RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: **GRC-R02**

What makes a good KRI? Using FAIR to discover meaningful metrics

Steve Reznik

Director, Operational Risk Management
ADP

Metrics

Love them!

"Without data, you are just another person with an opinion"

W. Edwards Deming

… or hate them?

Why stay?

- FAIR-based approach to better metrics
- Process workflow
- Case studies

RSAConference2019

Poll Question: Do your metrics indicate risk?

Poll the Audience

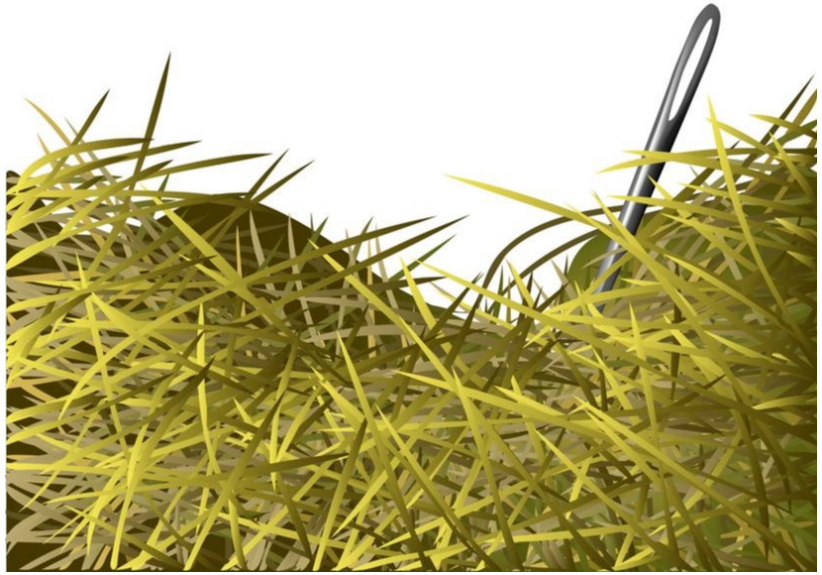
- GRC-R02
- Do your metrics indicate risk?
  - Yes
  - No
  - Maybe
- https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3860

Where's the risk?

- Inappropriate access privileges
- Absence of patching
- Disgruntled insiders
- Wireless access points
- Data breach
- Lack of user awareness
- Reputation damage
- Regulatory compliance
- Web applications

Which ones are:

- Objectives/requirements?
- Threats?
- Assets?
- Control deficiencies?
- Scenarios/events?
- Outcomes?



Where's the risk?

- Inappropriate access privileges
- Absence of patching
- Disgruntled insiders
- Wireless access points
- Data breach
- Lack of user awareness
- Reputation damage
- Regulatory compliance
- Web applications

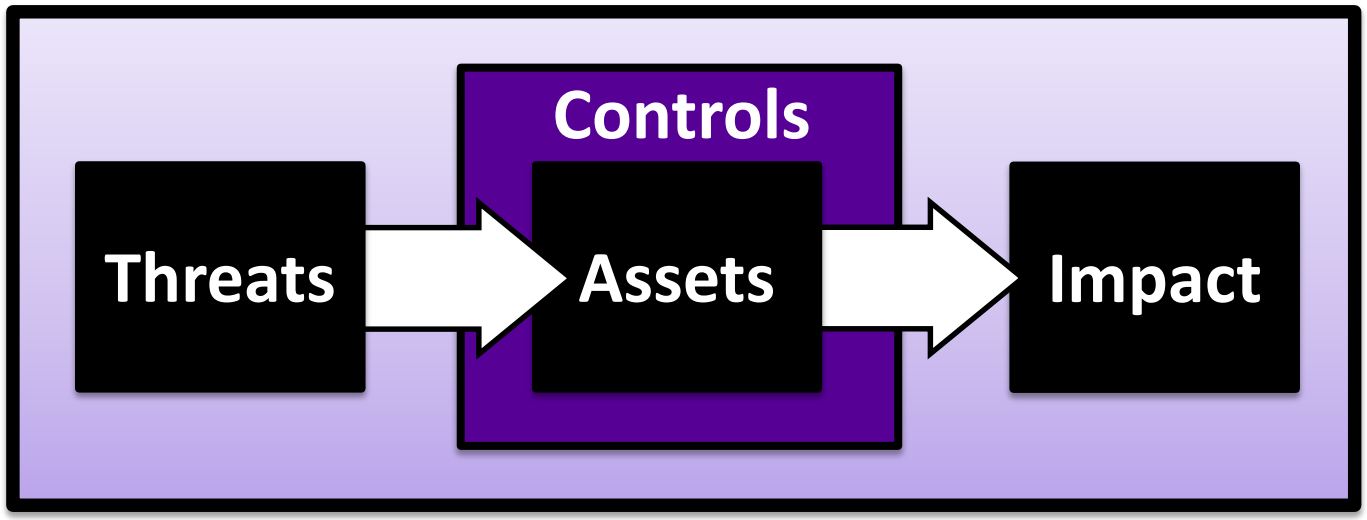
Which ones are:

- Objectives/requirements?
- Threats?
- Assets?
- Control deficiencies?
- Scenarios/events?
- Outcomes?

Courtesy of Robert Stroud

Risk is…

- The probable frequency and probable magnitude of future loss associated with a specific event
- The way in which possible losses may materialize are articulated in risk scenarios describing the action of a threat onto an asset of value and the resulting effect



Where's the risk *indicator*?

- Policy acknowledgements (%)
- Security alerts (#)
- Unpatched servers (#)
- Audited vendors (%)
- Incident response cost ($)
- Records breached (#)
- Application test time (Hrs)
- Open audit findings (#)
- NIST CSF efficacy level (1 –> 5)
- FICO Score (300 –> 850)

Which ones indicate:

- Performance?
- Control?
- Compliance?
- Risk? *Does it affect loss exposure?*

Where's the risk *indicator*?

- Policy acknowledgements (%)
- Security alerts (#)
- Unpatched servers (#)
- Audited vendors (%)
- Incident response cost ($)
- Records breached (#)
- Application test time (Hrs)
- Open audit findings (#)
- NIST CSF efficacy level (1 –> 5)
- FICO Score (300 –> 850)

Which ones indicate:

- Performance?
- Control?
- Compliance?
- Risk? *Does it affect loss exposure?*

Courtesy of Robert Stroud

Key Risk Indicator

Of crucial importance*

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

A gauge or meter of a specified kind*

*Source: Oxford Dictionary

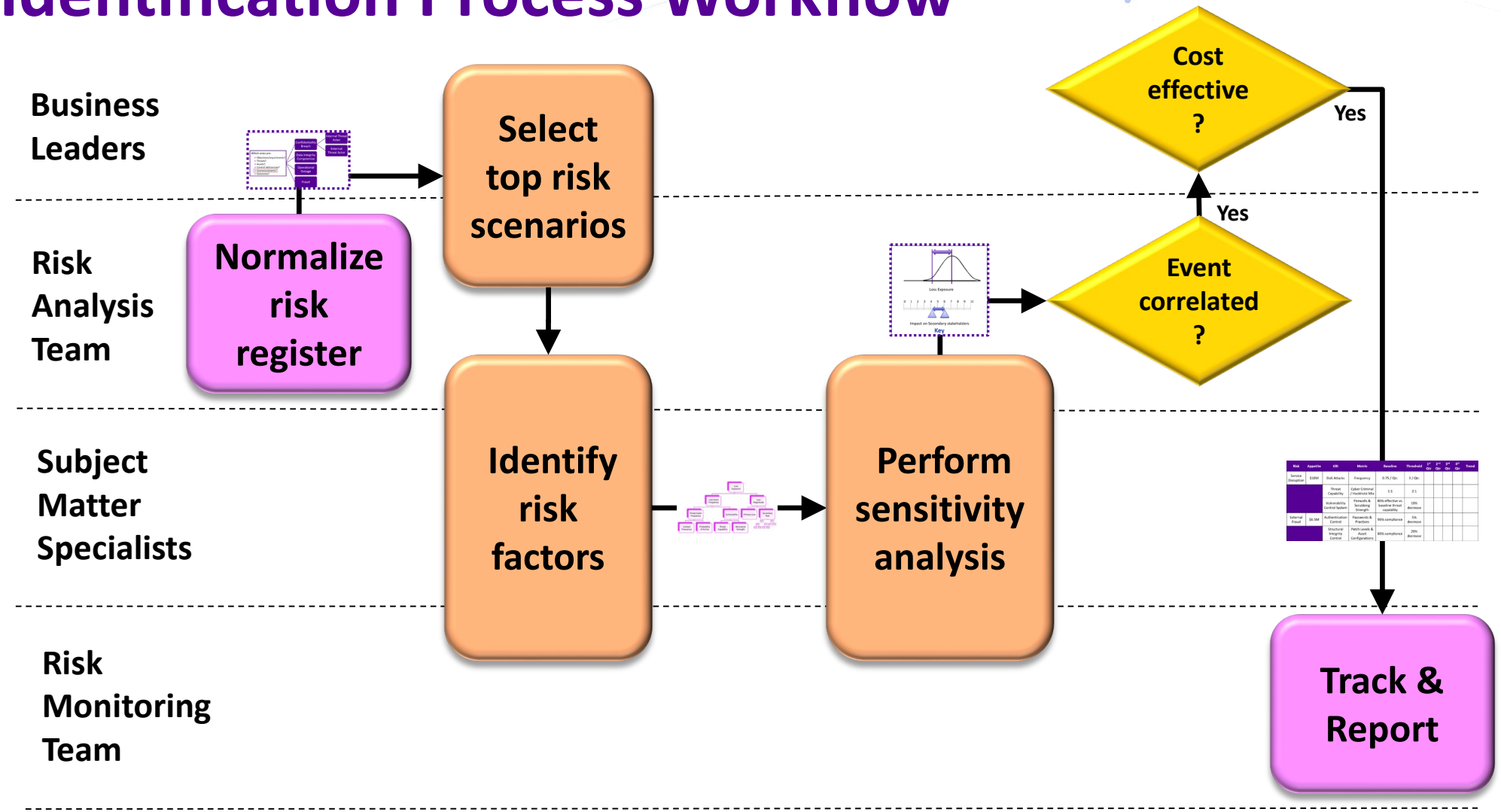
What makes a BETTER metric?

Traditional Candidates	Loss Event	Risk Factor	Loss Exposure Leverage	Cost to Measure & Report
Policy acknowledgements (%)				
Security alerts (#)	Various	TEF?		
Unpatched servers (#)		RS		$
Audited vendors (%)				
Incident response cost ($)	Various	PLM	CASE STUDIES WILL LOOK AT	$
Records breached (#)	Data Breach	PLM		
Application test time (Hrs)				
Open audit findings (#)				¢
NIST CSF efficacy level (1-5)				$$

RSAConference2019

Now, let's dig in!

KRI Identification Process Workflow



Normalize Risk Register

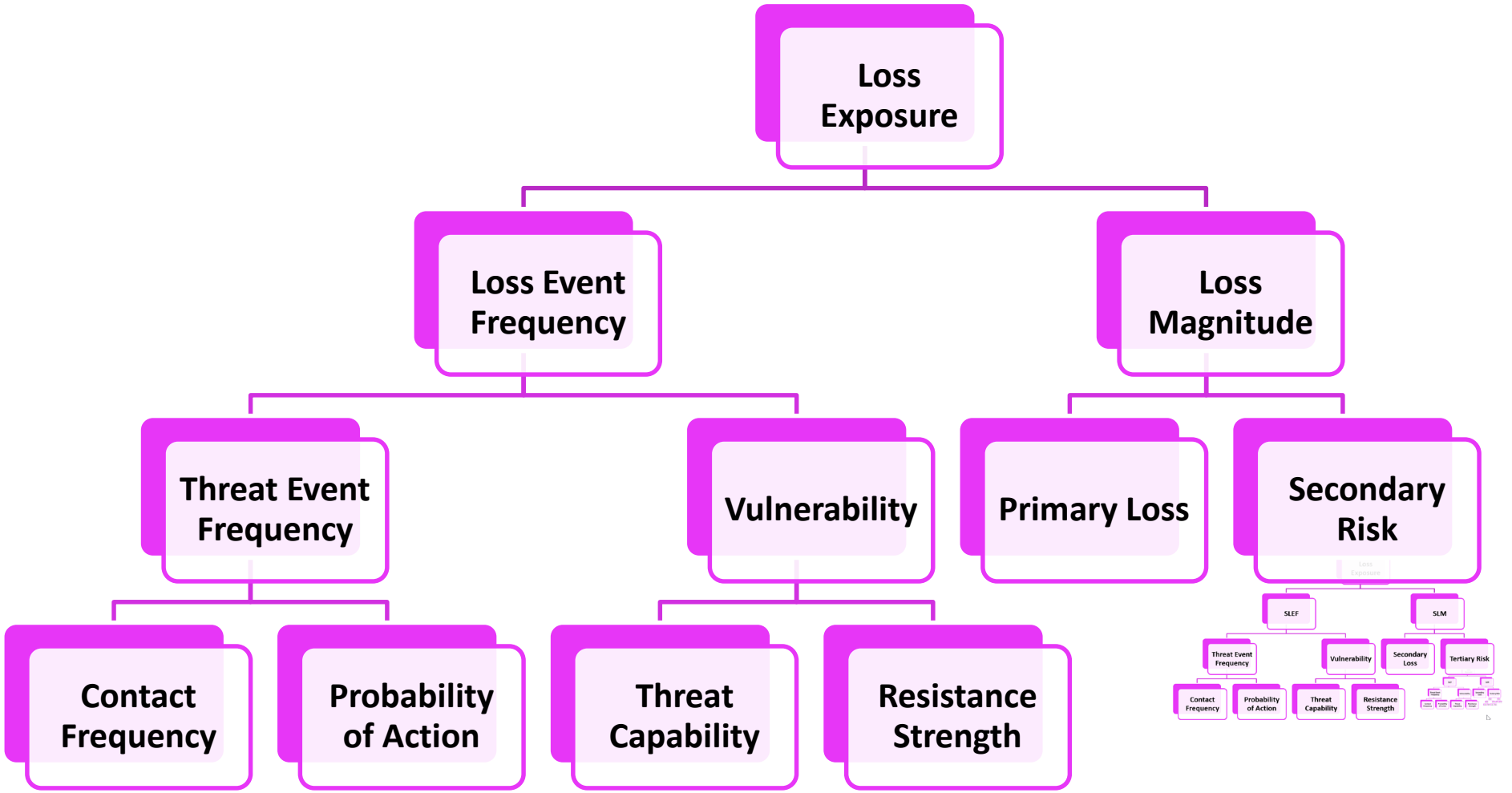
Which ones are:

- Objectives/requirements?
- Threats?
- Assets?
- Control deficiencies?
- Scenarios/events?
- Outcomes?

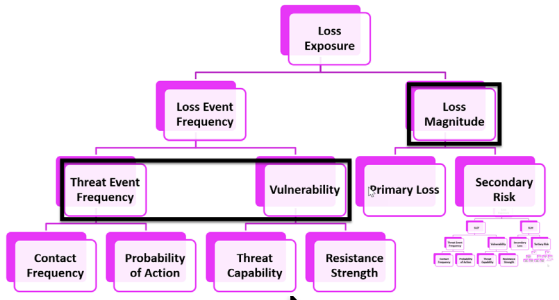
- Data Breach
  - Internal Threat Actor
    - Accidental
    - Malicious
  - External Threat Actor
- Financial Misstatement
- Service Disruption
- External Fraud

"Those are my top two…let me know how you plan to monitor"

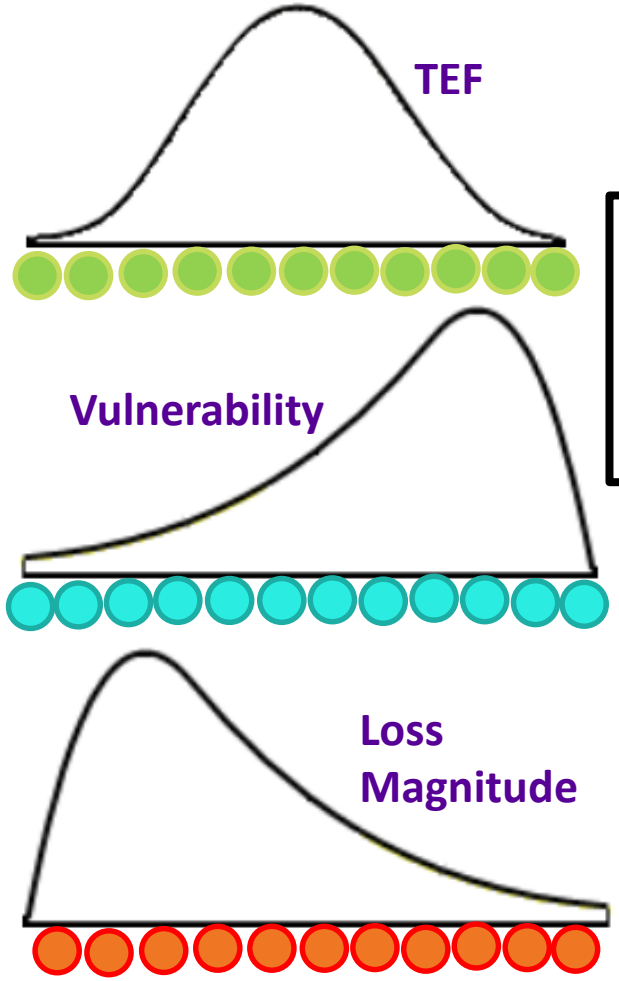
Identify Risk Factors



Risk Factors in Action – Monte Carlo Illustration



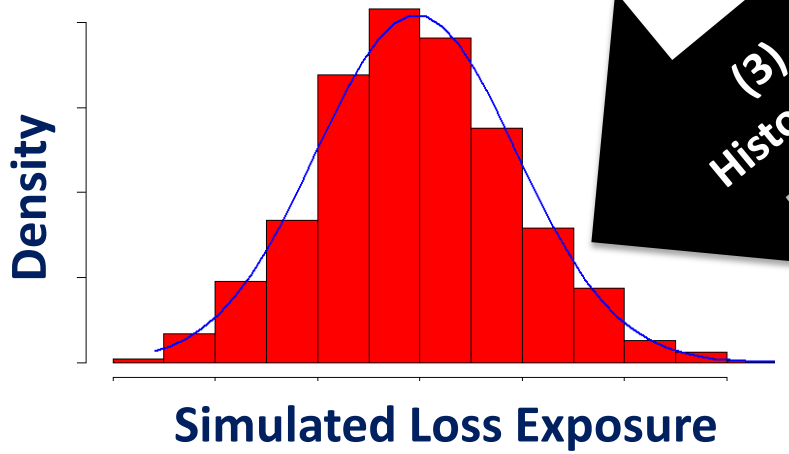
(1) Risk Factor Distributions



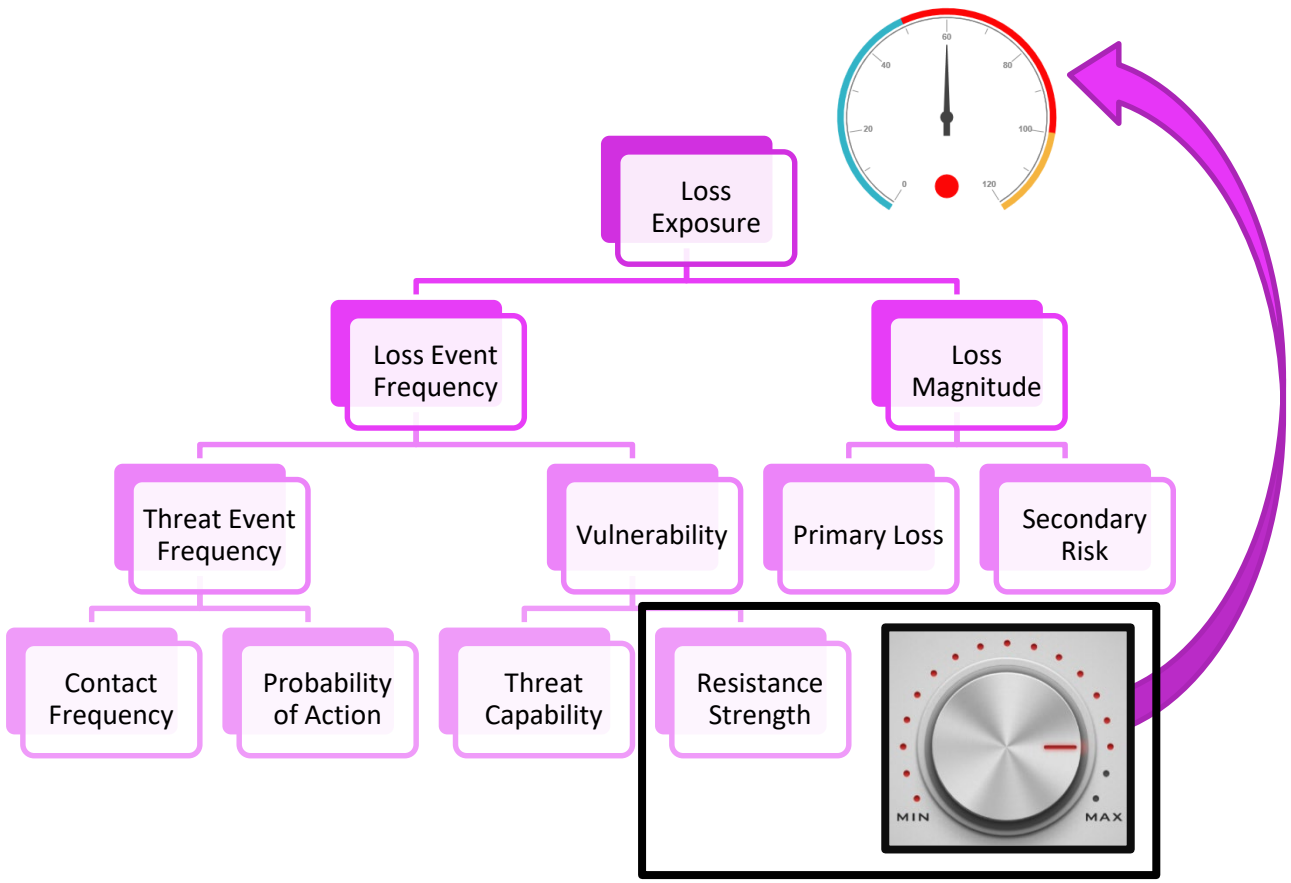
Random Numbers

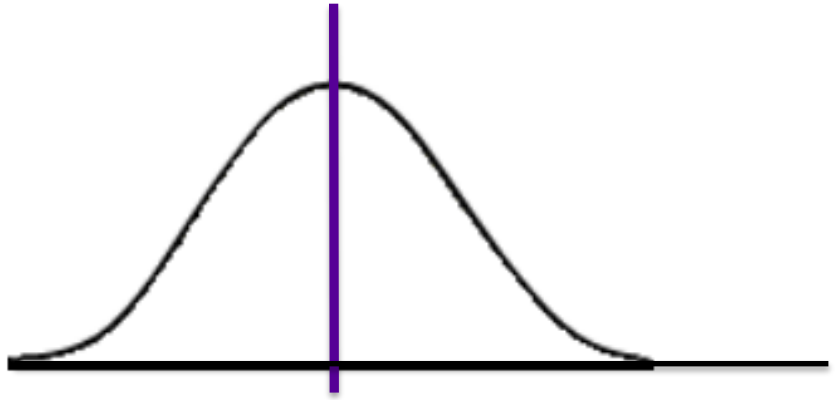
(2) Calculations *(Frequency * Magnitude)*

(3) Histogram

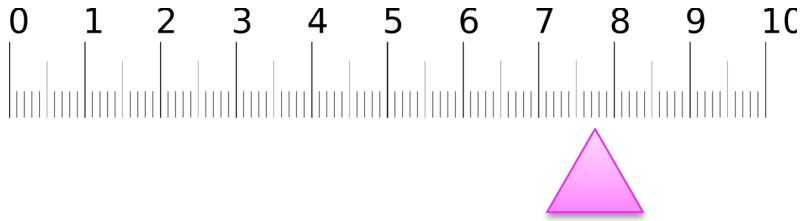


From Risk Factor to Risk Indicator



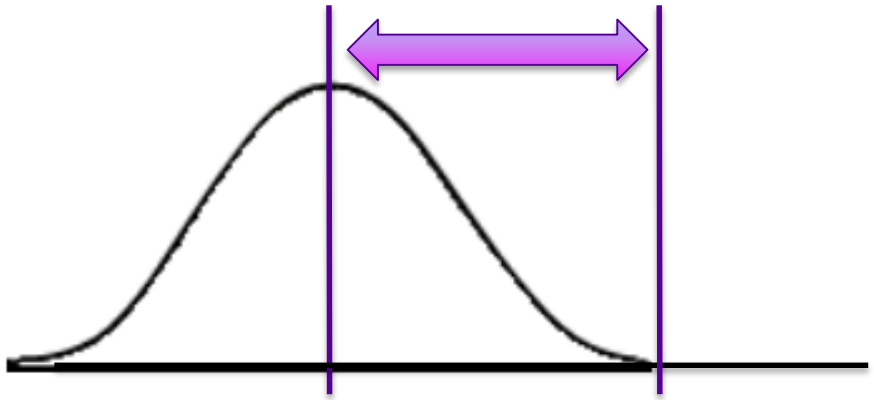


Loss Exposure

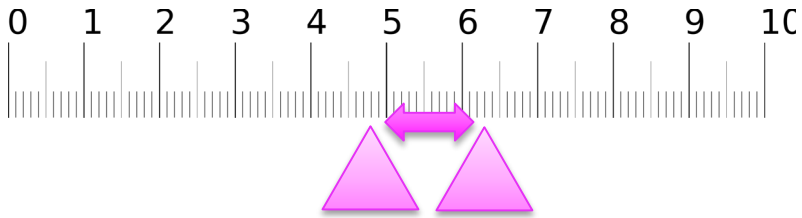


Resistance Strength

From Risk Indicator to *Key* Risk Indicator

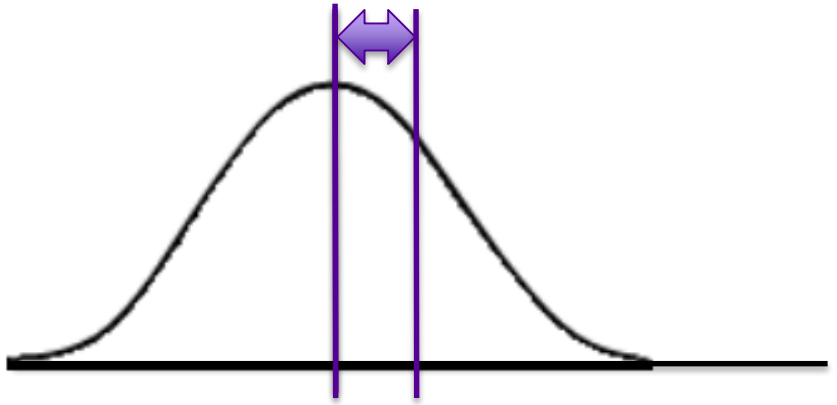


Loss Exposure

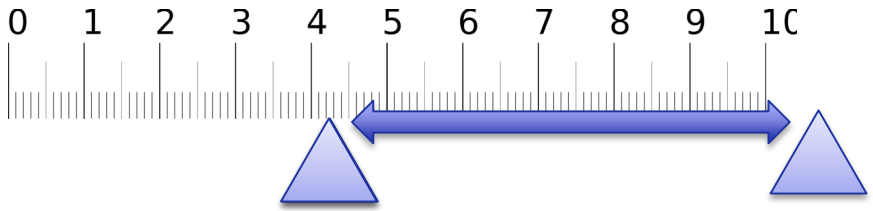


Resistance Strength

Key



Loss Exposure

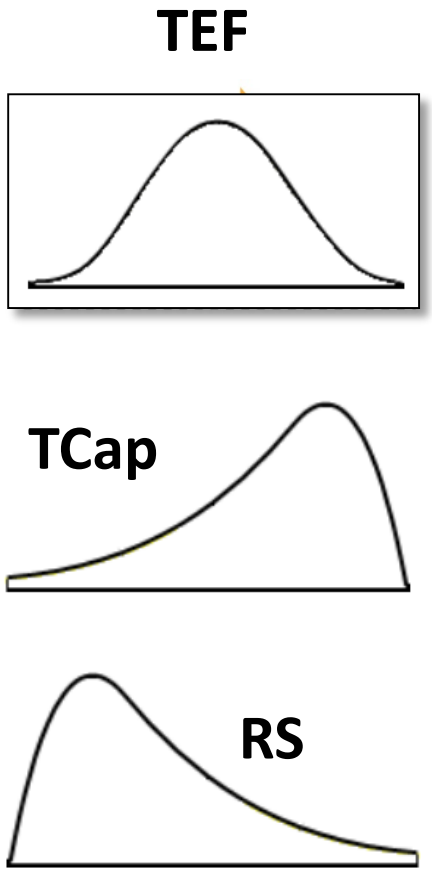


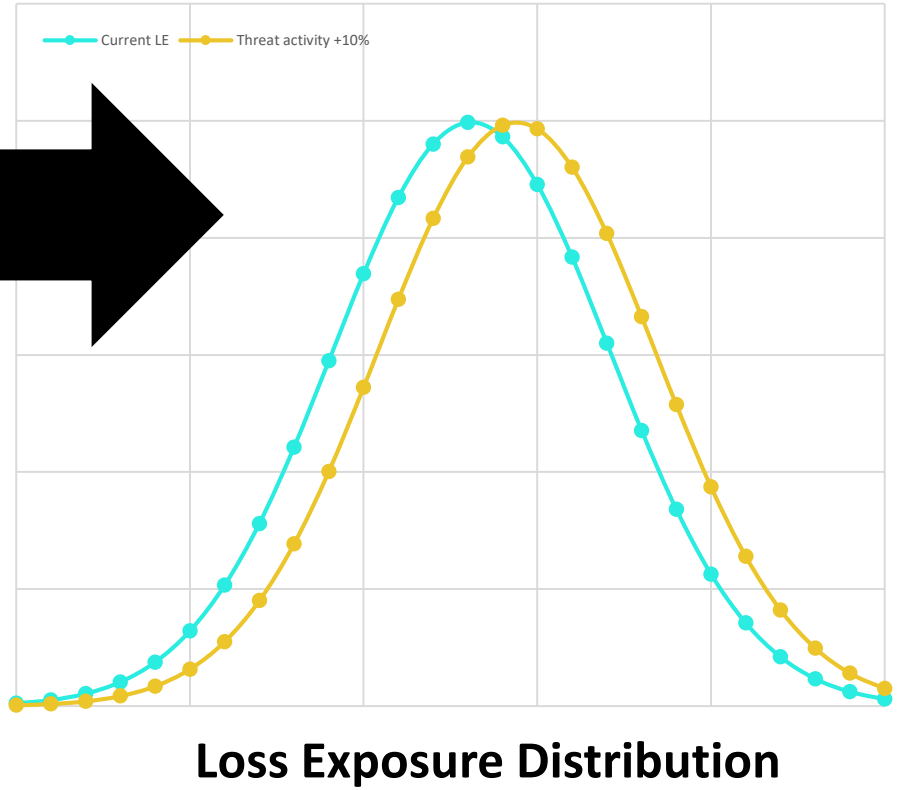
Primary Loss Magnitude

Not Key

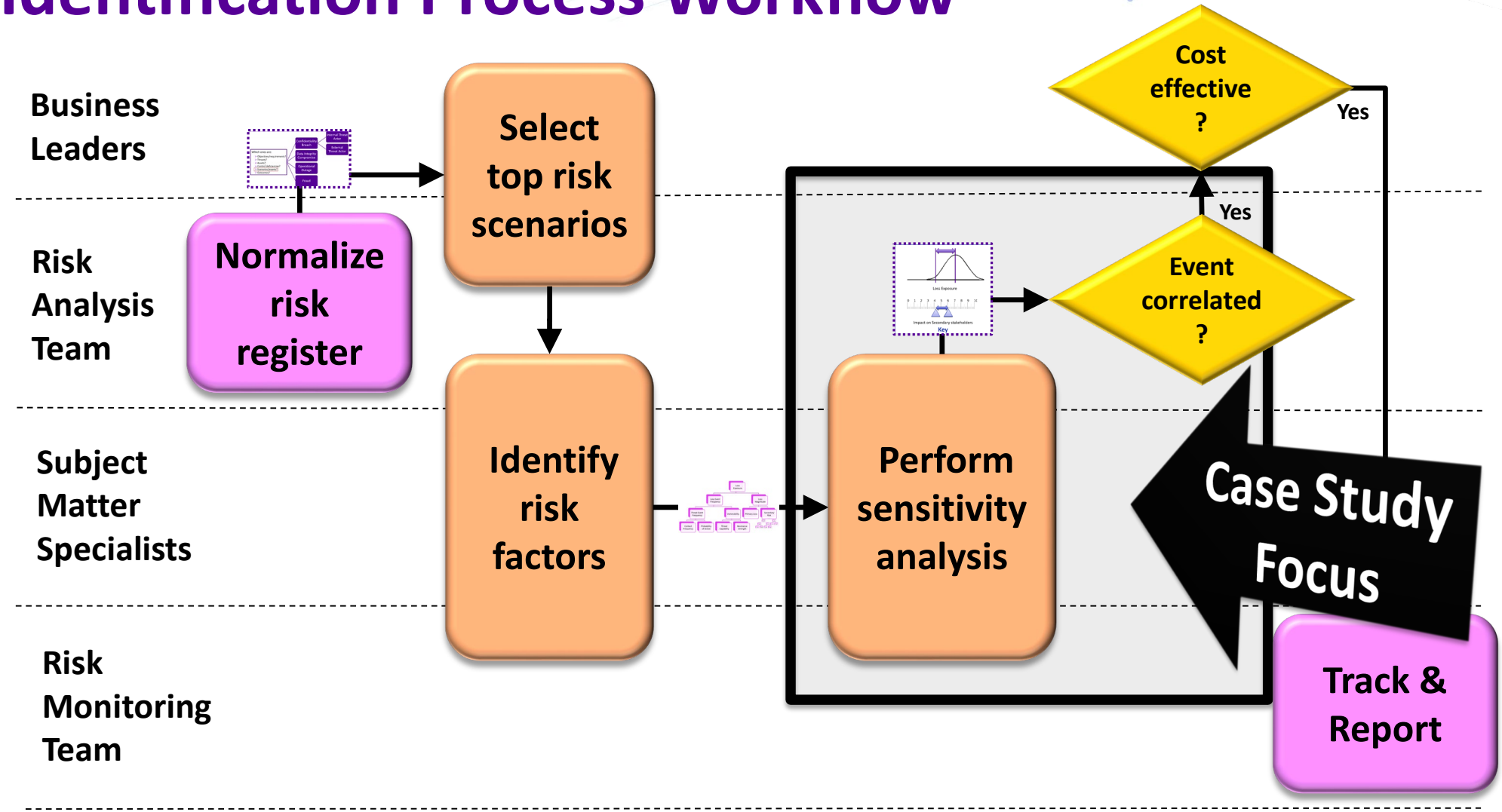
Perform Sensitivity Analysis

1) Choose Factor
2) Change It
3) Observe LE
4) Reset Factor
5) Repeat
6) Compare Leverage



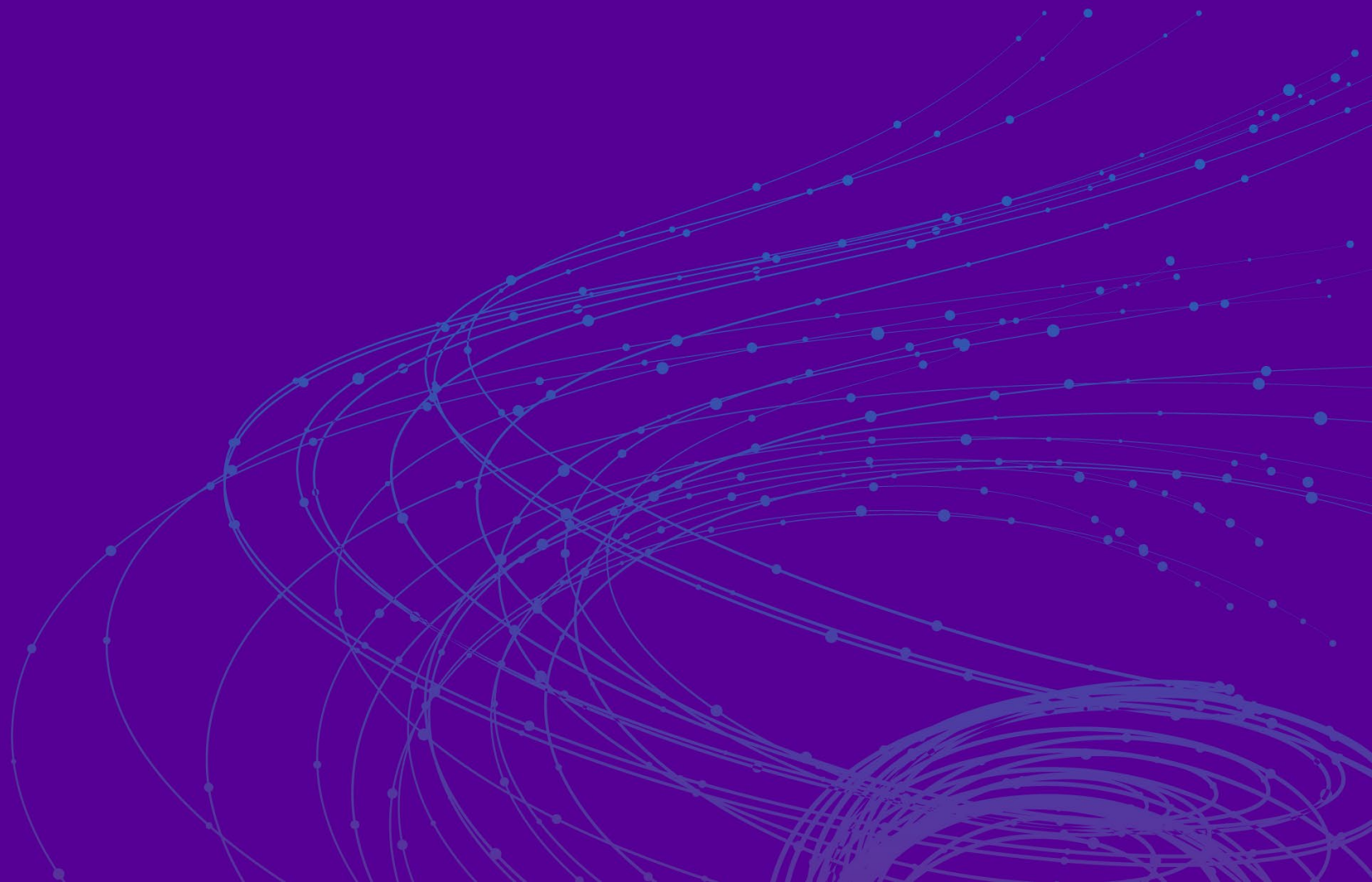


KRI Identification Process Workflow



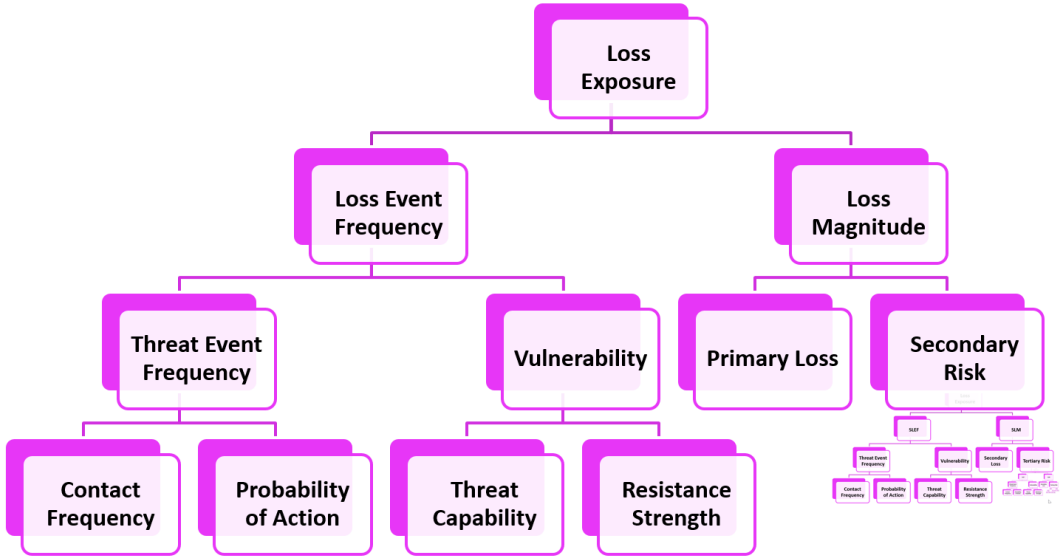
RSAConference2019

Case Study 1



Case Study 1 – Introduction

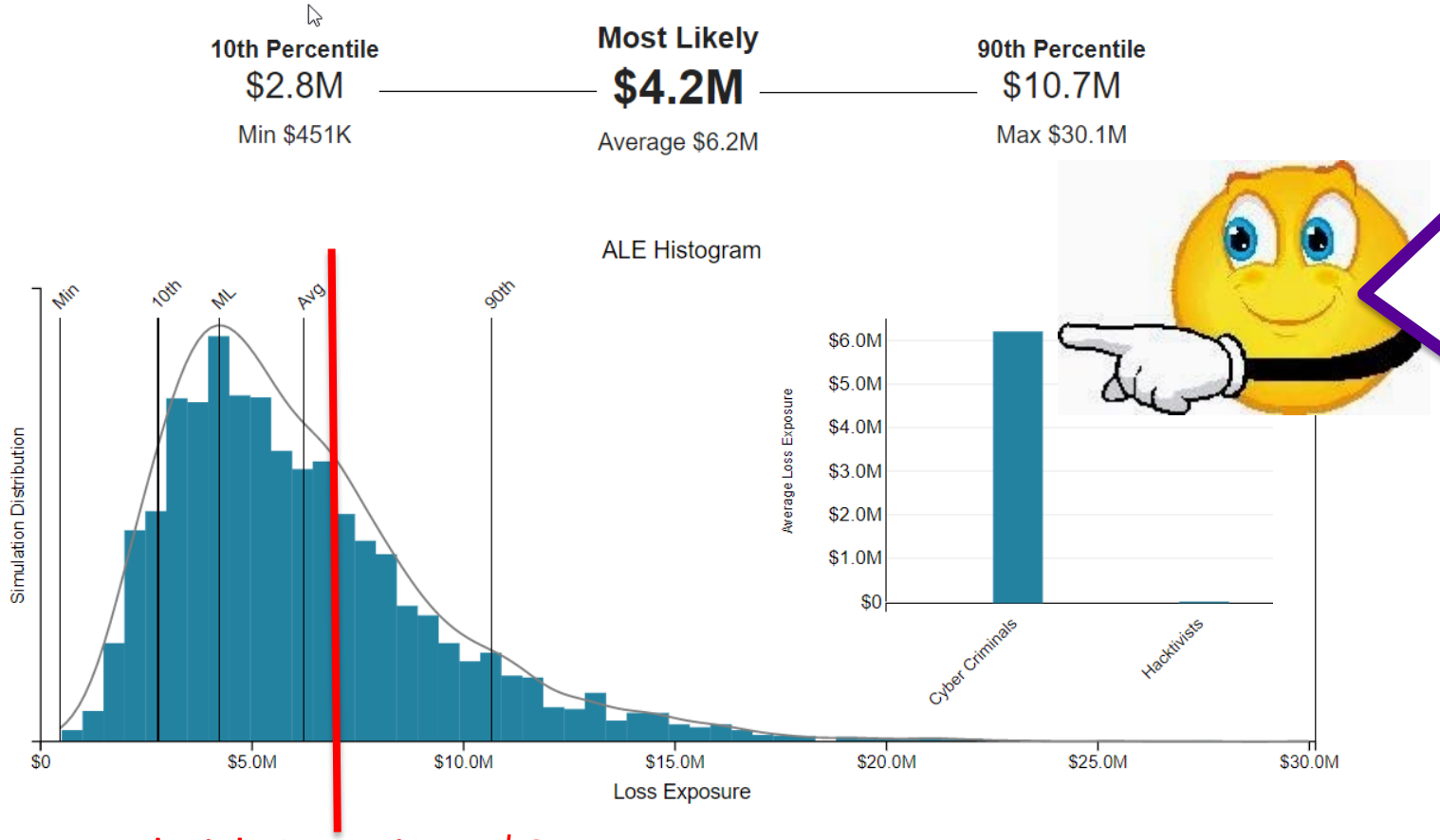
Risk Scenario: External Fraud



Risk Factor Components			Min	Most Likely	Max
Loss Event Frequency	TEF (#)	Cyber Criminals	6,000	7,000	10,000
		General Hacking Community	1,000	1,150	2,000
		Hacktivists	0	15	100
	TCap (%)	Cyber Criminals	60	75	99
		General Hacking	20	50	80
		Hacktivists	25	60	90
	Resistance Strength* (%)		0--80	25--85	50--90
Primary Loss Magnitude	Replacement Cost ($)		0	900	1,800
	Response Hours (#)		1	4	7
Secondary Risk	SLEF (%)		0	0.5	1
	Reputation Damage ($)		0	1M	5M

* Varies across five vulnerability control components

Case Study 1 – Baseline Estimate



Fraud Risk Appetite = $6.5M

"I see that cyber criminals are our top threat…now what factors, as they change, could indicate a fraud risk appetite violation, i.e., a 50% increase in loss exposure?"

Case Study 1 – Choose Factor, Change It, Observe LE

Risk Factor Components			Min	Most Likely	Max
Loss Event Frequency	TEF (#)	Cyber Criminals	6,000	7,000	10,000
		General Hacking Community	1,000	1,150	2,000
		Hacktivists	0	15	100
	TCap (%)	Cyber Criminals	60	75	99
		General Hacking	20	50	80
		Hacktivists	25	60	90
	Resistance Strength* (%)		0--80	25--85	50--90
Primary Loss Magnitude	Replacement Cost ($)		0	900	1,800
	Response Hours (#)		1	4	7
Secondary Risk	SLEF (%)		0	0.5	1
	Reputation Damage ($)		0	1M	5M

Resistance Strength – Vulnerability Control Component #3					
When authentication control degrades by…	20%	10%	5%	1%	0%
Loss exposure increases by…	395%	176%	79%	17%	0%
Loss Exposure	$20.8M	$11.6M	$7.5M	$4.9M	$4.2M

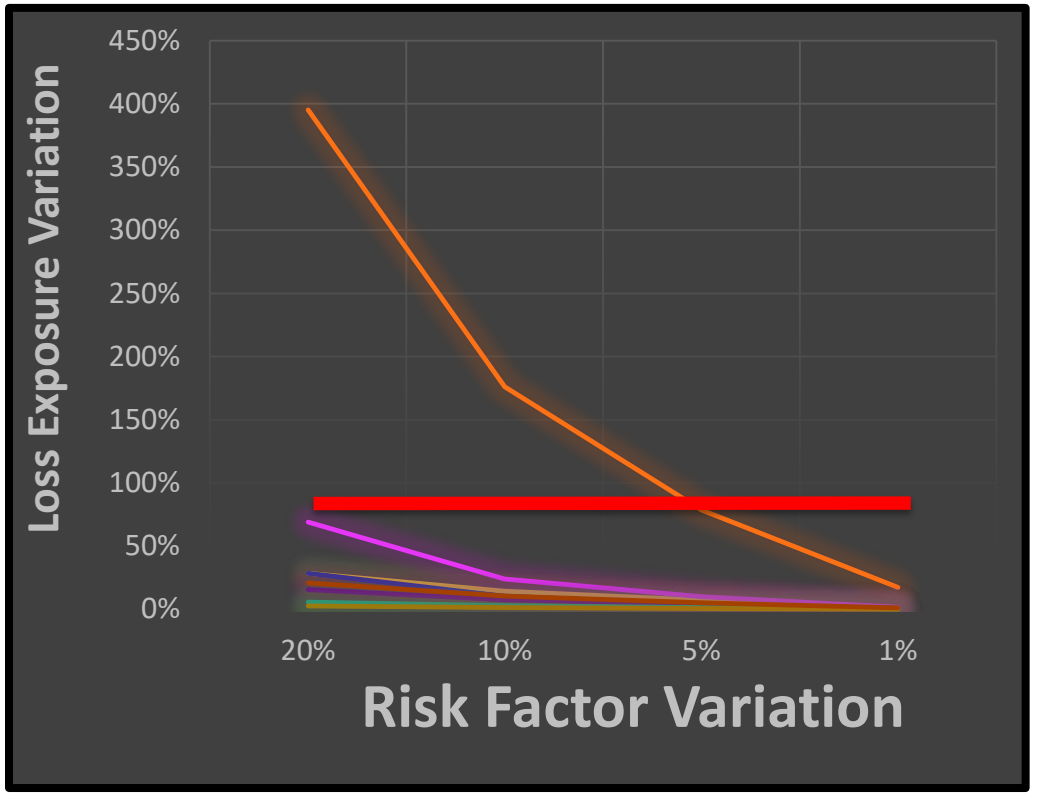
Fraud Risk Appetite = $6.5M

Case Study 1 – Reset Factor, Repeat, Compare Leverage

External Fraud Risk Factor Component	RFC Change	Loss Exposure Change	Leverage
RS – Authentication Control	5%	79%	1:16
RS – Structural Integrity Control		10%	1:2
TEF – Cyber Criminals		7%	1:1
SLM – Reputation Damage		5%	1:1

Case Study 1 – Compare Leverage Graph

Risk Factor – Component	20%	10%	5%	1%
TEF – Cyber Criminals	29%	14%	7%	1%
	5.4M	4.8M	4.5M	4.2M
RS – Authentication Strength	16%	8%	4%	1%
	4.9M	4.5M	4.4M	4.2M
RS – Structural Integrity	29%	10%	4%	1%
	5.4M	4.6M	4.4M	4.2M
RS – Authentication Control	395%	176%	79%	17%
	20.8M	11.6M	7.5M	4.9M
RS – Structural Integrity Control	69%	24%	10%	2%
	7.1M	5.2M	4.6M	4.3M
PLM – Replacement Cost	6%	3%	1%	0%
	4.4M	4.3M	4.3M	4.2M
PLM – Response Cost	3%	1%	1%	0%
	4.3M	4.3M	4.2M	4.2M
SLM – Reputation Damage	21%	10%	5%	1%
	5.1M	4.6M	4.4M	4.2M



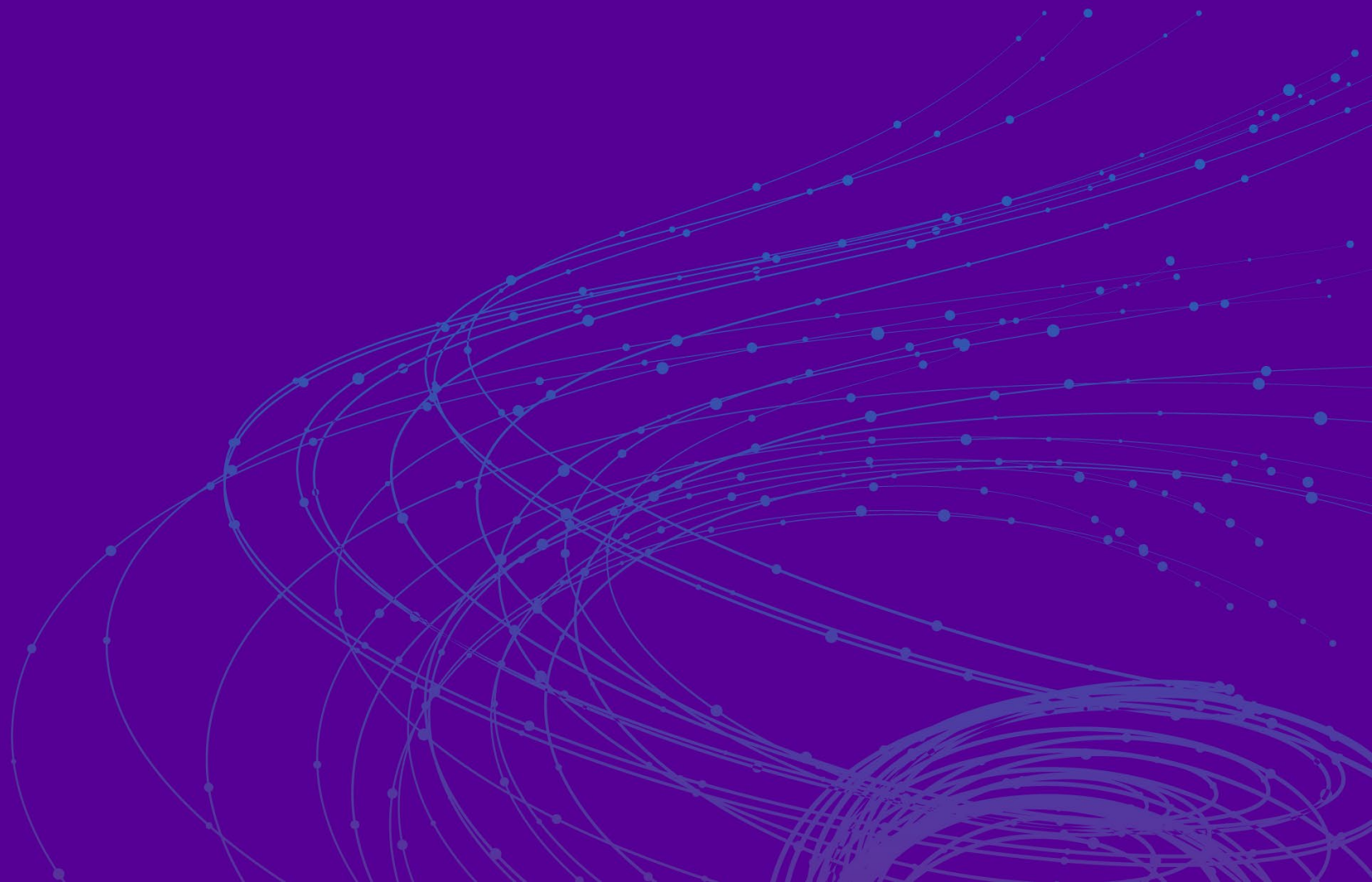
Case Study 1 – Business Leader Decision

Risk Factor – Component	20%	10%	5%	1%
TEF – Cyber Criminals	29%	14%	7%	1%
	5.4M	4.8M	4.5M	4.2M
RS – Authentication Strength	16%	8%	4%	1%
	4.9M	4.5M	4.4M	4.2M
RS – Structural Integrity	29%	10%	4%	1%
	5.4M	4.6M	4.4M	4.2M
RS – Authentication Control	395%	176%	79%	17%
	20.8M	11.6M	7.5M	4.9M
RS – Structural Integrity Control	69%	24%	10%	2%
	7.1M	5.2M	4.6M	4.3M
PLM – Replacement Cost	6%	3%	1%	0%
	4.4M	4.3M	4.3M	4.2M
PLM – Response Cost	3%	1%	1%	0%
	4.3M	4.3M	4.2M	4.2M
SLM – Reputation Damage	21%	10%	5%	1%
	5.1M	4.6M	4.4M	4.2M

"Now we're getting somewhere! I'll obtain budget to track those two external fraud risk indicators. But what about service disruption risk? We don't want more than $10M of that."

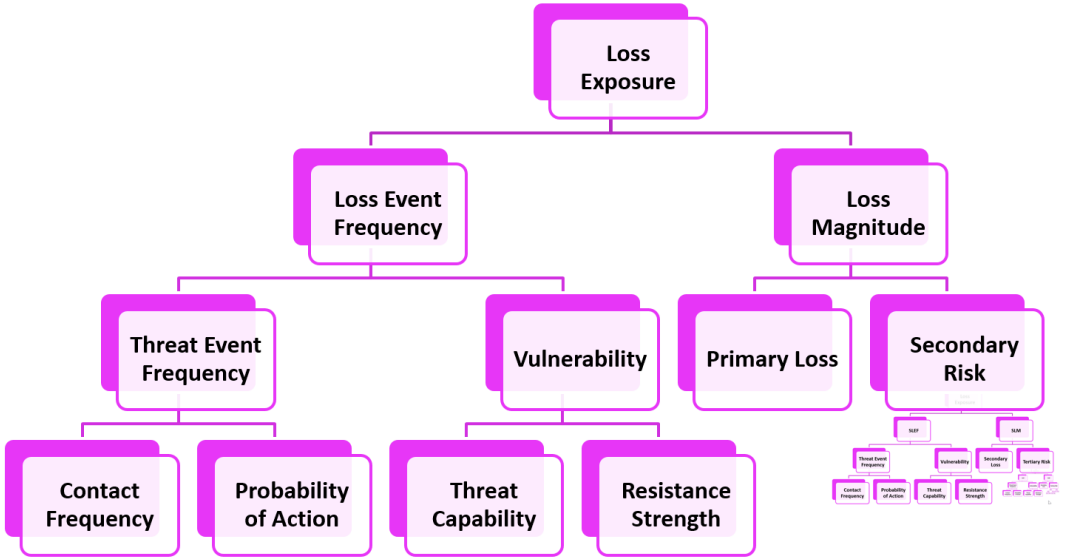
RSAConference2019

Case Study 2



Case Study 2 – Introduction

Risk Scenario: Service Disruption

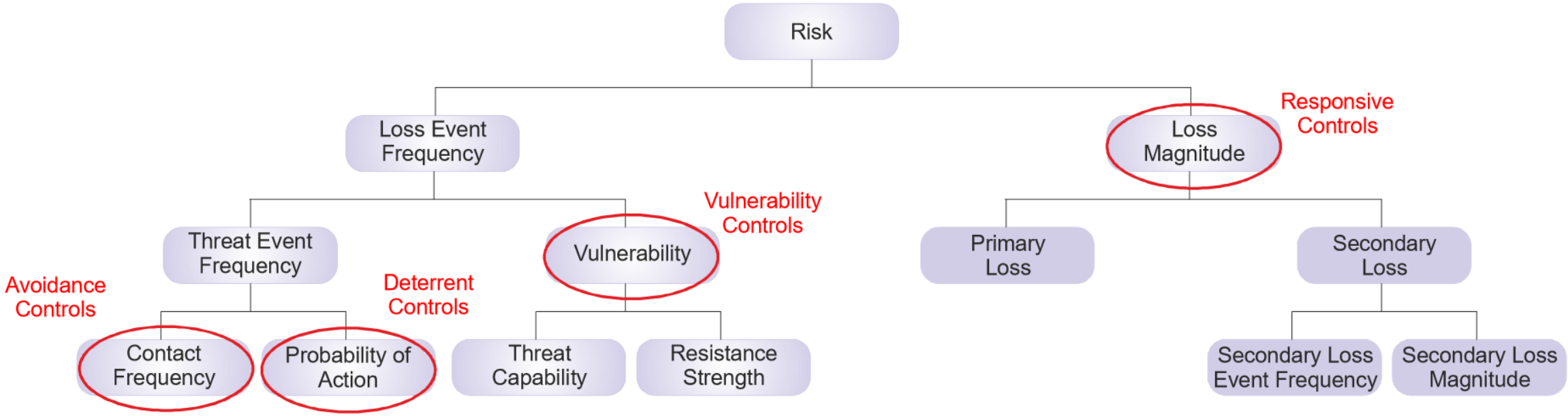


Risk Factor Components			Min	Most Likely	Max
Loss Event Frequency	TEF		1	4	10
	Threat Capability[1] (%)		30	56	85
	Resistance Strength[2] (%)		50	70	90
Primary Loss Magnitude	Primary Response Cost[3] ($)		10,000	10,000	100,000
	Productivity Loss ($)		0	50,000	500,000
Secondary Risk	SLEF (%)		50	50	100
	SLM	Secondary Response Cost ($)	10,000	100,000	1,000,000
		Fines & Judgments ($)	0	500,000	5,000,000
		Reputation Damage ($)	0	0	50,000,000

1) Latest threat intel says a 1:3 mix of cyber criminals / general hackers is attacking →
2) Effectiveness of vulnerability control system (firewalls, traffic scrubbing) as calibrated against the known threat continuum
3) Responsive controls in place and expected to contain 50% of successful attacks

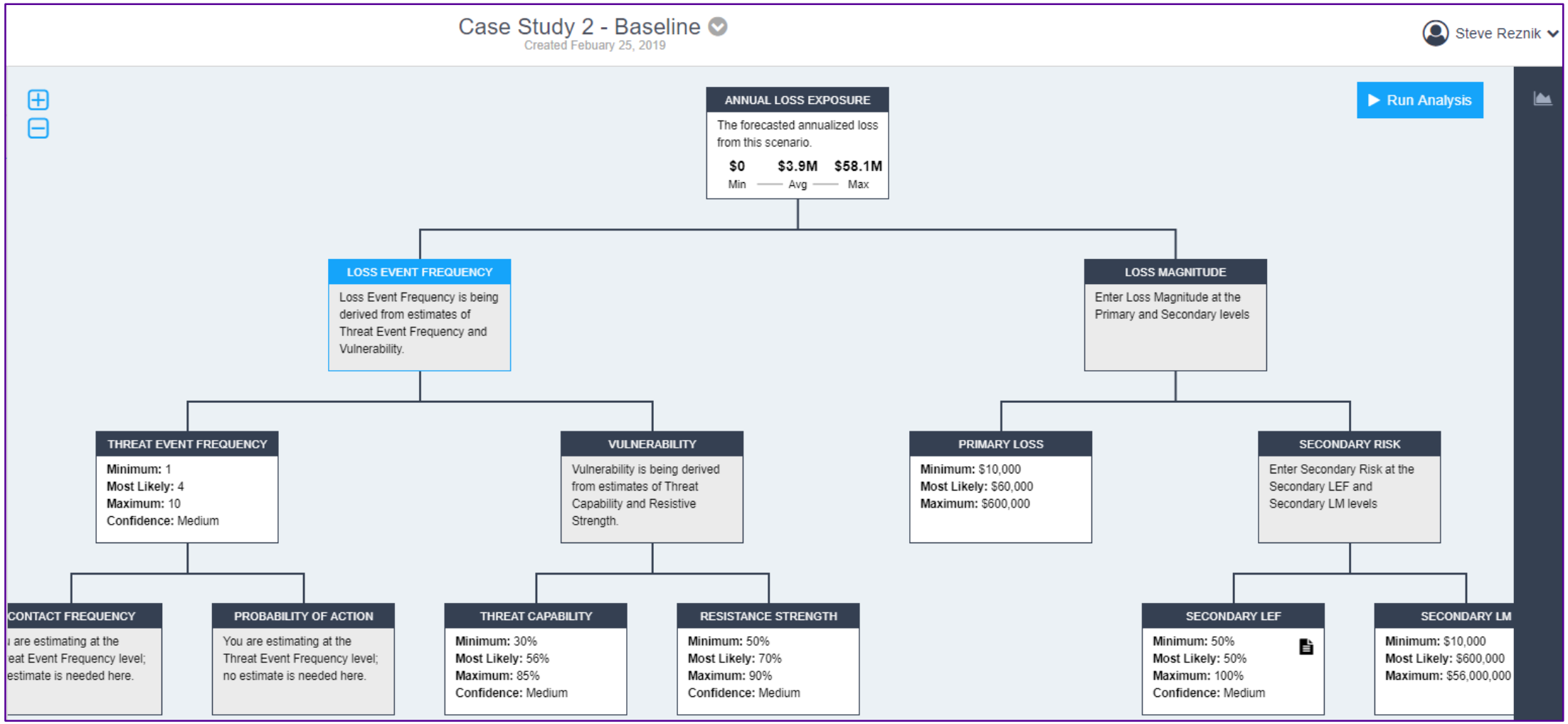
TCap Blend	Min	Most Likely	Max
Cyber Criminals	60%	75%	99%
General Hacking	20%	50%	80%
1:3	30%	56%	85%

"FAIR Friendly" Control Categories



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

Case Study 2 – Baseline Estimate Input



https://www.fairinstitute.org/fair-u

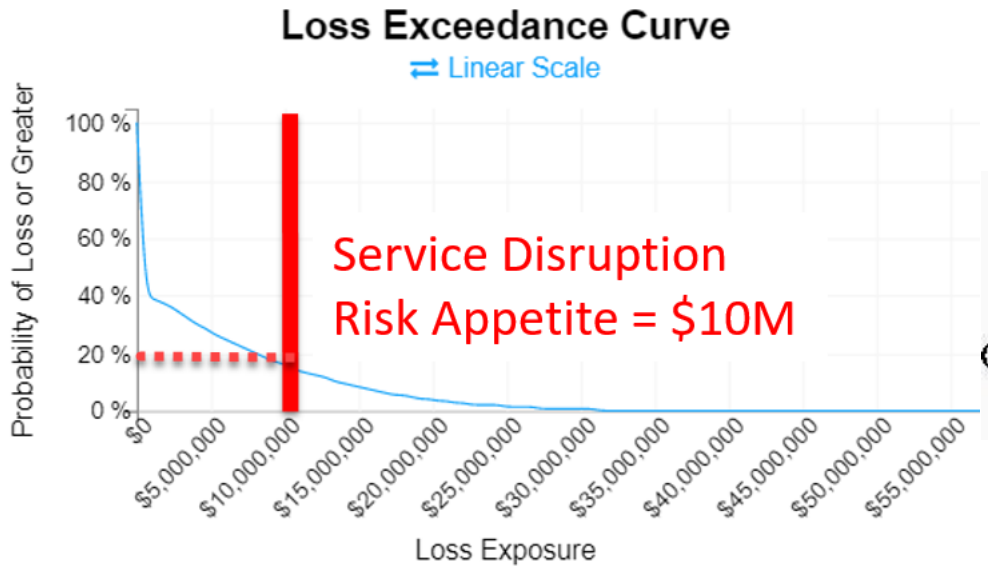
Case Study 2 – Baseline Estimate Output

Analysis Results

Risk

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

$0	$3.9M	$58.1M
Minimum	Average	Maximum



"A 20% chance of service disruption losses greater than $10M within the next 12 months… not bad… now show me how to keep an eye on this with better metrics."

Case Study 2 – Choose Factor, Change It, Observe LE

TCap	Min	Most Likely	Max	
Cyber Criminals	60%	75%	99%	*Blended*
General Hacking	20%	50%	80%	*Capability*
1:3	30%	56%	85%	*Increase*
1:2	33%	58%	86%	*4%*
1:1	40%	63%	90%	*11%*
2:1	47%	67%	93%	*19%*
3:1	50%	69%	94%	*22%*

Threat Capability				
When threat capability increases by …	**20%**	**10%**	**5%**	**0%**
Loss exposure increases by…	**213%**	**95%**	**41%**	**0%**
Loss Exposure	$12.2M	$7.6M	$5.5M	$3.9M
Leverage	1:11	1:9	1:8	

Service Disruption Risk Appetite = $10M

Case Study 2 – Wash, Rinse, Repeat

RS	Min	ML	Max
Baseline	50%	70%	90%
Degrade 5%	48%	67%	86%
Degrade 10%	45%	63%	81%
Degrade 20%	40%	56%	72%

Resistance Strength				
When vulnerability control strength degrades by …	**20%**	**10%**	**5%**	**0%**
Loss exposure increases by…	**236%**	**105%**	**920%**	**0%**
Loss Exposure	$13.1M	$8M	$7.5M	$3.9M
Leverage	1:12	1:11	1:18	

Service Disruption Risk Appetite = $10M

Case Study 2 – Compare Leverage

Service Disruption Risk Factor Component	RFC Change	Loss Exposure Change	Leverage
Resistance Strength	10%	105%	1:11
Threat Capability		95%	1:9
TEF, Reputation Damage		10%	1:2
Primary Response Cost, Productivity Loss, SLEF, Secondary Response Cost, Fines & Judgments		Nominal	

Case Study 2 – Business Leader Decision

Service Disruption Risk Factor Component	RFC Change	Loss Exposure Change	Leverage
Resistance Strength	10%	105%	1:11
Threat Capability		95%	1:9
TEF, Reputation Damage		10%	1:2
Primary Response Cost, Productivity Loss, SLEF, Secondary Response Cost, Fines & Judgments		Nominal	

"Wow! So we should monitor more than just resistance strength in this case. Our vulnerability controls could be humming along while only 10% more bad guy capability doubles service disruption risk."

RSAConference2019

Pulling it all together!

Risk Monitoring Dashboard Design

Risk	Appetite	KRI	Metric	Baseline	RAV Threshold	Quarterly Reporting				Trend
Service Disruption	$10M	TEF	Frequency of DoS Attack	1 / Qtr.	3					
		Active Threat Capability	Ratio of Cyber Criminals to General Hacking Community	1:3	1:1					
		Vuln Control System Status	Relative Strength of Firewalls & Traffic Scrubbing	70% effective vs. baseline threat capability	60% *(15% decrease)*					
External Fraud	$6.5M	Authentication Strength	Compliance of Passwords & Practices	90%	86% *(5% decrease)*					
		System Structural Integrity	Compliance of Patch Levels & Asset Configurations	80%	65% *(20% decrease)*					

Risk Monitoring Dashboard – Nine Months Later

Risk	Appetite	KRI	Metric	RAV	Q1	Q2	Q3	Q4	Trend
Service Disruption	$10M	TEF	Frequency of DoS Attack	3	1	0	2		
		Active Threat Capability	Ratio of Cyber Criminals to General Hacking Community	1:1	1:3	1:3	1:2		
		Vuln Ctrl System Status	Relative Strength of Firewalls & Scrubbing	60%	70%	70%	70%		
External Fraud	$6.5M	Authentication Strength	Compliance of Passwords & Practices	86%	90%	90%	90%		
		System Structural Integrity	Compliance of Patch Levels & Asset Configurations	65%	80%	75%	65%		

Risk Monitoring Dashboard – Twelve Months Later

Risk	Appetite	KRI	Metric	RAV	Q1	Q2	Q3	Q4	Trend
Service Disruption	$10M	TEF	Frequency of DoS Attack	3	1	0	2	2	
		Active Threat Capability	Ratio of Cyber Criminals to General Hacking Community	1:1	1:3	1:3	1:2	1:2	
		Vuln Ctrl System Status	Relative Strength of Firewalls & Scrubbing	60%	70%	70%	70%	75%	
External Fraud	$6.5M	Authentication Strength	Compliance of Passwords & Practices	86%	90%	90%	90%	92%	
		System Structural Integrity	Compliance of Patch Levels & Asset Configurations	65%	80%	75%	65%	80%	

RSAConference2019

Poll Question: Do your metrics indicate risk?

Poll the Audience

- GRC-R02
- Do your metrics indicate risk?
  - Yes
  - No
  - Maybe
- https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3861

Recap

Risk indicators should…	• Alert on required course corrections • Reduce the likelihood of unacceptable loss
A KRI should…	• Relate to a factor of loss exposure • Have a risk appetite violation threshold
Now you can…	• Identify BETTER! metrics!

RSAConference2019

Applying what you've learned

Apply it

By next week…

- **Select a top risk scenario**

By next month…

- **Gather risk factor data**
- **Estimate loss exposure***

Before summer vacation…

- **Choose candidates with more leverage**
- **Set risk appetite violation thresholds**
- **Track and report!**

* FREE TOOLS AVAILABLE!!! → FAIR-U and The Open FAIR™ Risk Analysis Tool

RSAConference2019

Q&A