February Community Meetup

THREAT MODELING CONNECT
POWERED BY IRIUSRISK

Show Me the Money: Open FAIR and the ROI for Threat Modeling

February 22nd | 11AM ET

Speakers:

Simone Curzi
Principal Consultant, Cyber @ Microsoft

John Linford
Security Portfolio Forum Director @The Open Group

Ken St. Cyr
Sr. Architect, Cybersecurity@ Microsoft

About the Community Meetup

- **Our Goal**
  Exchange real-world experience, share practical knowledge, validate ideas to improve our own practice.

- **Chatham House Rule**
  Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

- **Video is optional but highly recommended :)**

📅 Agenda of Today

11:00	Welcome, intro, photo
11:05	Presentation & demo
11:40	Q&A, Discussion
11:55	Closing & Announcements

Photo Time!

About me

John Linford
Security Portfolio Forum Director
The Open Group

The Open Group is a global consortium of 900+ Member organizations that enables the achievement of business objectives through technology standards.

John facilitates consensus-based Standards process for Security Portfolio:

- -Security Forum
- -Open Trusted Technology Forum
- -Assured Dependability Work Group

Open FAIR and Open FAIR 2 Foundation Certified

BS, Economics & MA, Applied Economics from San Jose State University

Ken to revise

About me

- 20 years at Microsoft
- Author & co-author of multiple books and publications for Sybex Wiley, IT Pro Magazine, Redmond Magazine, and others
- Lectured in dozens of venues, internally at Microsoft and events hosted by Forrester, IT Pro Connections, and SANS

Ken St. Cyr
Senior Architect, Cyber
Microsoft

https://www.linkedin.com/in/ken-st-cyr-02332a5

About me

Simone Curzi
Principal Consultant, Cyber
Microsoft

24 years in Microsoft

Current role: Principal Consultant, Cyber

- Regular speaker to conferences like MS [Tech]Ready, MS Spark, DevSecOps Days, (ISC)2 Security Congress
- Co-author of a book on Azure Security for developers, with Michael Howard and Heinrich Gantenbein
- Blog & papers author (Evolving Threat Modeling, Integrating threat modeling with DevOps - Security documentation | Microsoft Learn)
- Active participant of the Open Group project for adopting Open FAIR as part of Threat Modeling processes
- Author of a Threat Modeling tool, Threats Manager Studio

Outline

WHY?

Why Threat Modeling needs Open FAIR?

WHAT?

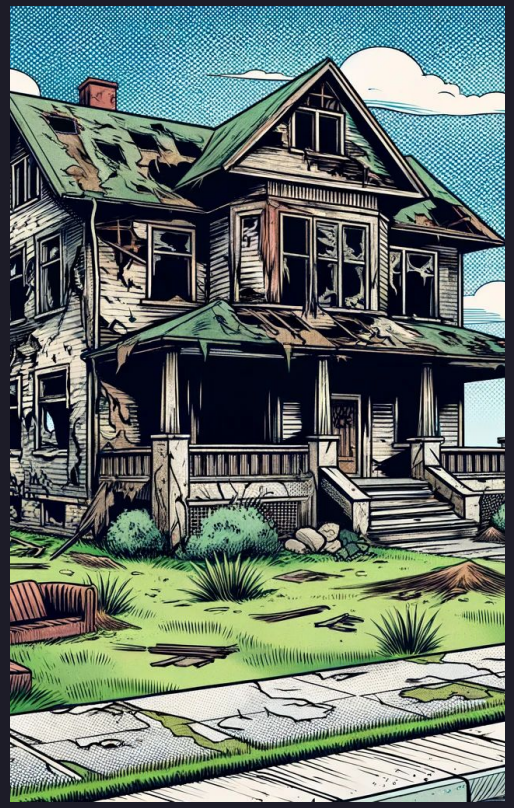
What is Open FAIR?

HOW?

How can we combine them together?

Why?

Imagine if we renovated homes the same way security investments are made...



Acquire a house that's in bad shape, but shows some promise

Make a list of everything that's wrong

Fix the stuff that makes it look nice, but the house is still in shambles

Why?

We all know what threat modeling is, right?

We analyze representations of a system

and seek answers to good questions

THREAT MODELING MANIFESTO

What is threat modeling?

Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

At the highest levels, when we threat model, we ask four key questions:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

Why threat model?

When you perform threat modeling, you begin to recognize what can go wrong in a system. It also allows you to pinpoint design and implementation issues that require mitigation, whether it is early in or throughout the lifetime of the system. The output of the threat model, which are known as threats, informs decisions that you might make in subsequent design, development, testing, and post-deployment phases.

Who should threat model?

You. Everyone. Anyone who is concerned about the privacy, safety, and security of their system.

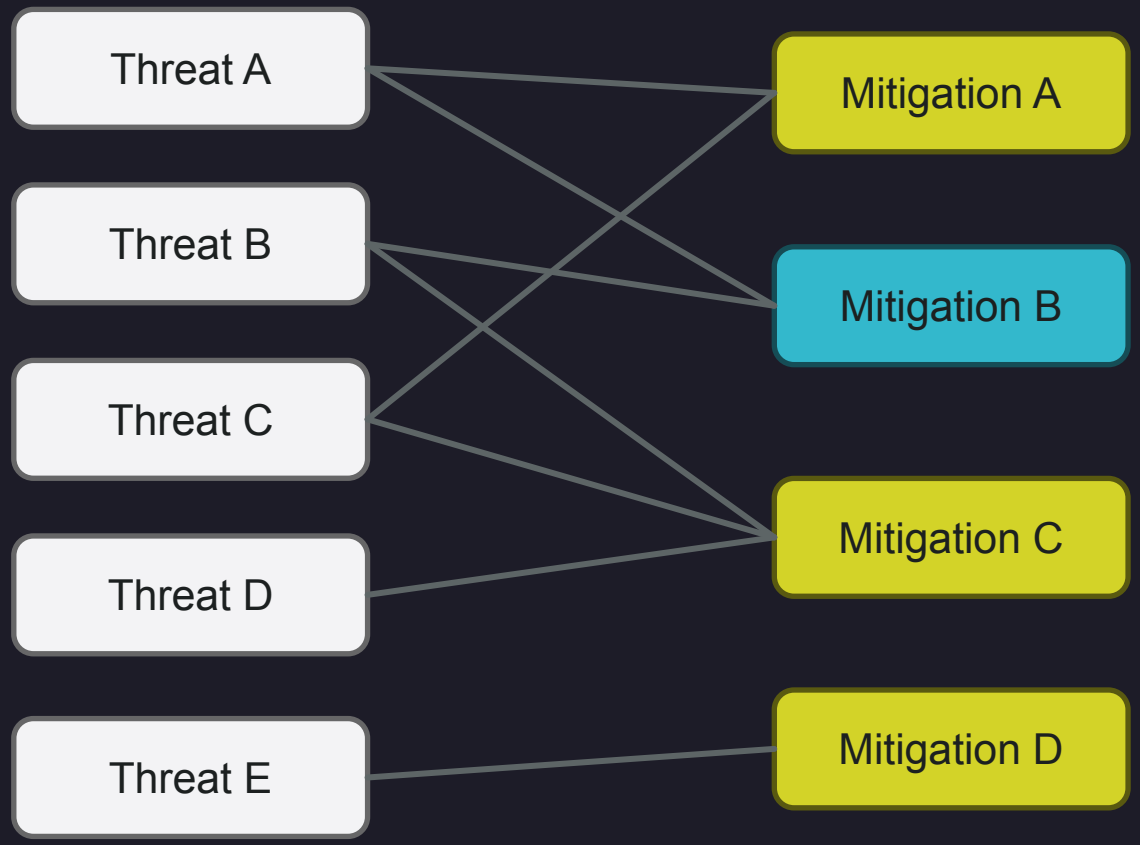
How should I use the Threat Modeling Manifesto?

Use the Manifesto as a guide to develop or refine a methodology that best fits your needs. We believe that following the guidance in the Manifesto will result in more effective and more productive threat modeling. In turn, this will help you to successfully develop more secure applications, systems, and organizations and protect them from threats to your data and services. The Manifesto contains ideas, but is not a how-to, and is methodology-agnostic.

https://www.threatmodelingmanifesto.org/

Why?

What we get from a Threat Model



The Threat Model produces threat events and mitigations

All threat events should have at least one associated mitigation

All mitigations have at least one associated threat event

Mitigations have a status. Some of them already exist, while others need to be implemented

Why?

What the BDM needs to know

> Where do I spend my limited security budget?

How severe is the situation? Is the severity enough to justify a $1,000,000 investment?

Can I go to production securely now? How long before I can?

If we implement an alternative architecture, are we going to do better from a security perspective? How much better?

What is the ideal set of mitigations I should implement to optimize overall costs with security improvements?

Is my project implementing security adequately?

Why?

How we typically answer the BDM questions

			IMPACT				
			Negligible	Minor	Moderate	Critical	Catastrophic
			<$10K	$10K to <$100K	$100K to <$1M	$1M to <$10M	>$10M
Likelihood	Frequent	99%+	Medium	Medium	High	High	High
	Likely	>50%-99%	Medium	Medium	Medium	High	High
	Occasional	>25%-50%	Low	Medium	Medium	Medium	High
	Seldom	>1%-25%	Low	Low	Medium	Medium	Medium
	Improbable	<1%	Low	Low	Low	Medium	Medium

Scenario A

Likelihood is 20%

Impact is $100 Million

.2 x $100,000,000 = **$20,000,000**

Scenario B

Likelihood is 2%

Impact is $10 Million

.02 x $10,000,000 = **$200,000**

From an actuarial viewpoint, Scenario B represents
100th the risk of Scenario A, yet they **occupy the *same cell*** in the risk matrix!

Why?

Threat Modeling only solves one part of the equation

Why?

Then we add Quantitative Risk Analysis (Open FAIR) to...

1

Measure the current risk

Given a threat modeled system, what is its annualized loss expectancy, if I do nothing?

This is your baseline.

2

Optimize the effort

Given a threat modeled system, what is the optimal set of mitigations I should implement to minimize the cost due to its annualized loss expectancy, combined with the implementation and the maintenance of the mitigations?

This is your proposed change.

3

Measure the improvements

Given a threat modeled system, how much does the annualized loss expectancy improve sprint over sprint, due to the implementation of the identified mitigations?

This shows your ROSI.

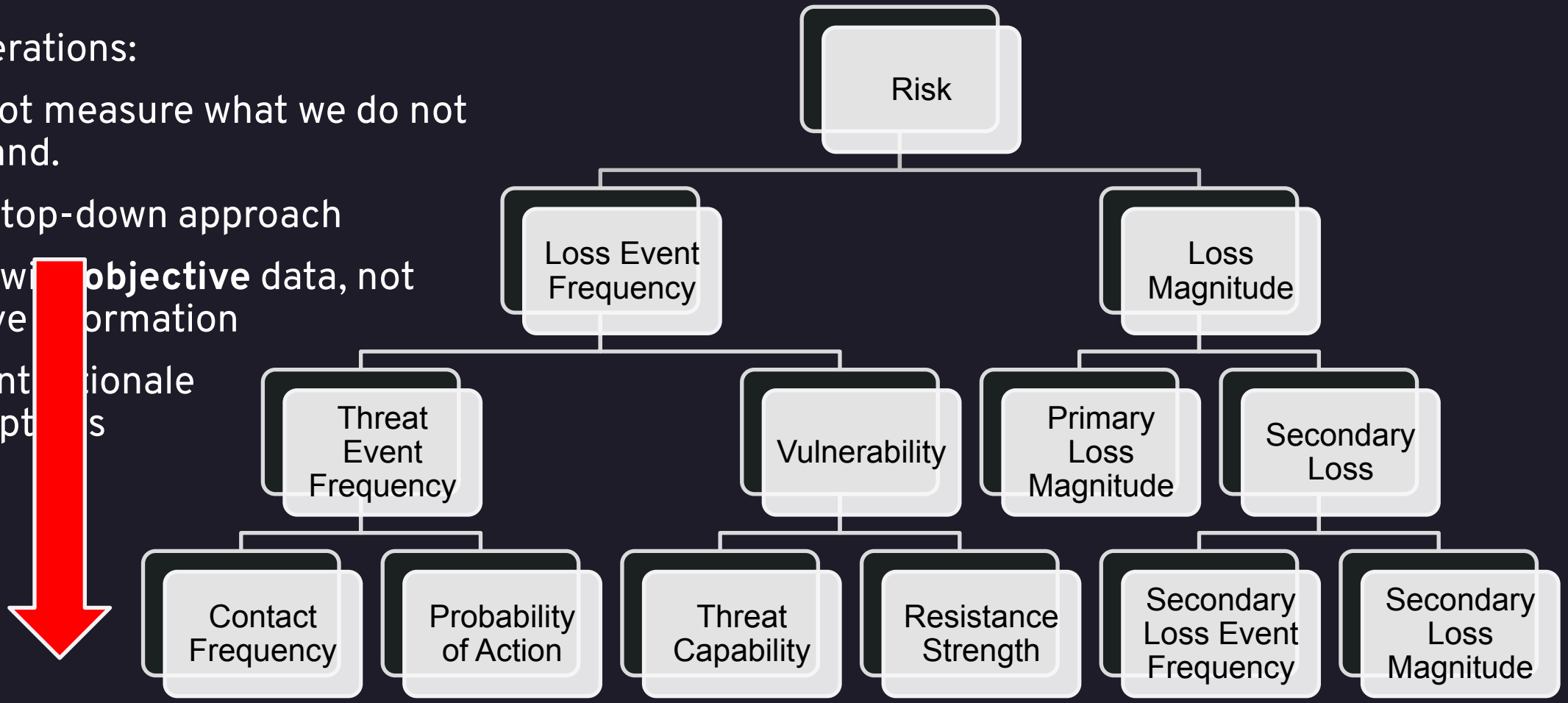
What?

Open FAIR™ Taxonomy

Risk = Probable frequency and probable magnitude of future loss

Key considerations:

- We cannot measure what we do not understand.
- Utilize a top-down approach
- Analyze wi**objective** data, not subjective ormation
- Document ionale & assumpt s



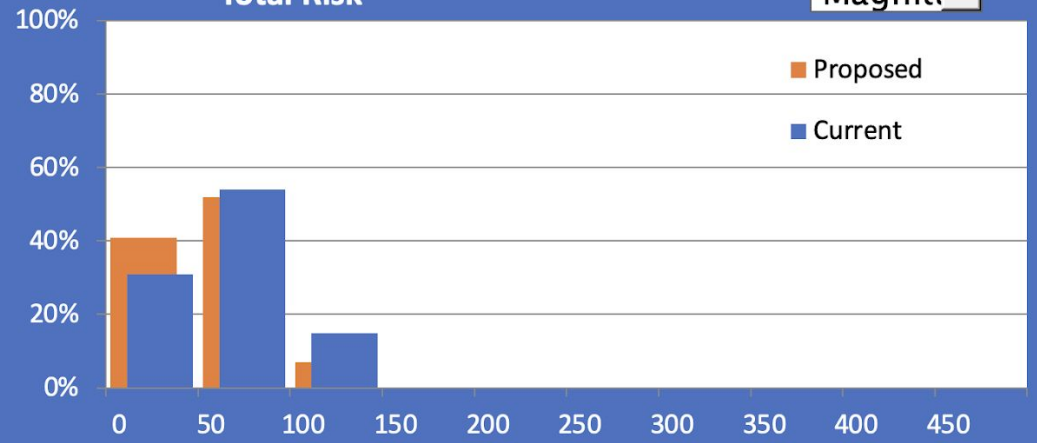
What?

Open FAIR™ Risk Analysis Tool

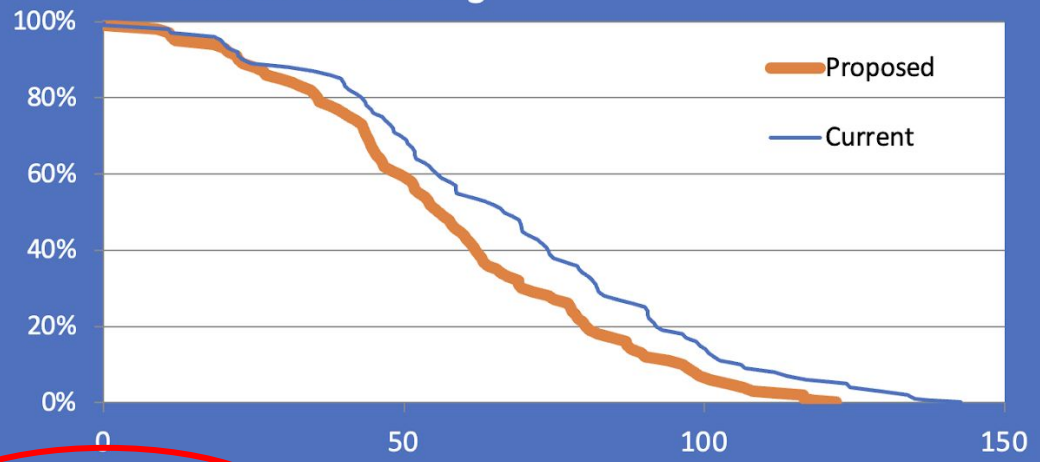
User's Guide

Loss Magnitude/yr. $000s

Total Risk — Magnitu



Chance of Exceeding



Simulated Loss — Trial 1/100

Cur.	Prop.
84.8	60.0
Diff.	24.8

Average Loss

Cur.	Prop.
67.0	57.6
Diff.	9.3

Percentile Loss 95%

Cur.	Prop.
123.7	103.7
Diff.	20.0

Chance Loss Exceeds 5

Cur.	Prop.
98%	98%
Diff.	0%

Loss Units	Loss Measure
$	000s

Bins: 10 — Width: 50

Magnitude Display Mode: Total Risk

Sums Primary and Secondary Risk across all potential events

What?

Loss Event Frequency/yr.
Calculated Below

☐ Drill Down

User's Guide

Threat Event Frequency/yr.
Calculated Below

☑ Drill Down

Vulnerability

Min	ML	Max
40%	50%	60%
35%	45%	50%

☐ Drill Down

Contact Frequency/yr.

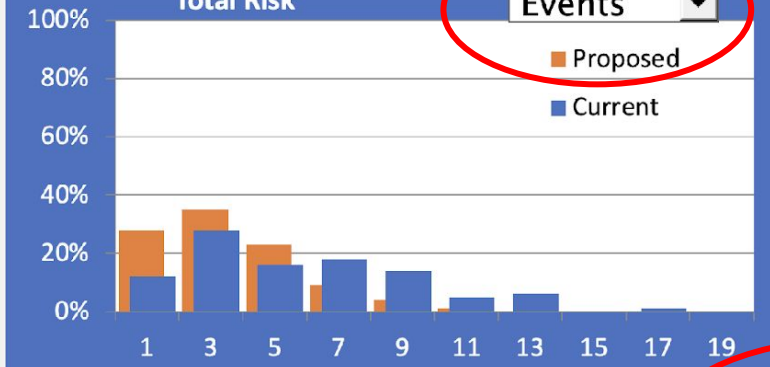
	Cur.	Pro.
Min	5	4
ML	20	18
Max	50	45

Probability of Action

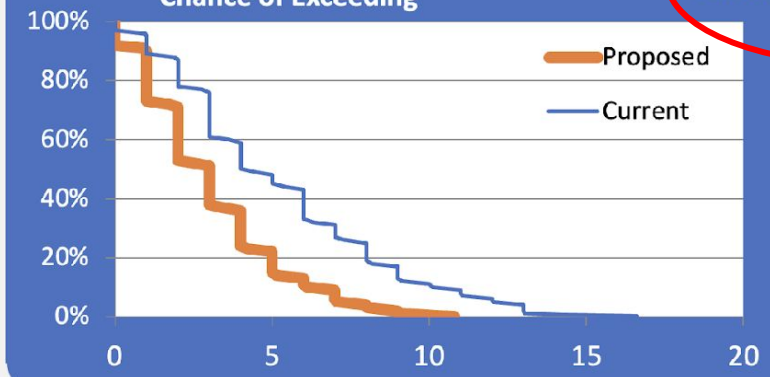
	Cur.	Pro.
Min	10%	9%
ML	40%	35%
Max	75%	50%

Loss Events/yr.
Total Risk

Events



Chance of Exceeding



Simulated Events
Trial 1/100

Cur.	Prop.
11.0	0.0
Diff.	11.0

Average Events

Cur.	Prop.
5.3	3.1
Diff.	2.2

Percentile Events 90%

Cur.	Prop.
10.1	6.1
Diff.	4.0

Chance Events Exceeds 50

Cur.	Prop.
0%	0%
Diff.	0%

Magnitude Display Mode

Total Risk

Sums Primary and Secondary Risk across all potential events

What?

Loss Magnitude
Calculated Below

Drill Down

User's Guide

Primary Loss Magnitude

Current	Min	ML	Max
Productivity	5	18	20
Replacement	6	8	10
Response			
Reputation			
Competitive Adv.			
Judgments			

Proposed	Min	ML	Max
Productivity	3	12	15
Replacement	5	7	8
Response			
Reputation			
Competitive Adv.			
Judgments			

Secondary Loss Magnitude

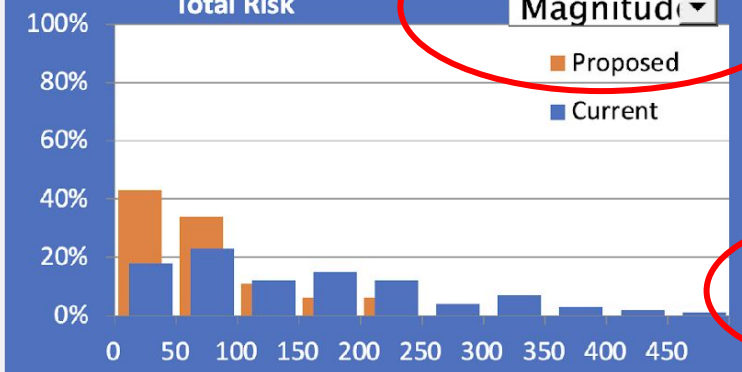
SLEF	Min	ML	Max
Current	0%	30%	60%
Proposed	0%	25%	50%

Current	Min	ML	Max
Productivity			
Replacement			
Response	3	9	15
Reputation	4	10	16
Competitive Adv.	5	11	17
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response	2	8	13
Reputation	3	10	16
Competitive Adv.	3	8	10
Judgments			

Loss Magnitude/yr. $000s
Total Risk

Magnitud



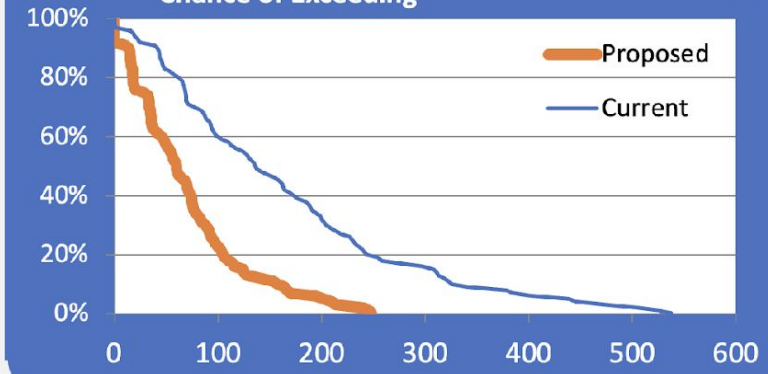
Simulated Loss
Trial 1/100

Cur.	Prop.
382.7	156.2
Diff.	226.5

Average Loss

Cur.	Prop.
165.5	70.6
Diff.	94.8

Chance of Exceeding



Percentile Loss 90%

Cur.	Prop.
325.9	157.0
Diff.	168.9

Chance Loss Exceeds 3

Cur.	Prop.
96%	91%
Diff.	5%

Bins 10

Width 50

Magnitude Display Mode: Total Risk

Sums Primary and Secondary Risk across all potential events

How?

Sample	Dimension (Mean)	Dim.Deviation	Dim.SquareDev
1	$ 70,322	$ 5,779	$ 33,391,062
2	$ 44,656	$ (19,888)	$ 395,512,656
3	$ 6,262	$ (58,282)	$ 3,396,733,242
4	$ 64,359	$ (185)	$ 34,040
5	$ 45,984	$ (18,560)	$ 344,455,040
6	$ 87,379	$ 22,836	$ 521,460,060
7	$ 60,781	$ (3,763)	$ 14,156,406
8	$ 91,055	$ 26,512	$ 702,859,632
9	$ 87,129	$ 22,586	$ 510,104,810
10	$ 87,508	$ 22,965	$ 527,368,260

Number of samples	10
Average	$ 64,544
Sample Variance	716230578.9
Standard deviation for sampling distribution	8463.0407
Range of the Average for the population (99% confidence)	
Min	$ 42,709
Max	$ 86,378
Threat Events	200
Selected Populations per Threat Event	3
Population size	600
Expected value for the Dimension for the overall population (99% confidence)	
Min	$ 25,625,313
Max	$ 51,826,887

How?

Demo

Live demo of the excel-based simulation template

Summary

Your Go-Dos

1. Check out our first blog post on the topic: https://aka.ms/tm-openfair
2. Join our team within the Open Group to further extend the approach
3. Start rethinking the role of Security, today

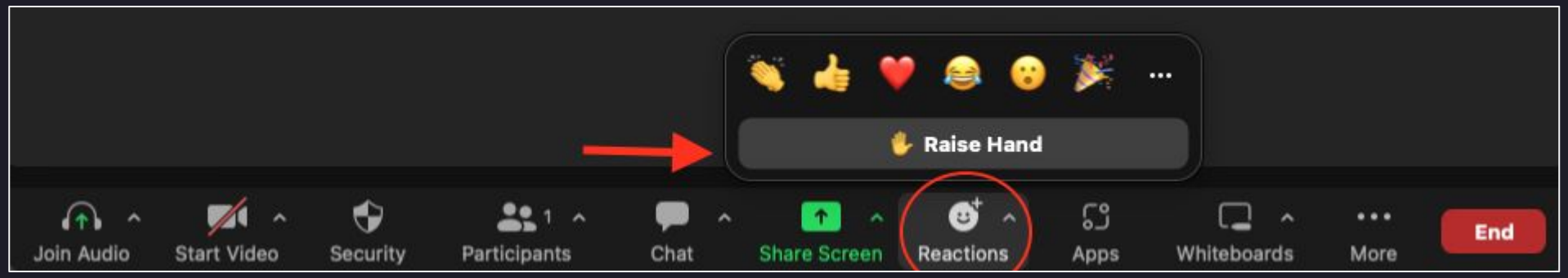
About Open Group and co-authors of Open FAIR

- Core Team
  - John Linford, Open Group
  - Simone Curzi, Microsoft
  - Dan Riley, Kyndryl
  - Ken St. Cyr, Microsoft
- Previous Contributors
  - David Vose, Vose Software
  - Altaz Valani, Info-Tech Research Group
- Special thanks to
  - John Feezell, Kyndryl

Discussion

How do you move your organization from predominantly utilizing qualitative risk analysis to quantitative risk analysis, and how do you handle opposition to this transition?

Use "✋ Raise Hand" feature to let the hosts know you have something to share.



Next meetup

Topic: Enhancing threat modeling process using security testing

Date: March 28, 2024 11AM ET

Register: threatmodelingconnect.com/events

THREAT MODELING CONNECT MASTERCLASS

Threat Modeling Maturity Model

March 14, 11:00am-noon ET

Simone Curzi,
Principal Consultant, Cyber @Microsoft

Altaz Valani,
Principal Advisory Director @Info-Tech Research Group


THREAT MODELING
CONNECT
HACKATHON
APRIL 1-21, 2024
IN PARTNERSHIP WITH
SHOSTACK
+ ASSOCIATES

EARLY BIRD REGISTRATION NOW OPEN. **UP TO 40% OFF**

THREAT MODCON 2024

LISBON

June 29

THREAT MODCON 2024

SAN FRANCISCO

September 28