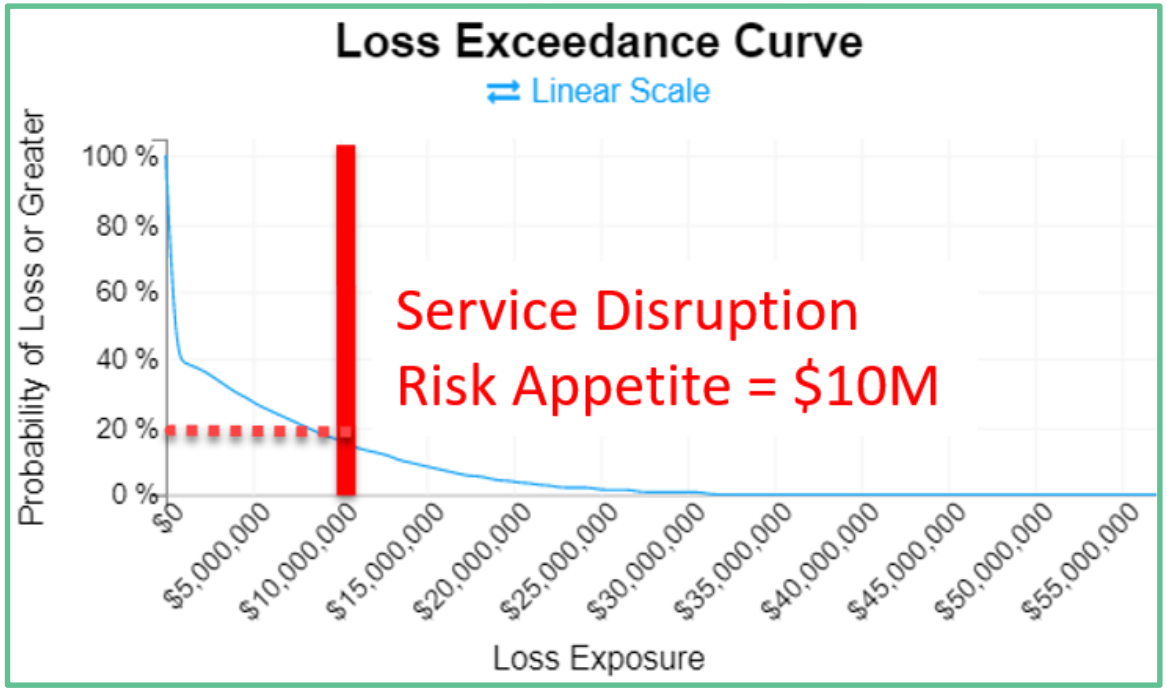
RSAConference2020

Probability distributions and trade studies



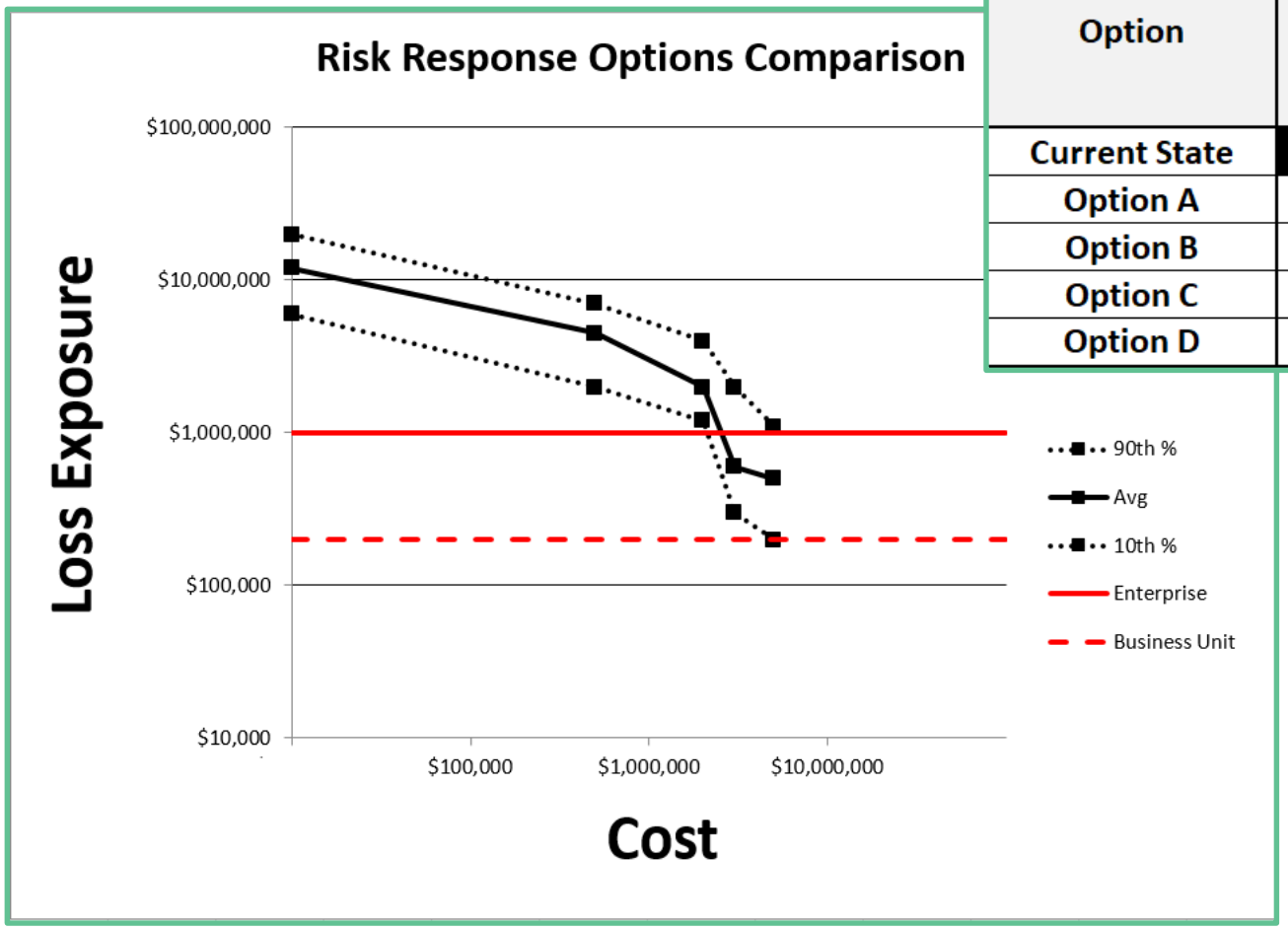
Probability Distributions





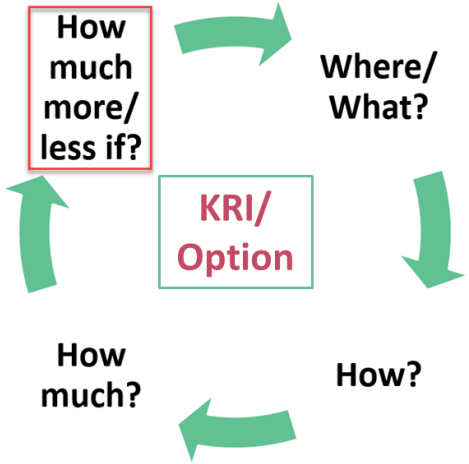
"A 40% probability in the next 12 months of > 100k lost customer transactions in any 24 hour period"

Trade Studies



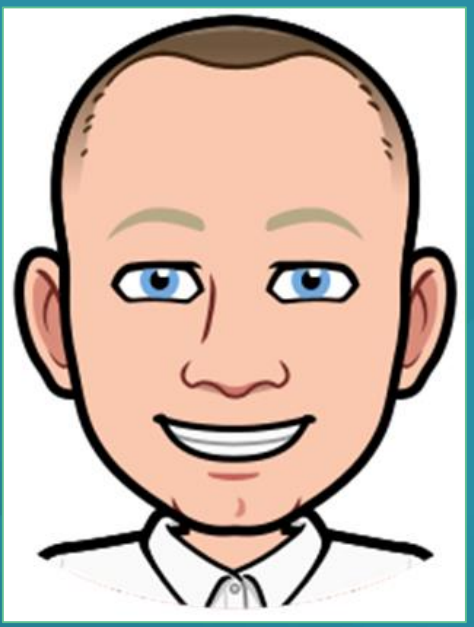
Option	Cost ($USD)	Annual Loss Exposure			Risk Reduction Benefit/ Cost Ratio
		10th %	Average	90th %	
Current State		$6,000,000	$12,000,000	$20,000,000	
Option A	$500,000	$2,000,000	$4,500,000	$7,000,000	15 to 1
Option B	$2,000,000	$1,200,000	$2,000,000	$4,000,000	5 to 1
Option C	$3,000,000	$300,000	$600,000	$2,000,000	4 to 1
Option D	$5,000,000	$200,000	$500,000	$1,100,000	2 to 1

- Risk
- Cost
- Schedule
- Scope
- Disruption



RSAConference2020

External requirements for risk assessment



Entities referencing “Risk Assessment”

- FHFA
- FIPS 200
- GDPR
- GLBA
- HIPAA Privacy Rule
- HIPAA Security Rule
- PCI-DSS
- SSAE 18

- COBIT 2019
- FFIEC
- HITRUST CS
- ISO 31000
- ISO/IEC 27001
- NIST CSF
- NYDFS
- SEC – Cybersecurity Disclosures

Mapping to external requirements

Entity	Risk Assessment Requirement	Point
FHFA	Develop strategies to mitigate those risks to the availability, integrity, confidentiality, and accountability of information and information systems	Where/What? How much less if?
GDPR	Conduct data protection impact assessments to identify and reduce the data protection risk within projects and systems, and thereby reduce the likelihood of privacy harms to affected EU citizens	Where/What? How much less if?
PCI - DSS	Determine the significance of risks in order to prioritize mitigation efforts…using numerical values in the risk assessment can result in more objective results…implement a risk-assessment process that identifies critical assets, threats, and vulnerabilities, and results in a formal, documented analysis of risk	Where/What? How much? How much less if?

Mapping to external requirements

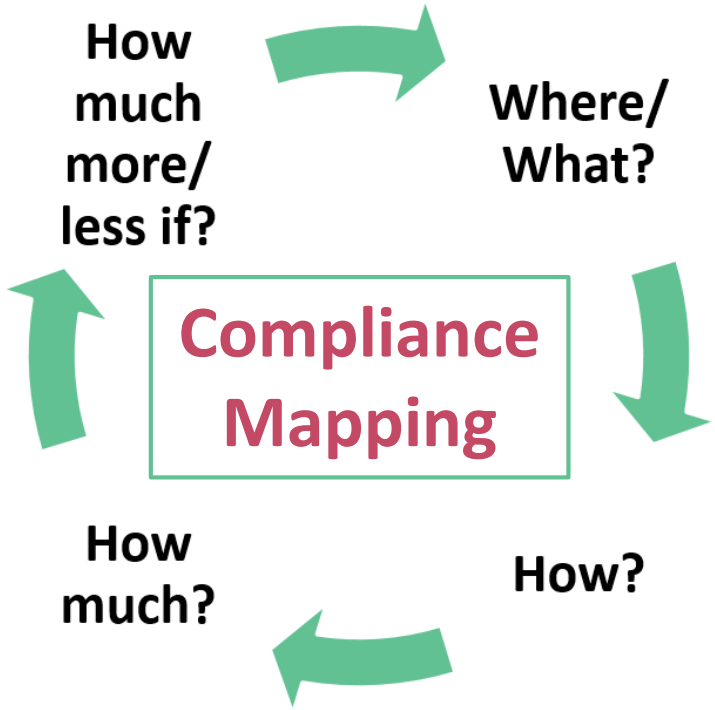
Entity	Risk Assessment Requirement	Point
COBIT 2019	Recommends articulating risk scenarios and providing decision makers with probabilities, ranges of loss, and confidence levels…based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends	How? How much? How much more if?
ISO/IEC 27001	Establish and maintain certain information security risk criteria…the value of the identified assets in terms of their confidentiality, integrity and availability…the threats and vulnerabilities that affect the security of those assets…the impact on the organization should the assets be compromised; and the likelihood of them being compromised	Where/What? How? How much?
NIST CSF	The organization…analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization…use cyber threat information from internal and external sources	Where/What? How much?

Getting started with external requirements

REGULATORY/ COMPLIANCE RISK ASSESSMENT OVERVIEW FOR FAIR PRACTITIONERS

DISCLAIMER: This document is a compilation of requirements from various regulatory and compliance entities. It is intended to be used as an overview of risk assessment requirements, including commonalities amongst entities. It is a point-in-time document; therefore, users are responsible for keeping up with new and changing requirements.

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
PCI-DSS	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk.	"at least annually and upon significant changes to the environment"	Discussed but no specific recommendation	Yes PCS DSS Risk Assessment Guidelines discuss "Risk Evaluation" as a way to "determine the significance of risks in order to prioritize mitigation efforts" and that using numerical values in the risk assessment can result in more objective results	Yes PCS DSS Risk Assessment Guidelines identifies a "need for the continuous monitoring of risks throughout the year"	Compliance activity details for numerous requirements are to be determined by the annual risk assessment.	FAIR, NIST SP 800-30, OCTAVE, ISO 27005
COBIT 2019	Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management. Source: COBIT 2019 Management Objective APO12 – Managed Risk.	Not Specified	Yes Recommends articulating risk scenarios and	Yes Estimate the frequency and magnitude of loss	Yes Based on all risk profile data, define a set of risk	Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic	CMMI Cyber Maturity Platform; COSO ERM; ISO/IEC 27005:2011; NIST CSF; NIST 800-53



RSAConference2020

Case Study

Risk Appetite

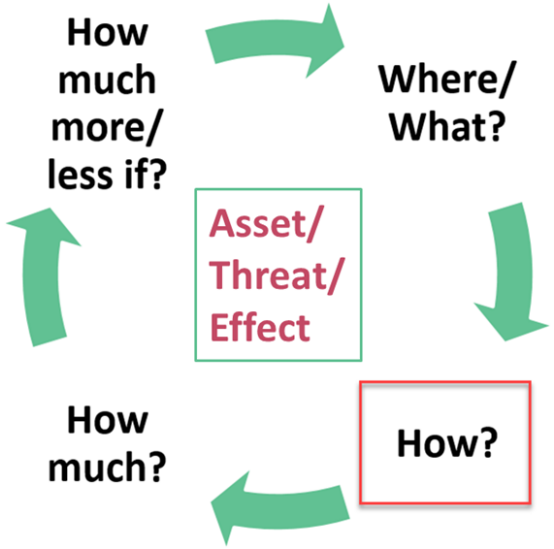
Event	Probability	Impact
PII disclosure	10%	> 1M records (C)
Lost customer transactions in any 24 hour period	5%	> 100k transactions (I-Data)
Total fraud losses due to external threats	Yearly	< $4M (I-$)
Successful denial of critical services during peak customer demand timeframe	20%	> 4 hours downtime (A)
Financial misstatement stemming from an IT or cyber-related problem	5%	> $10M misstatement
Cybersecurity related regulatory action against the company	5%	Consent decree

Assets

Loss event scenarios

BANK OF THE VALE

Event	Asset	Threat Community	Threat Type	Threat Effect
Data Breach	Customer dB	Cyber Criminals	Malicious	C
Data Breach	Email	Cyber Criminals	Malicious	C
Service Disruption	Email	Administrator	Error	A
Processing Error	MF Apps	Developer	Malicious	I
System Outage	MF Apps	Developer	Error	A
Ransomware	3rd Party	Cyber Criminals	Malicious	A
External Fraud	Web Platform	Cyber Criminals	Malicious	I
Service Disruption	Web Platform	General Hackers	Malicious	A
Ransomware	Trading Platform	Cyber Criminals	Malicious	A



Shopping for Data – CC > Cust dB > C

Risk Factor Components			Min	Most Likely	Max
Loss Event Frequency	TEF (#)		0.5	1	2
	Threat Capability (%)		60	75	99
	Resistance Strength (%)		75	80	85
Primary Loss	Primary Response Cost (Hrs)		1,000	2,500	8,000
Secondary Risk	SLEF (%)		100	100	100
	SLM	Secondary Response Costs ($)	3.5M	48M	110M
		Fines and Judgments ($)	1.5M	16M	40M
		Reputation Damage ($)	40M	60M	80M

- Database administrators/owners
- Cybersecurity management
- Sales and Marketing
- Human Resources
- External: NetDiligence, Advisen

Loss event scenarios – Quantified

Event	Asset	Threat Community	Threat Type	Threat Effect	Min	10th	Average	90th	Max
Data Breach	Customer dB	Cyber Criminals	Malicious	C			$47,000,000	$160,000,000	$230,000,000
Data Breach	Email	Cyber Criminals	Malicious	C			$5,500,000	$19,000,000	$27,000,000
Service Disruption	Email	Administrator	Error	A			$1,900,000	$5,500,000	$11,000,000
Processing Error	MF Apps	Developer	Malicious	I			$2,700,000	$6,500,000	$10,000,000
System Outage	MF Apps	Developer	Error	A			$1,800,000	$3,500,000	$6,000,000
Ransomware	3rd Party	Cyber Criminals	Malicious	A	$860,000	$3,000,000	$5,000,000	$7,000,000	$13,000,000
External Fraud	Web Platform	Cyber Criminals	Malicious	I	$450,000	$2,800,000	$6,200,000	$11,000,000	$30,000,00
Service Disruption	Web Platform	General Hackers	Malicious	A			$3,900,000	$15,000,000	$58,000,000
Ransomware	Trading Platform	Cyber Criminals	Malicious	A		$1,000,000	$1,600,000	$3,000,000	$5,000,000

Top three scenarios by percentile

Event	Asset	Threat Community	Threat Type	Threat Effect	90th
Data Breach	Customer dB	Cyber Criminals	Malicious	C	$160,000,000
Data Breach	Email	Cyber Criminals	Malicious	C	$19,000,000
Service Disruption	Web Platform	General Hackers	Malicious	A	$15,000,000

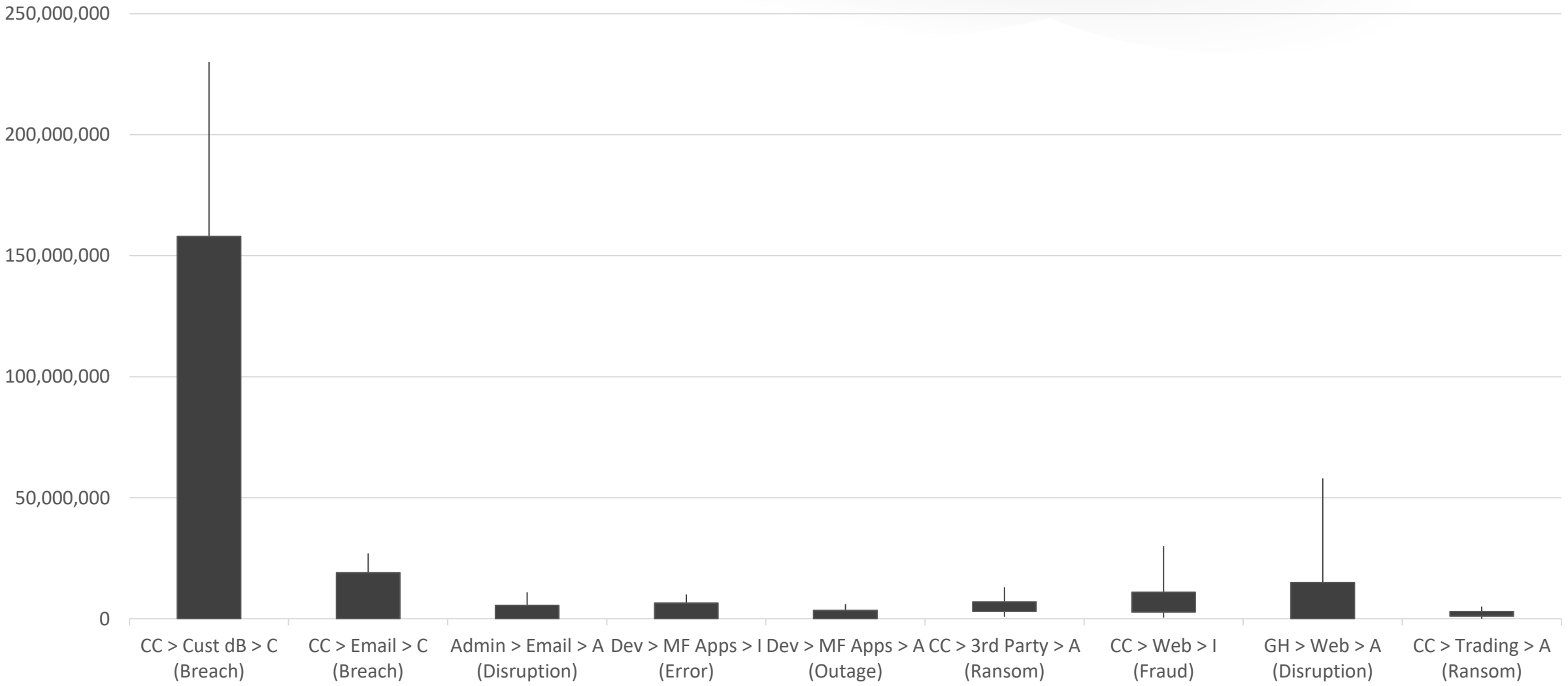
10% probability of losses greater than $160M

Event	Asset	Threat Community	Threat Type	Threat Effect	Average
Data Breach	Customer dB	Cyber Criminals	Malicious	C	$47,000,000
External Fraud	Web Platform	Cyber Criminals	Malicious	I	$6,200,000
Data Breach	Email	Cyber Criminals	Malicious	C	$5,500,000

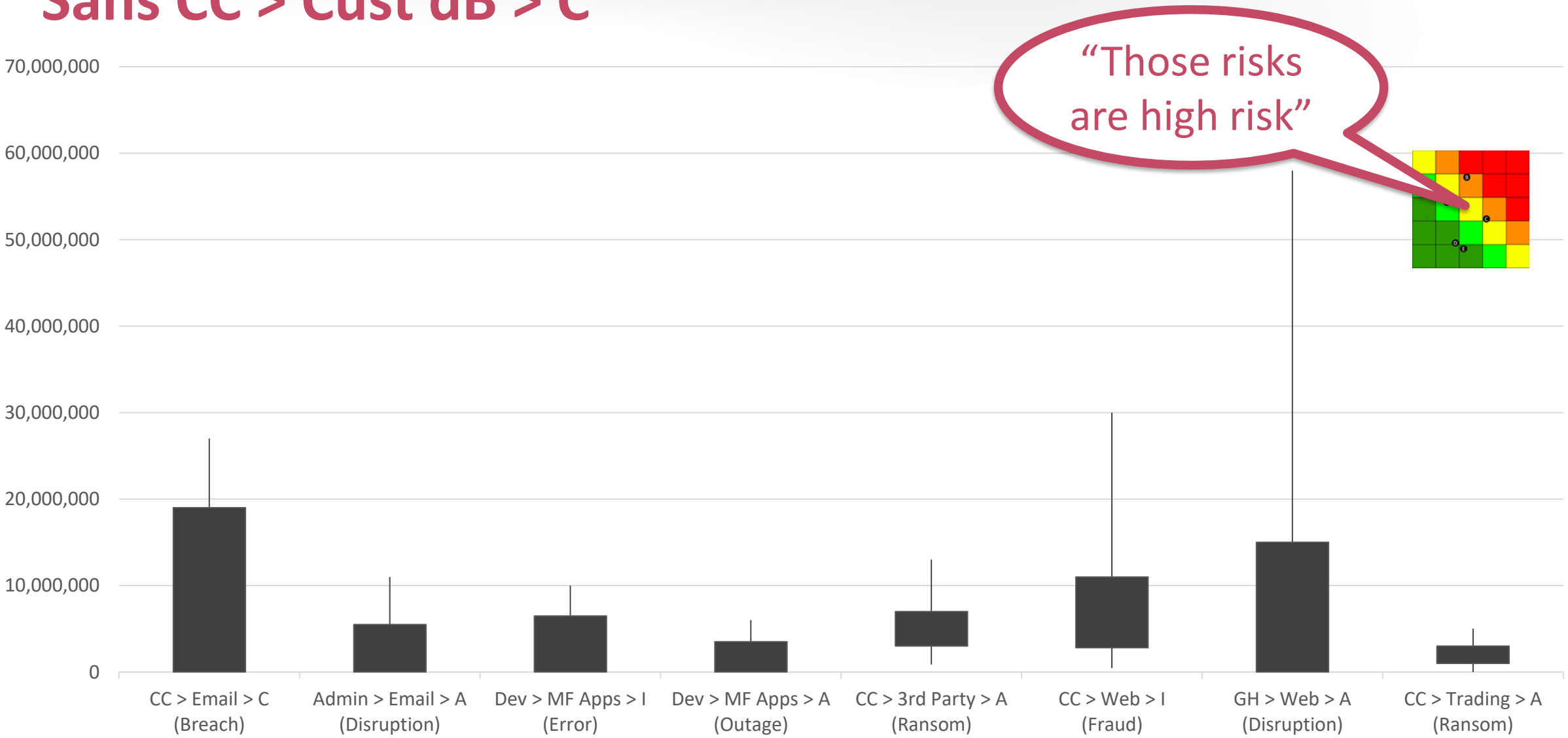
Event	Asset	Threat Community	Threat Type	Threat Effect	10th
Ransomware	3rd Party	Cyber Criminals	Malicious	A	$3,000,000
External Fraud	Web Platform	Cyber Criminals	Malicious	I	$2,800,000
Ransomware	Trading Platform	Cyber Criminals	Malicious	A	$1,000,000

90% probability of losses greater than $3M

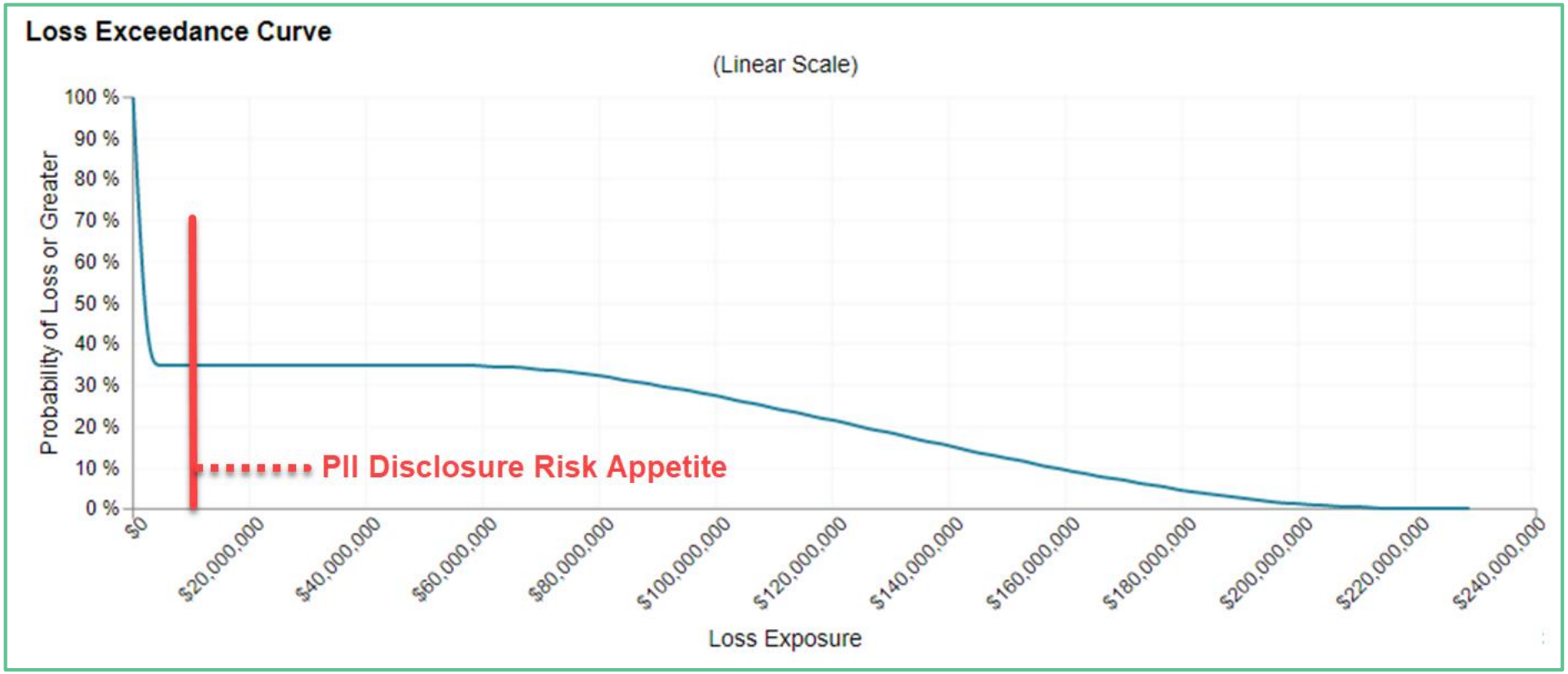
Comparing scenarios



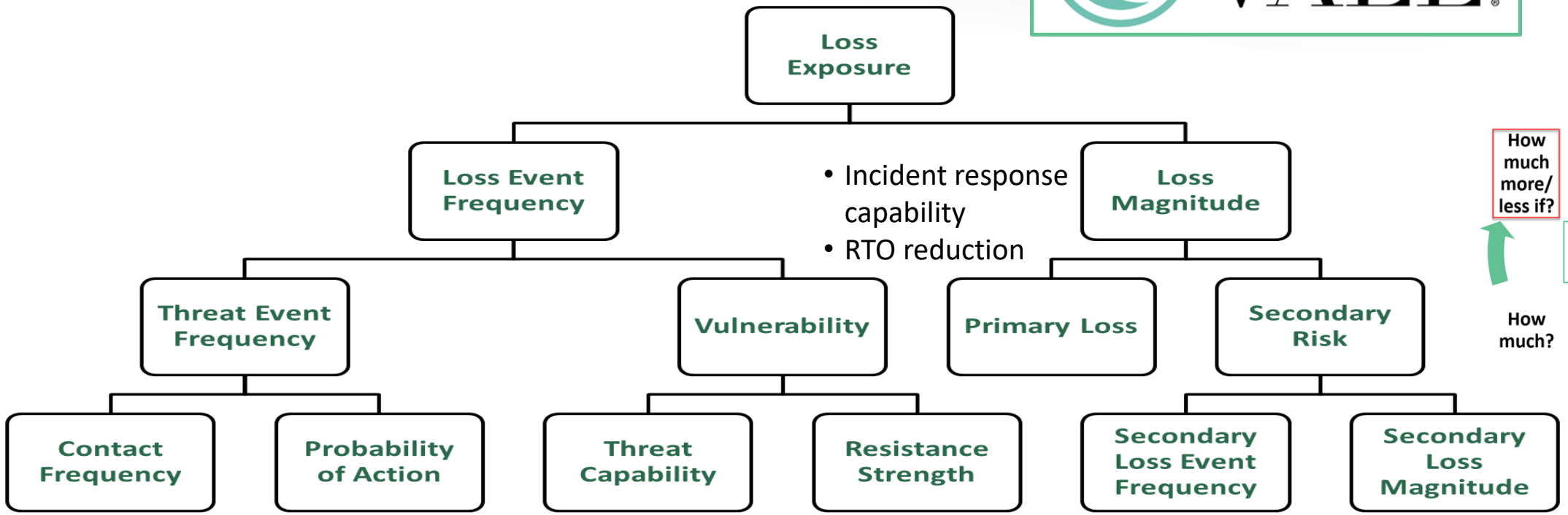
Comparing scenarios – Sans CC > Cust dB > C



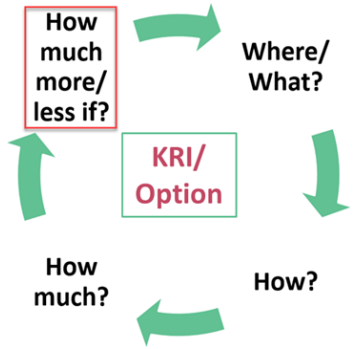
Comparison to risk appetite – CC > Cust dB > C



Trade Study Library



- Incident response capability
- RTO reduction



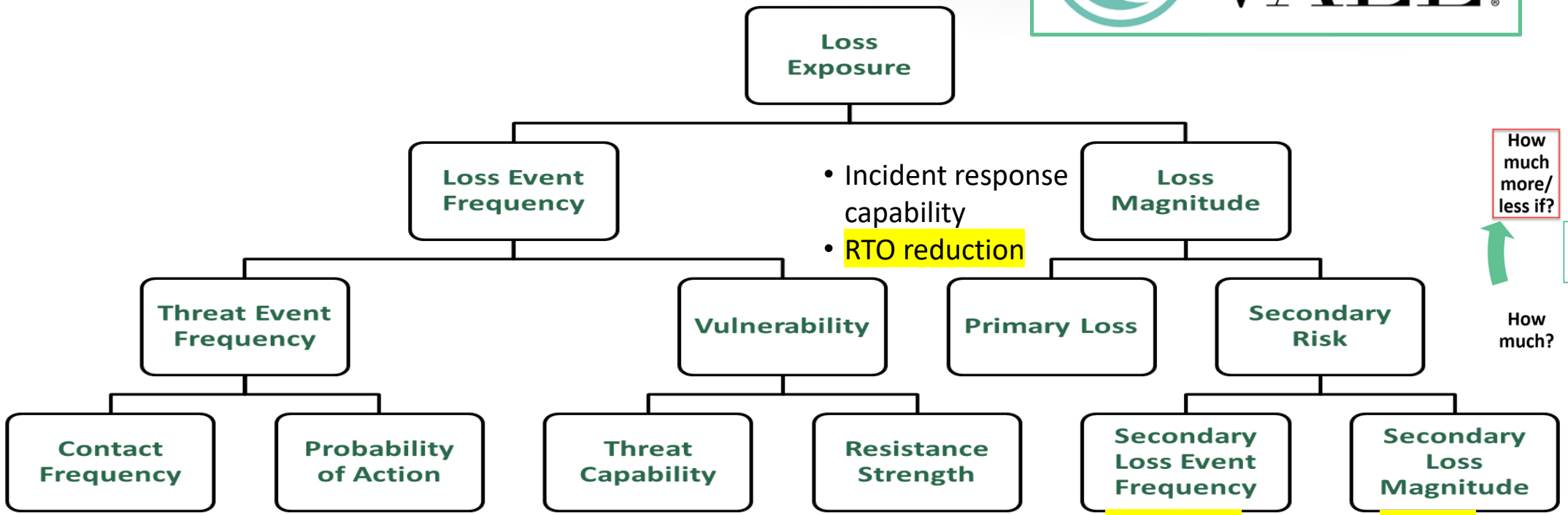
- Firewalls
- Email notification
- Simulated phishing
- Anti-fraud task force
- End point protections
- Database internalization
- Security awareness training

- UDD
- DLP Upgrade
- Traffic scrubbing
- Asset configurations
- Patching compliance
- Password compliance
- Zero Trust Architecture

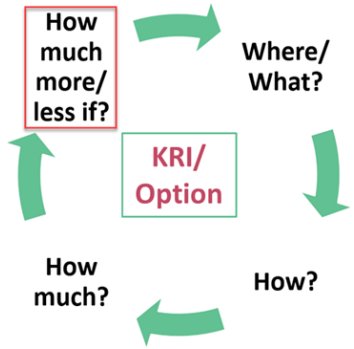
- Encryption
- Tokenization
- Forensic capability

- Purging
- SLA review
- RTO reduction
- Cyber insurance

Trade Study Candidates



- Incident response capability
- RTO reduction



- Firewalls
- Email notification
- Simulated phishing
- Anti-fraud task force
- End point protections
- Database internalization
- Security awareness training

- UDD
- DLP Upgrade
- Traffic scrubbing
- Asset configurations
- Patching compliance
- Password compliance
- Zero Trust Architecture

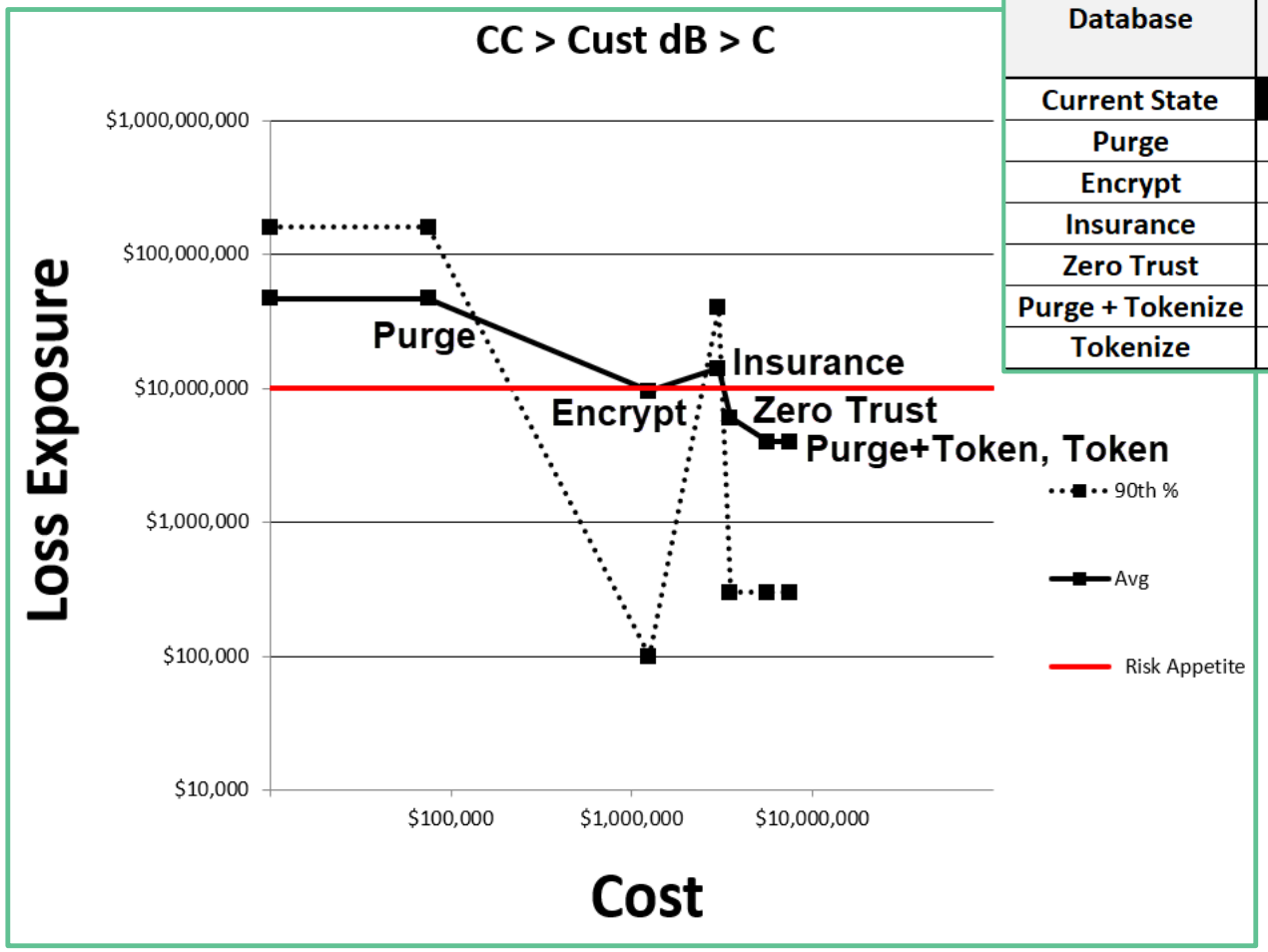
- Encryption
- Tokenization
- Forensic capability

- Purging
- SLA review
- RTO reduction
- Cyber insurance

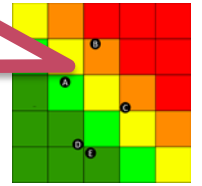
Trade Study – CC > Cust dB > C (Breach)

BANK OF THE VALE

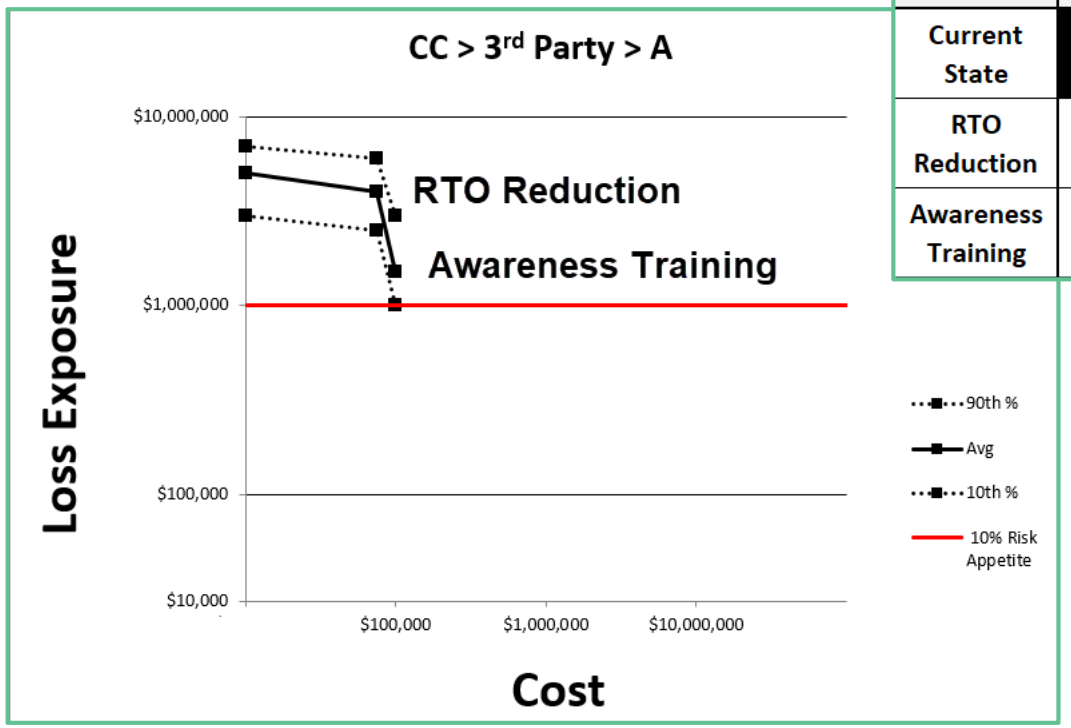
Customer Database	Project Cost Average	Project Cost 90%	Risk Factor Mod	Annualized Loss Exposure Average	Annualized Loss Exposure 90th %	Risk Reduction Benefit/ Cost Ratio
Current State				$47,000,000	$160,000,000	
Purge	$75,000	$100,000	SLM	$47,000,000	$160,000,000	0 to 1
Encrypt	$1,250,000	$2,000,000	SLEF	$9,500,000	$100,000	30 to 1
Insurance	$3,000,000	$3,000,000	SLM	$14,000,000	$40,000,000	11 to 1
Zero Trust	$3,500,000	$5,000,000	RS	$6,000,000	$300,000	12 to 1
Purge + Tokenize	$5,625,000	$7,500,000	SLEF	$4,000,000	$300,000	8 to 1
Tokenize	$7,500,000	$10,000,000	SLEF	$4,000,000	$300,000	6 to 1



"This return on control talk is beyond me… please stop showing off!"



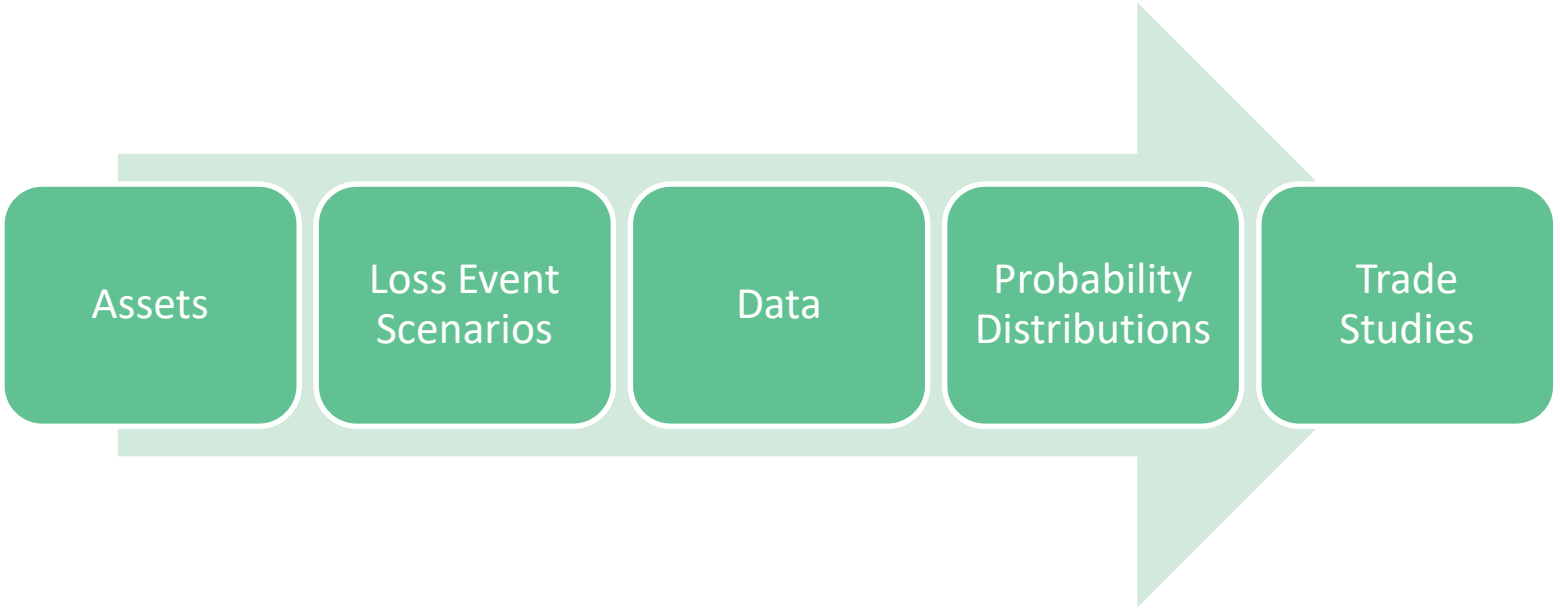
Trade Study – CC > 3rd Party > A (Ransomware)

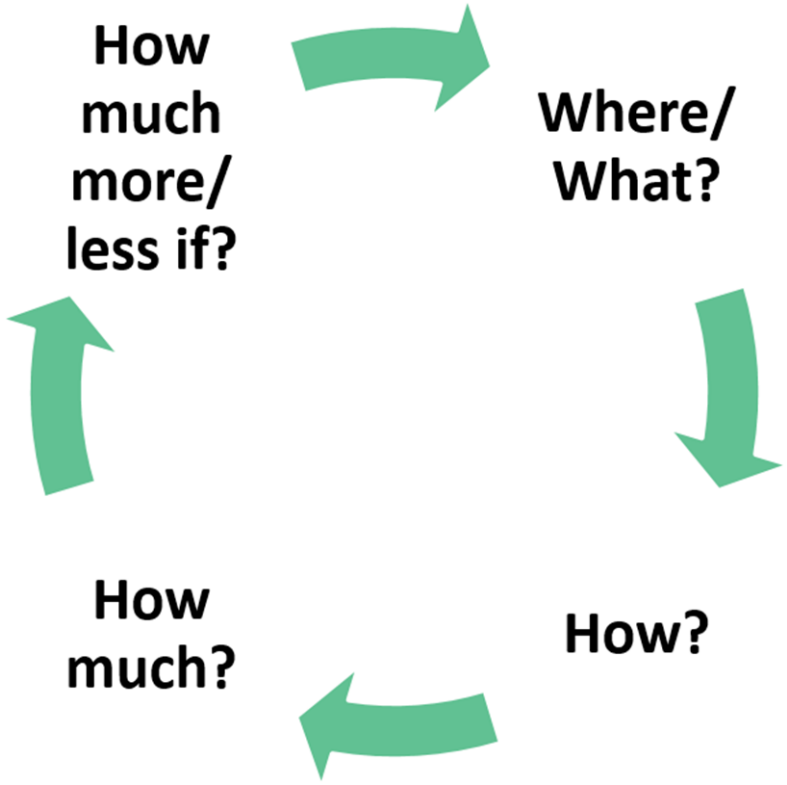


	Project Cost				Annualized Loss Exposure			
Customer Database	10%	Average	90%	Risk Factor Mod	10th %	Average	90th %	Risk Reduction Benefit/ Cost Ratio
Current State					$3,000,000	$5,000,000	$7,000,000	
RTO Reduction	$50,000	$75,000	$100,000	PL/ SLM	$2,500,000	$4,000,000	$6,000,000	13 to 1
Awareness Training	$50,000	$100,000	$200,000	CF	$1,000,000	$1,500,000	$3,000,000	35 to 1

Value with Compliance

BANK OF THE VALE





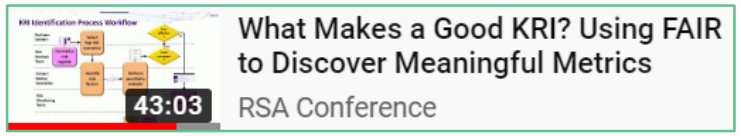
RSAConference2020

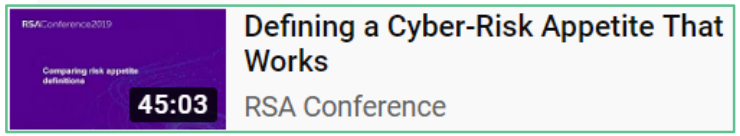
Wrapping things up

Troubleshooting your risk assessment

- **No one seems to care**
  - Have you tossed the heat map? Still calling findings risk?
  - Is cyber risk represented as a probability distribution?
  - Are decision makers seeing a variety of vetted risk response options?
- **No idea what to do next**
  - Have you mapped assets? What's the loss event scenario?
  - Are factors of frequency and magnitude documented?
  - Did you revisit the loss event scenario?
- **Not used for a strategic decision**
  - Are you comparing cost vs. risk reduction benefit?
  - Is there demand for this approach?
  - Is your team ready to jump into the decision-making process?
- **Cannot aggregate assessments**
  - Is there an enterprise loss event taxonomy?
  - Are quantitative ranges estimated before qualitative reporting labels?

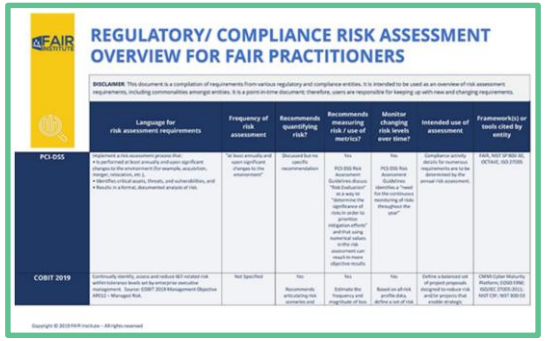
Resources for further study and engagement

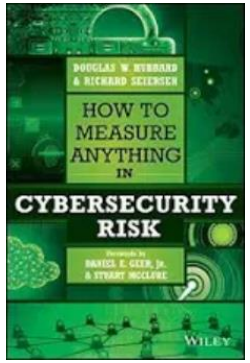


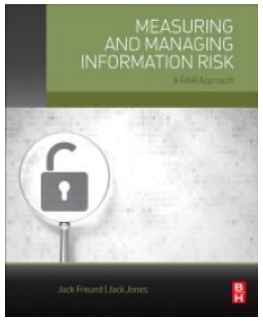


How much more/ less if?

Where/ What?

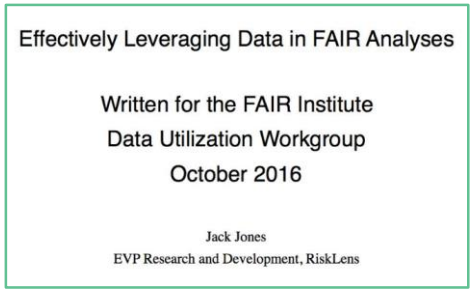


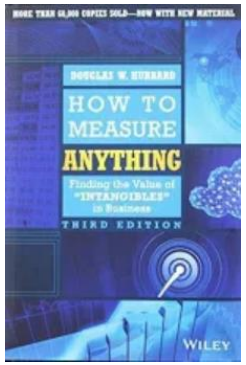




How much?

How?





FAIR INSTITUTE

Recap

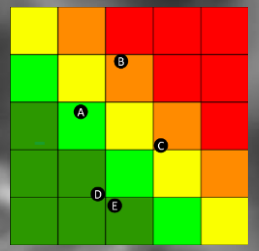
Your risk assessment procedure should include…	• **Steps for “Where/What?”, “How?”, “How much?”, “How much more/less if?”** • **Mapping to external requirements**
Your risk assessment report should include…	• **Answers to “Where/What?”, “How?”, “How much?”, “How much more/less if?”** • **How meets external requirements**
Now you can…	• **Better assign resources & prioritize budget** • **Provide value with compliance**

RSAConference2020

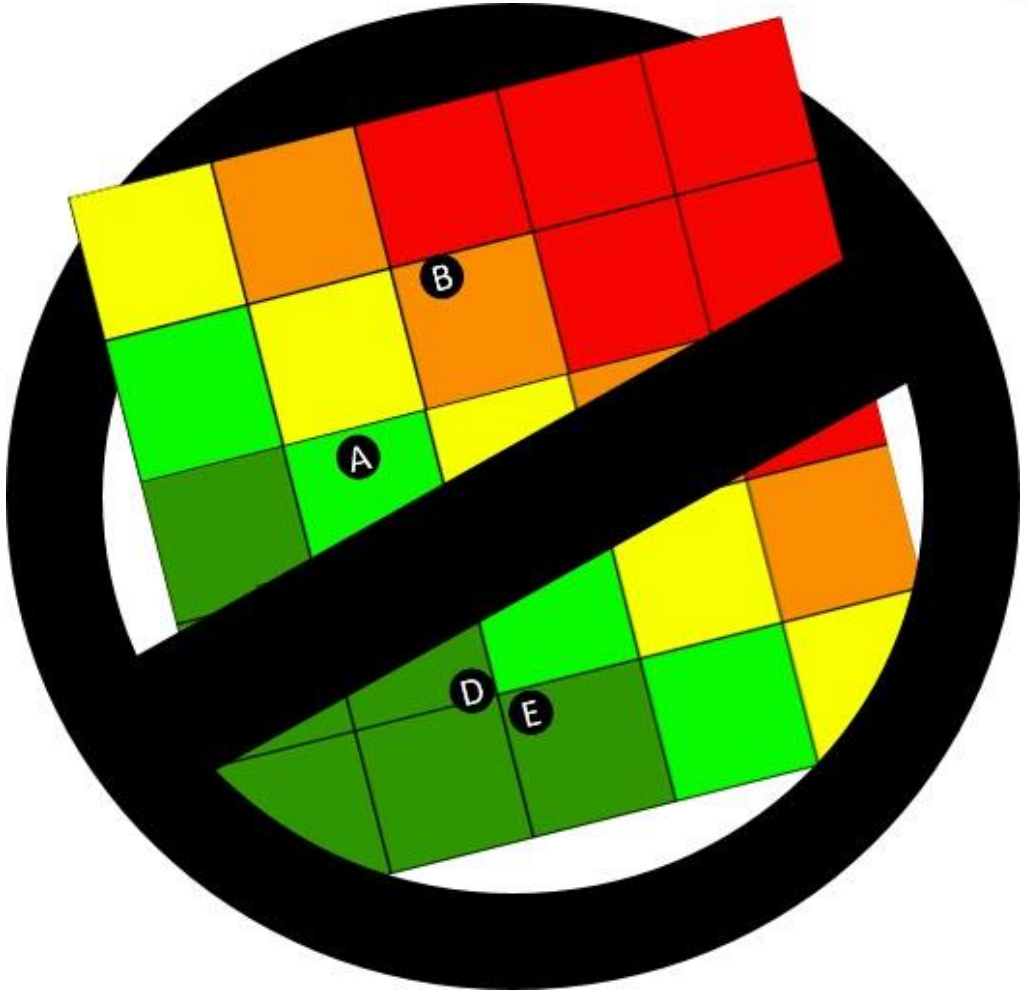
Applying what you've learned

Apply it

By next month…	• **Identify critical assets and their value** • **Document loss event factors** • **Identify external requirements**
By summer vacation…	• **“Shop” for data** • **Analyze loss event factors and response options** • **Map to external requirements**
Before end of year…	• **Expand scope**

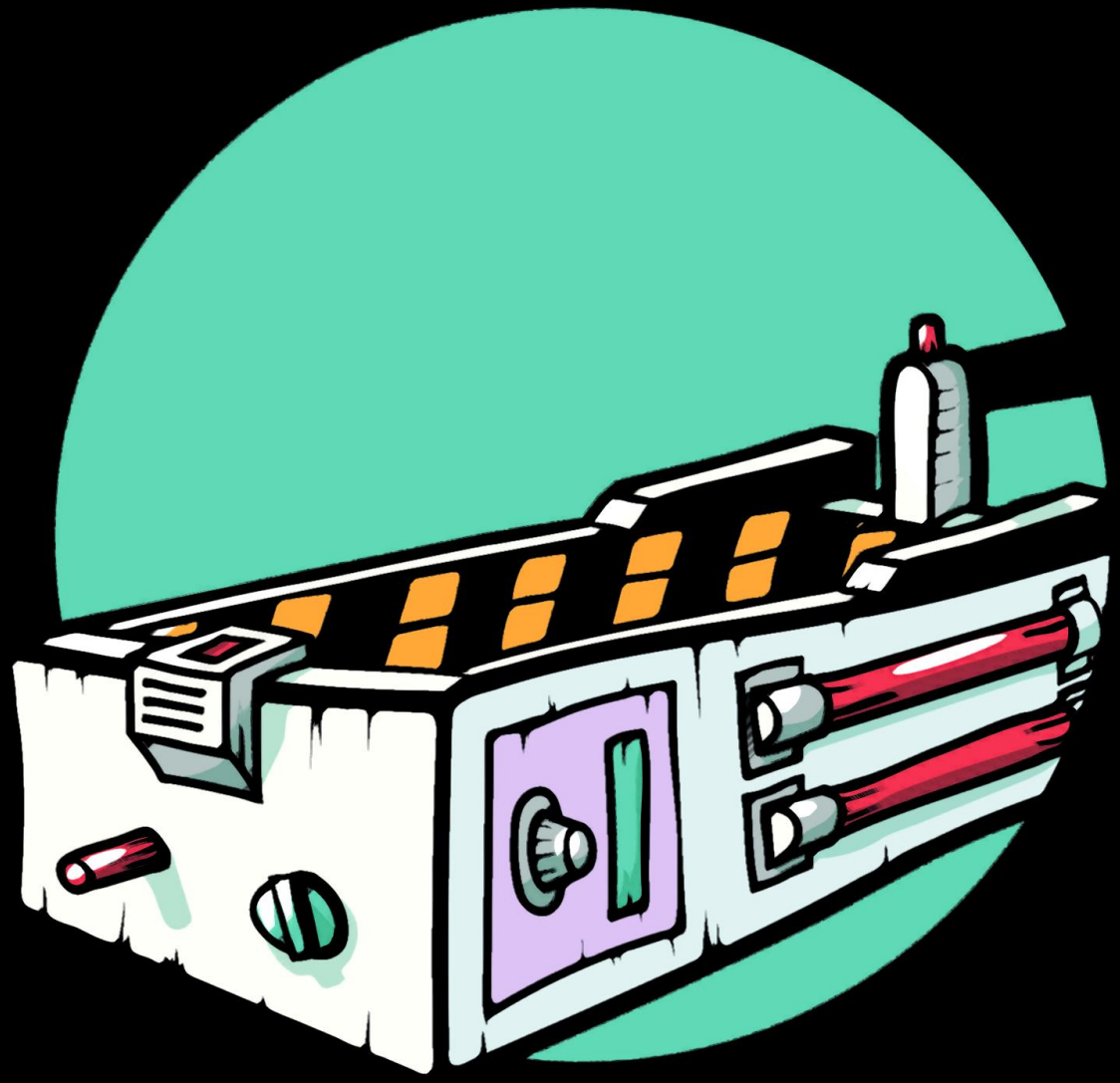

A
B
C
D
E

“I ain’t afraid of no ghost!”




FUD, FUD, FUD,
FUD, FUD, FUD,
FUD, FUD...

What’s in your risk assessment?



RSAConference2020

Q&A