

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: LAB2-R10

Let's Make Risk A Game!

4,000 Cyber-Risks in Your Hand.

Dr. Earl Crane



Founder, Chairman
Emergynt
@earlcranephd

Joel Benge

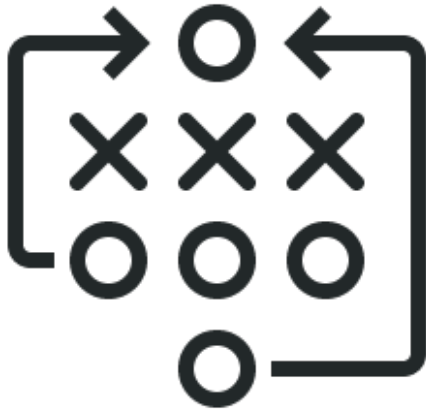


Strategist
ADG Creative
@joelmbenge

#RSAC

To Survive Doomsday

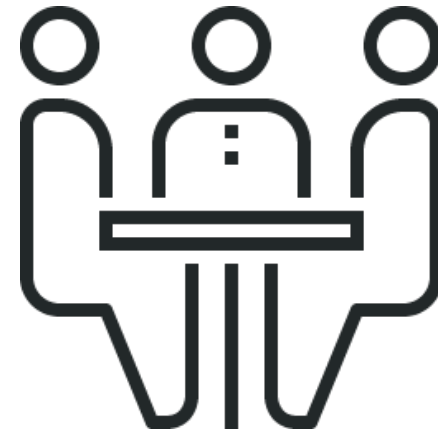
**Change of
Position**



**Change of
Mindset**

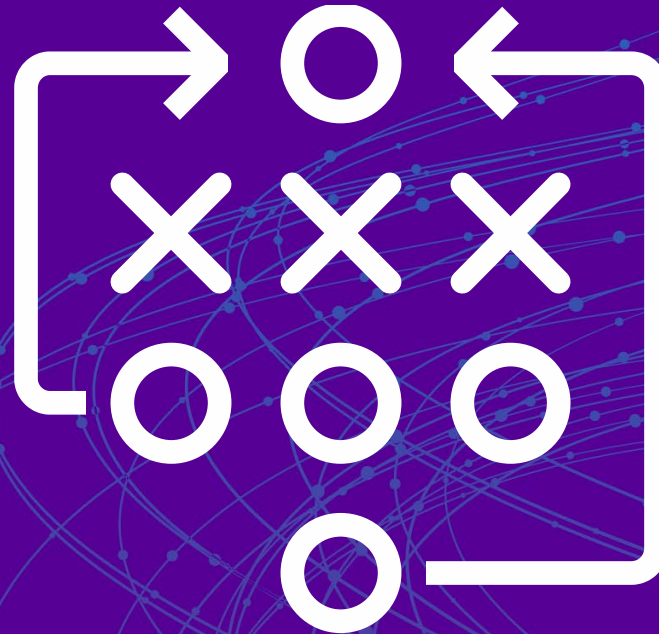


**Change of
Conversation**

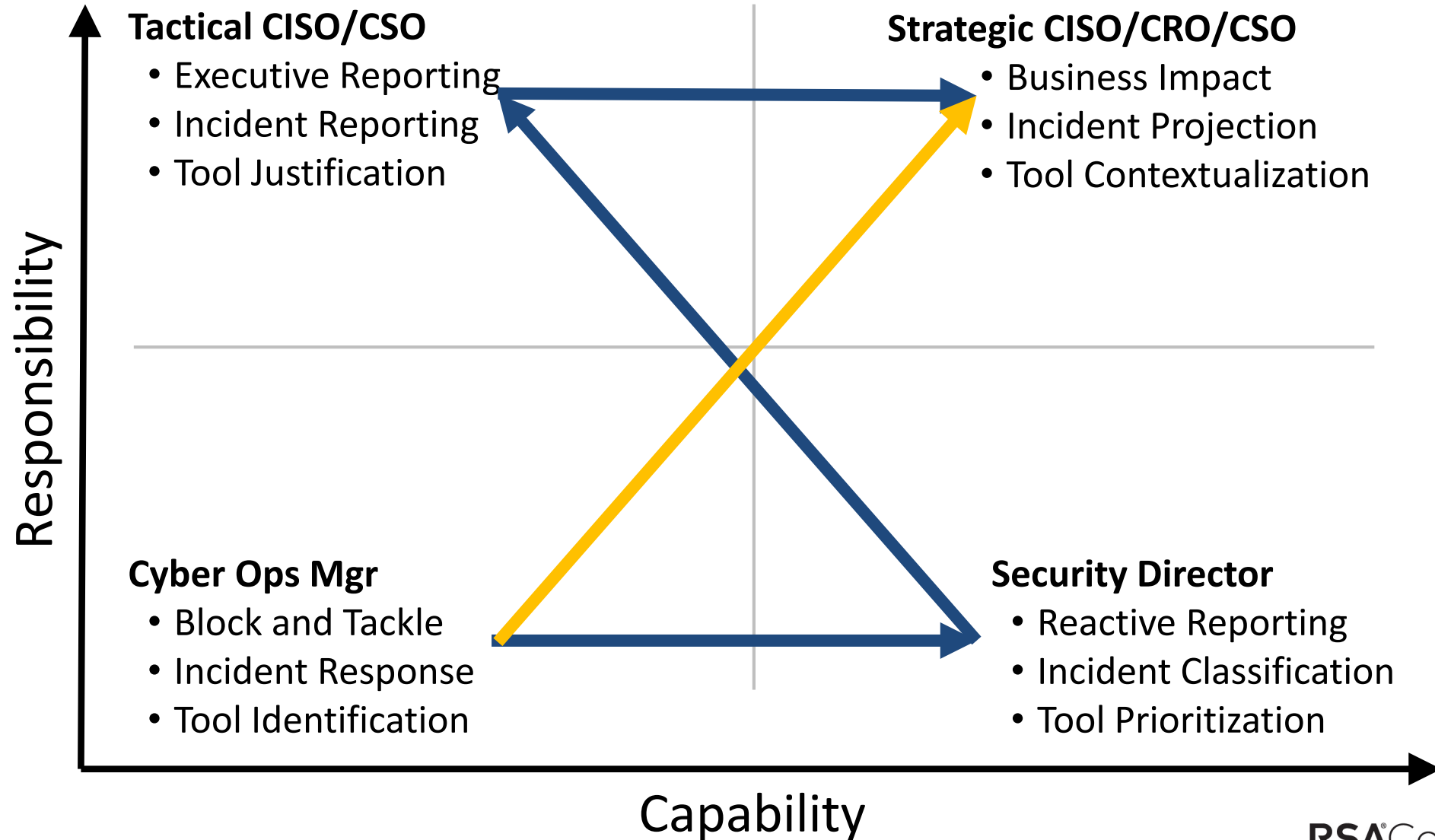


Change Your Position

“This isn’t **bunchball** soccer.”



Where do you want to be?



Three lines of defense

First Line



Risk Ownership

Operational management

- Day-to-day tempo
- Provide strategy for controls
- Identify, assess, control, and mitigate risks
- Security is designed into the systems

Second Line



Risk Oversight

Work closely with first line

- Support mgmt policies, define roles and responsibilities, and set goals for implementation
- Provide risk management frameworks
- Identify known & emerging issues
- Identify shifts implicit risk appetite
- Assist mgmt in developing processes and controls to manage risks and issues

Third Line

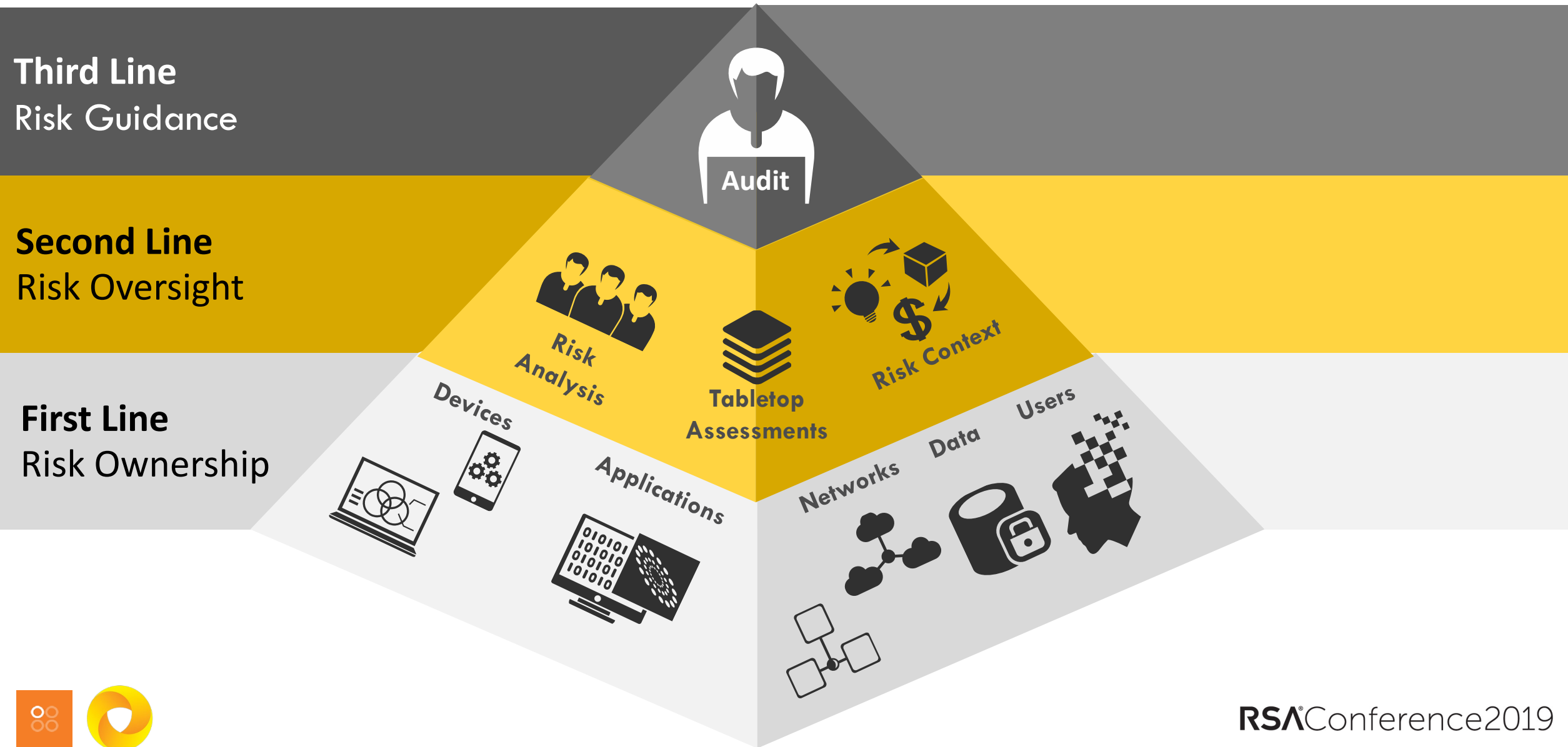


Risk Guidance

Independent assurance function

- Periodic audit and review, including operational efficacy, safeguarding, reporting, and compliance
- Report sufficiently high in the organization and to governing body

Different Responsibilities, Different Tools



Third Line
Risk Guidance

Second Line
Risk Oversight

First Line
Risk Ownership



Audit



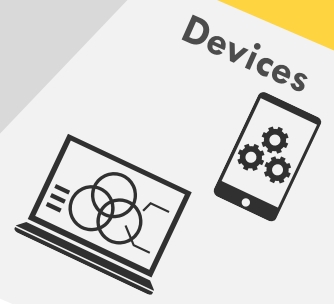
Risk Analysis



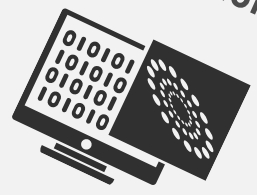
Risk Context



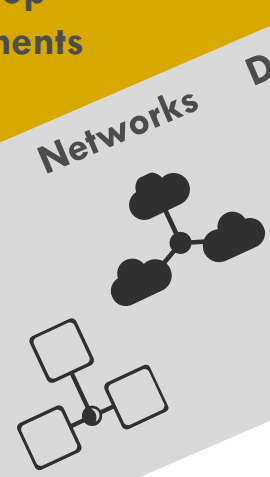
Tabletop Assessments



Devices



Applications



Networks



Data



Users



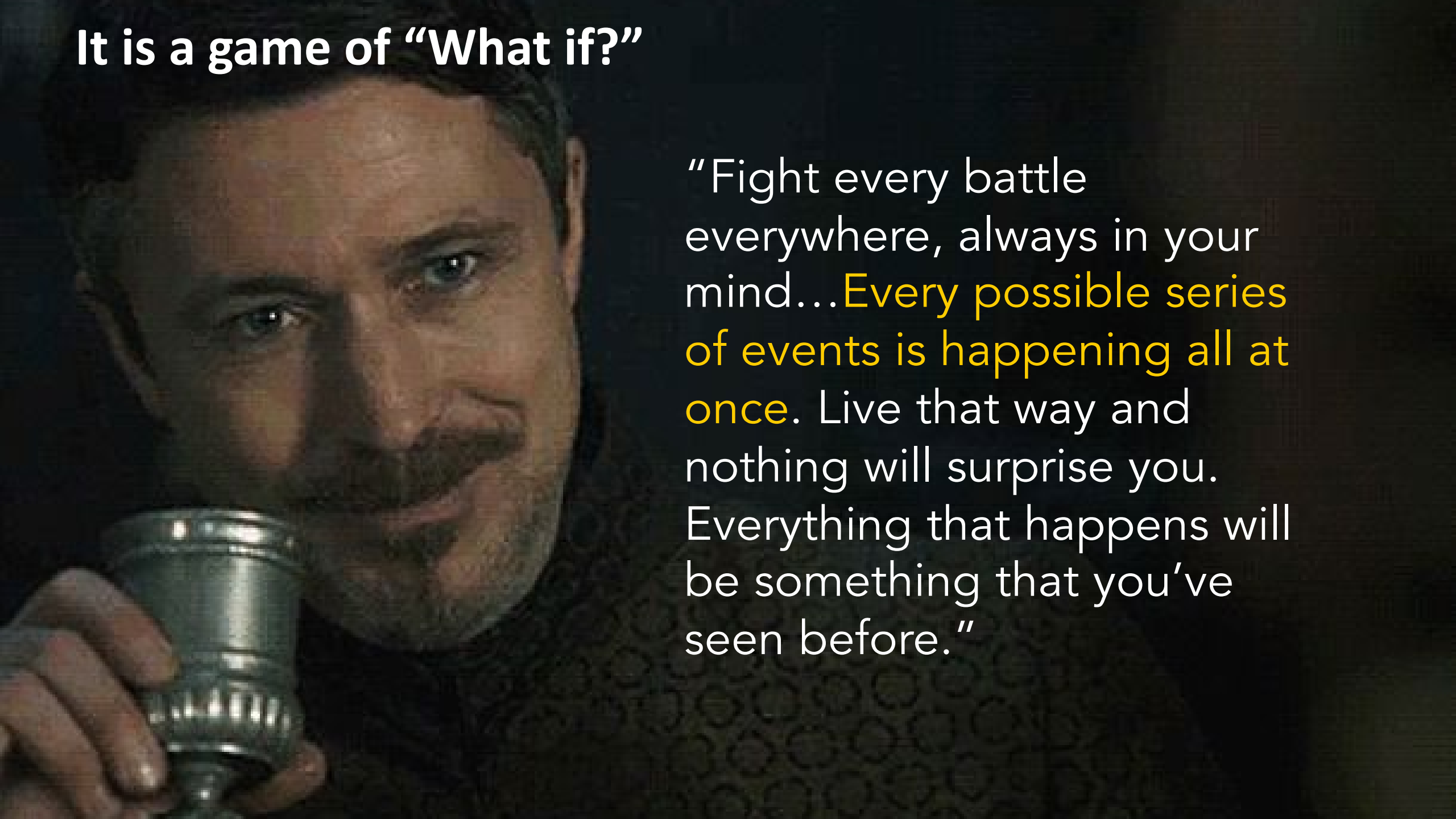
Change Your Mindset

What are you **willing** to risk?



Risk is not a game of “Whack-A-Mole”

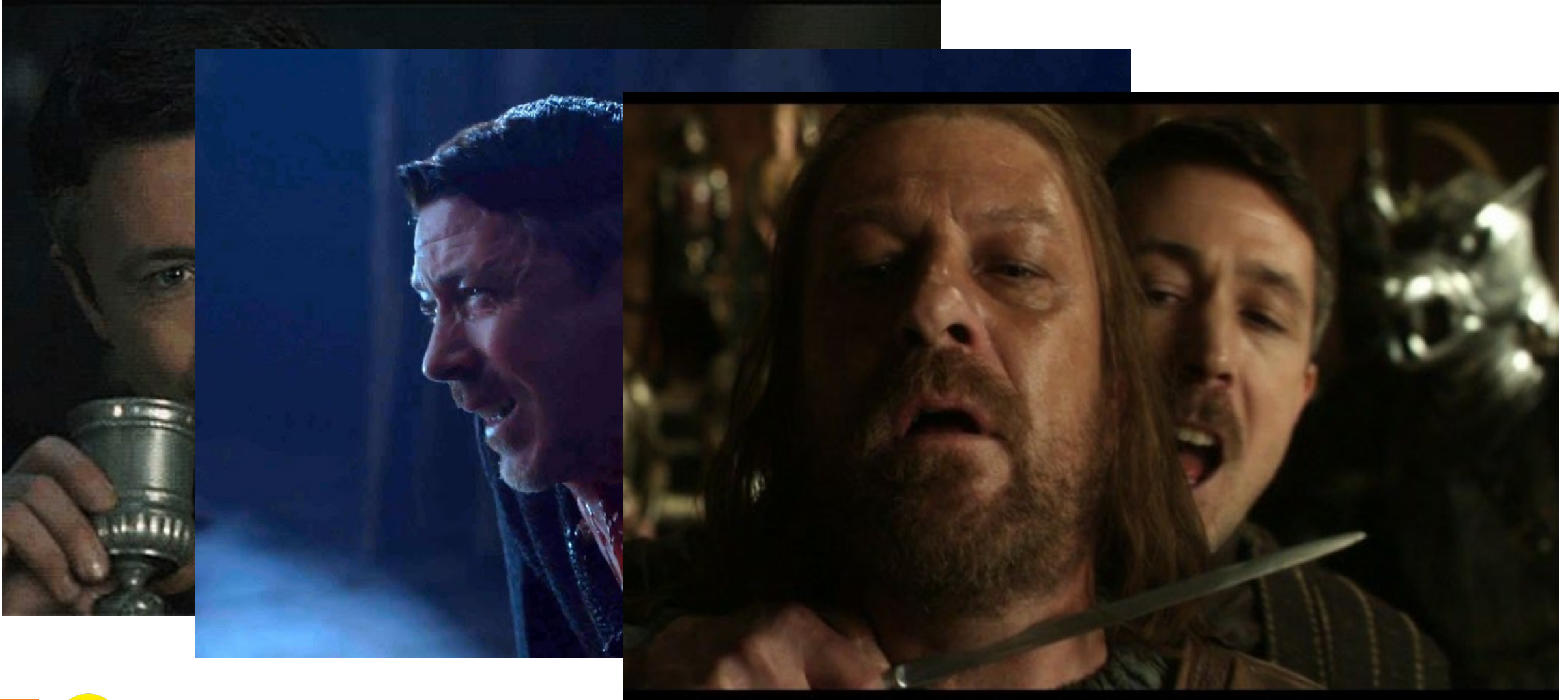


A close-up photograph of a man with a beard and mustache, looking directly at the camera. He is holding a metallic, cylindrical cup to his lips with his right hand. The background is dark and out of focus.

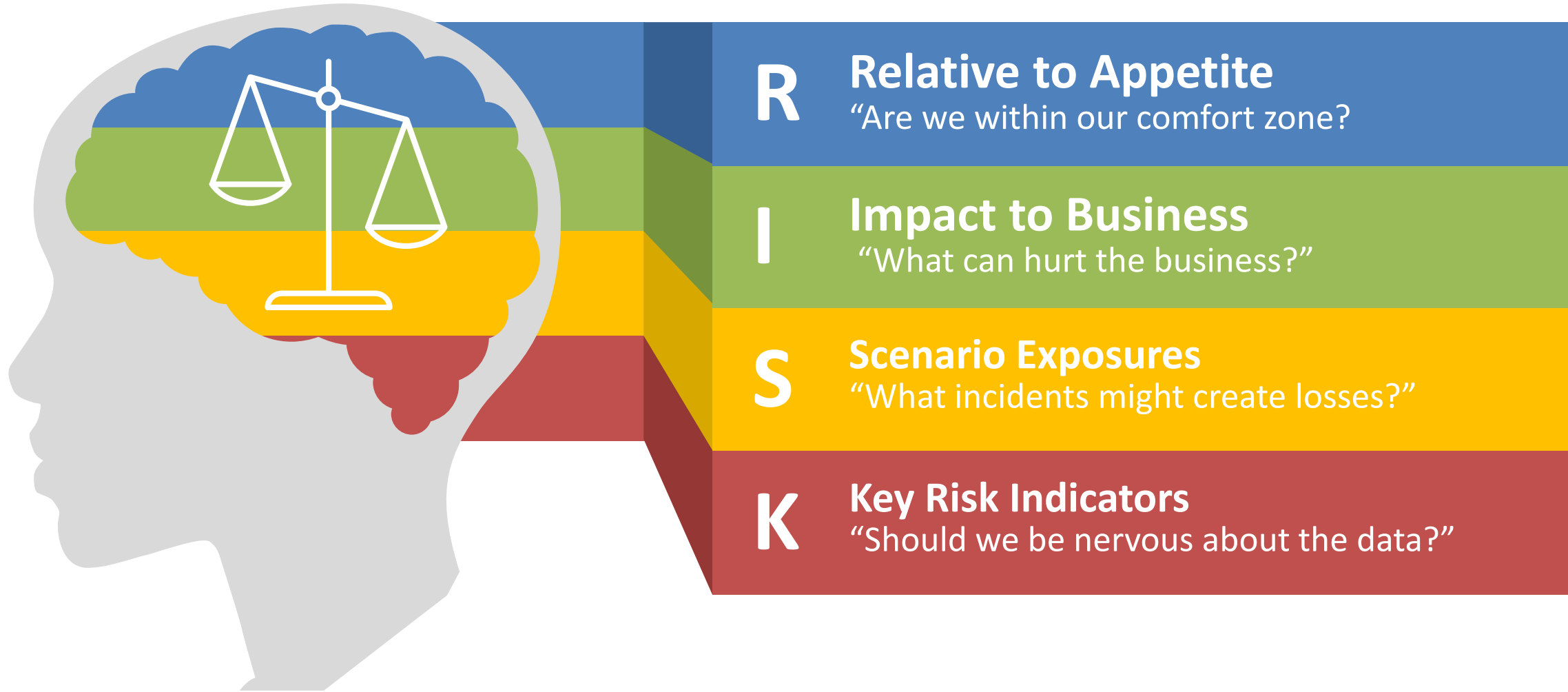
It is a game of “What if?”

“Fight every battle everywhere, always in your mind...**Every possible series of events is happening all at once.** Live that way and nothing will surprise you. Everything that happens will be something that you’ve seen before.”

What's the worst that could happen?

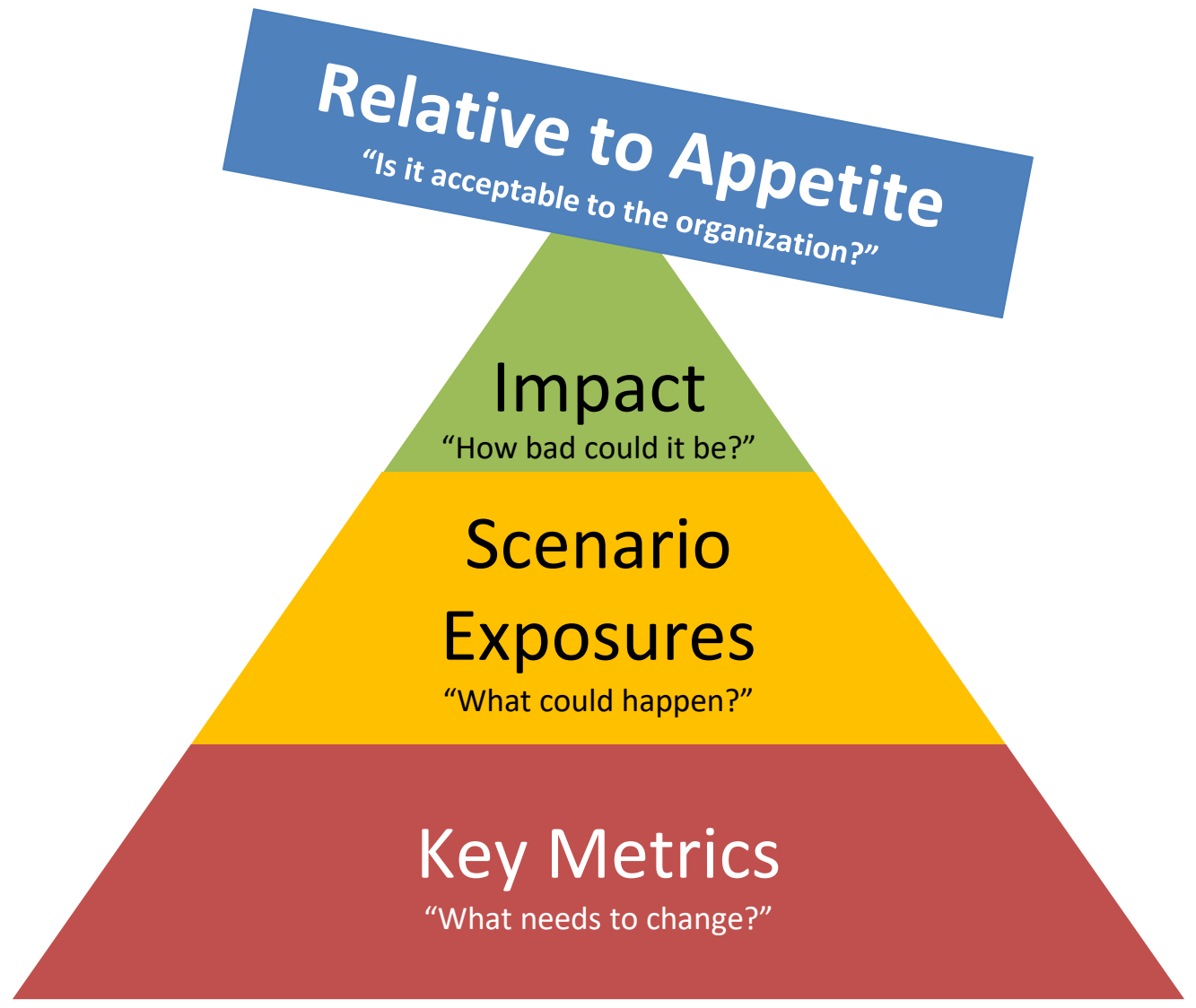


The Second-Line Risk Mindset



Cyber Risk Management Model

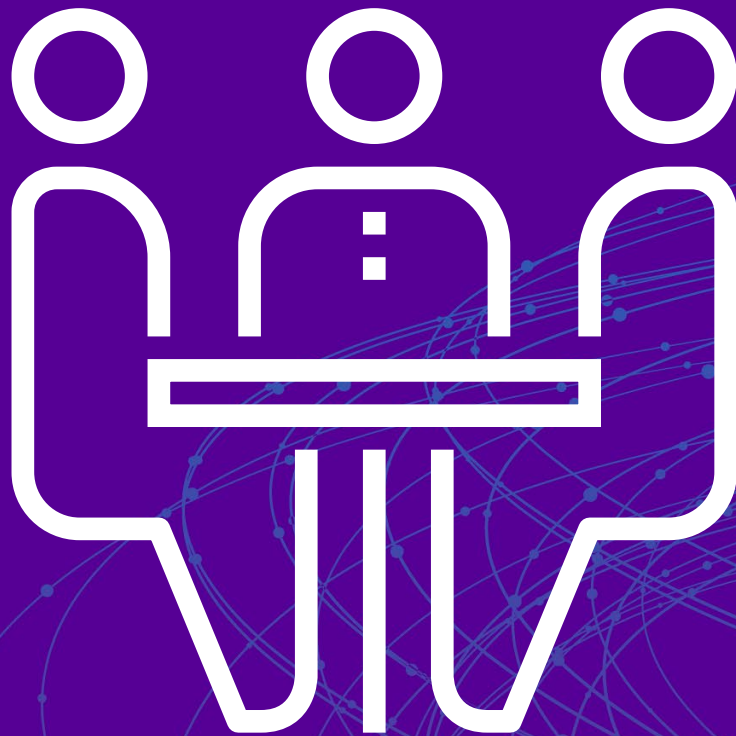
R
I
S
K



RSA[®]Conference2019

Change Your
Conversation

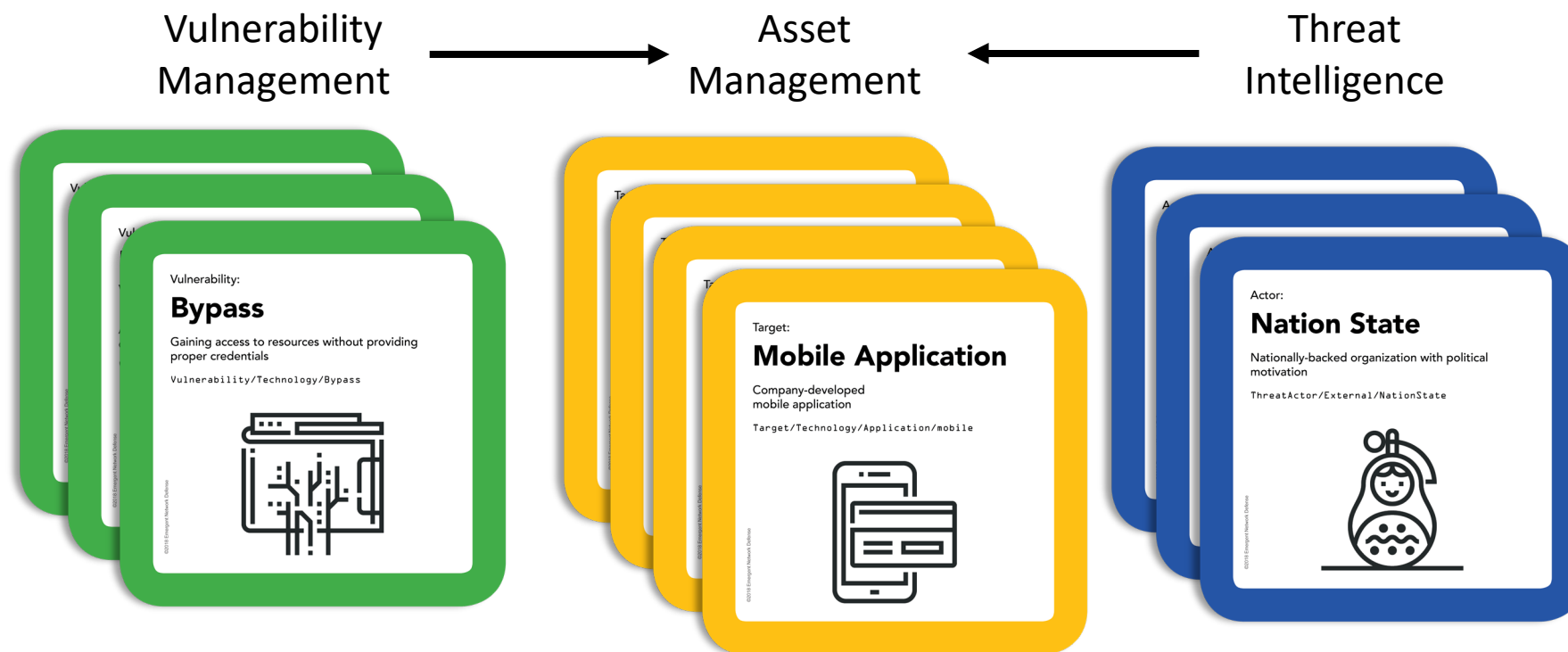
“We Are **Yellow.**”



Shall we play a game?

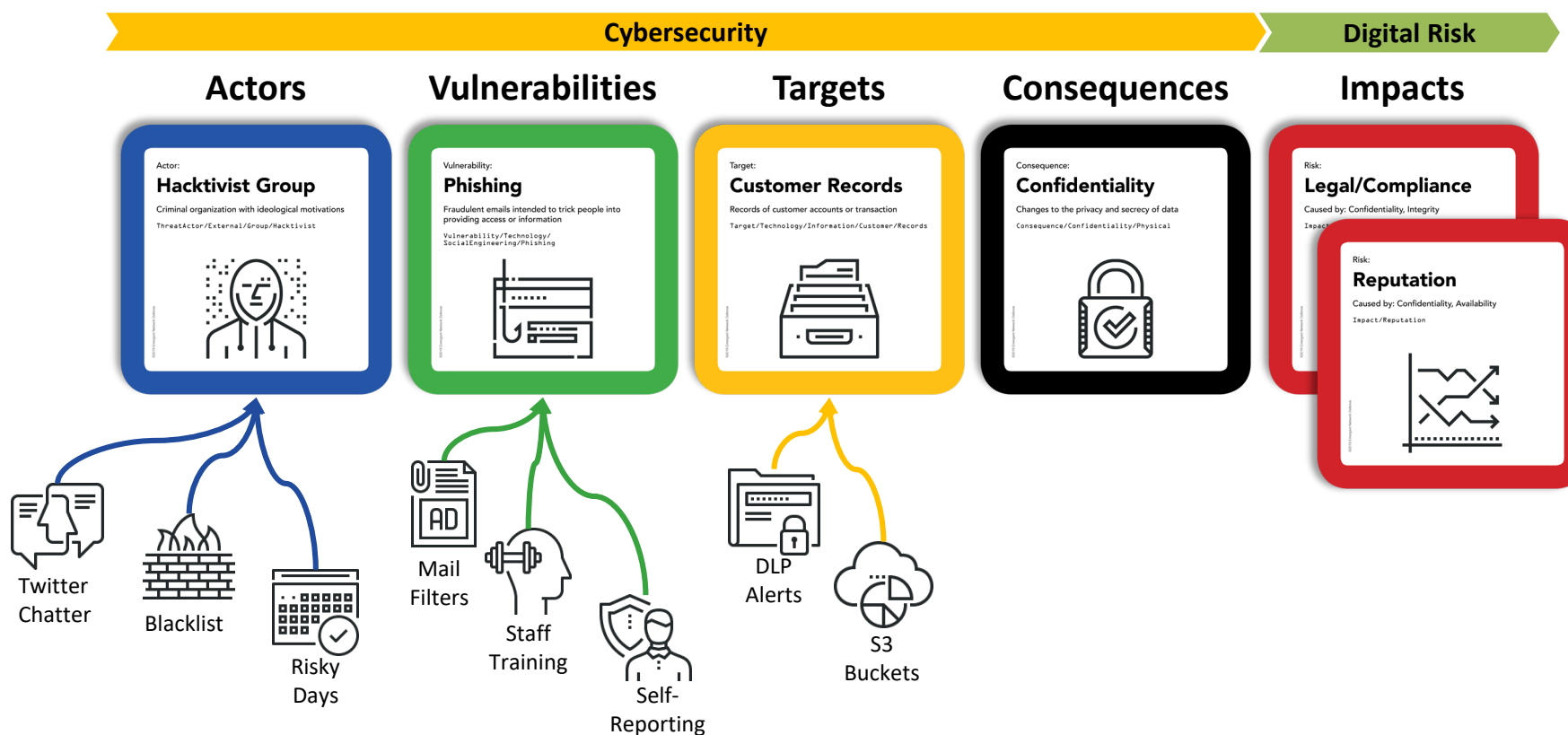


Progression of Risk Management Approaches



Scenario-Analysis Approach

Example Scenario: Hacktivists takes advantage of a **phishing** vulnerability that results in **data leak** of **customer records** that triggers a **legal** and **reputation losses**.



Composing Loss Exposure Scenarios

Scenario	Actor	Vulnerability	Target	Consequence
1. External Untrusted Malicious Actor uses vulnerability in 3rd Party network to gain access and compromise 3rd Party systems, resulting in theft of credentials	/ThreatActors/ External/ Untrusted/Malicious	/Systems/ITSystems/ Network/ 3rdParty	/BusinessAssets/Data/ Flow	Consequence/ Confidentiality/Leaked
2. Internal Untrusted Malicious Internal Actor mis-uses legitimate credentials to gain access to Internal sensitive systems, resulting in loss of network integrity	/ThreatActors/ Internal/ Untrusted/Malicious	/Architecture/Security/ TrustBoundaries	/BusinessAssets/Data/ Flow	Consequence/Integrity/ UnAssured
3. Internal Untrusted Malicious Actor installs malware on internal servers , enabling file transfer and commands outside of normal traffic flow, resulting in a loss of network integrity	/ThreatActors/ Internal/ Untrusted/Malicious	/LogicalSystemStack/OS/ Software/Installed	/LogicalSystemStack/ Network	Consequence/Integrity/ Impacted
4. Internal Untrusted Malicious Actor installs malware to exfiltrate Sensitive Data, resulting in leak of confidential information	/ThreatActors/ Internal/ Untrusted/Malicious	/LogicalSystemStack/OS/ Software/Installed	/Assets/Business/Data/ Customer	Consequence/ Confidentiality/Leaked



Reusing Exposure Objects allows for many more scenarios

Risk Modeling for Fun and Profit

Shall We Play A Game?



Shall We Play A Game?

Actor:

Hacktivist Group

Criminal organization with ideological motivations

ThreatActor/External/Group/Hacktivist



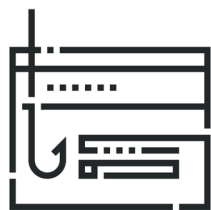
©2018 Emergent Network Culture

Vulnerability:

Phishing

Fraudulent emails intended to trick people into providing access or information

Vulnerability/Technology/
SocialEngineering/Phishing



©2018 Emergent Network Culture

Target:

Customer Records

Records of customer accounts or transaction

Target/Technology/Information/Customer/Records



©2018 Emergent Network Culture

Consequence:

Confidentiality


Changes to the privacy and secrecy of data

Consequence/Confidentiality/Physical



©2018 Emergent Network Culture

Lights, Camera, DOOMSDAY! (exercise time!)

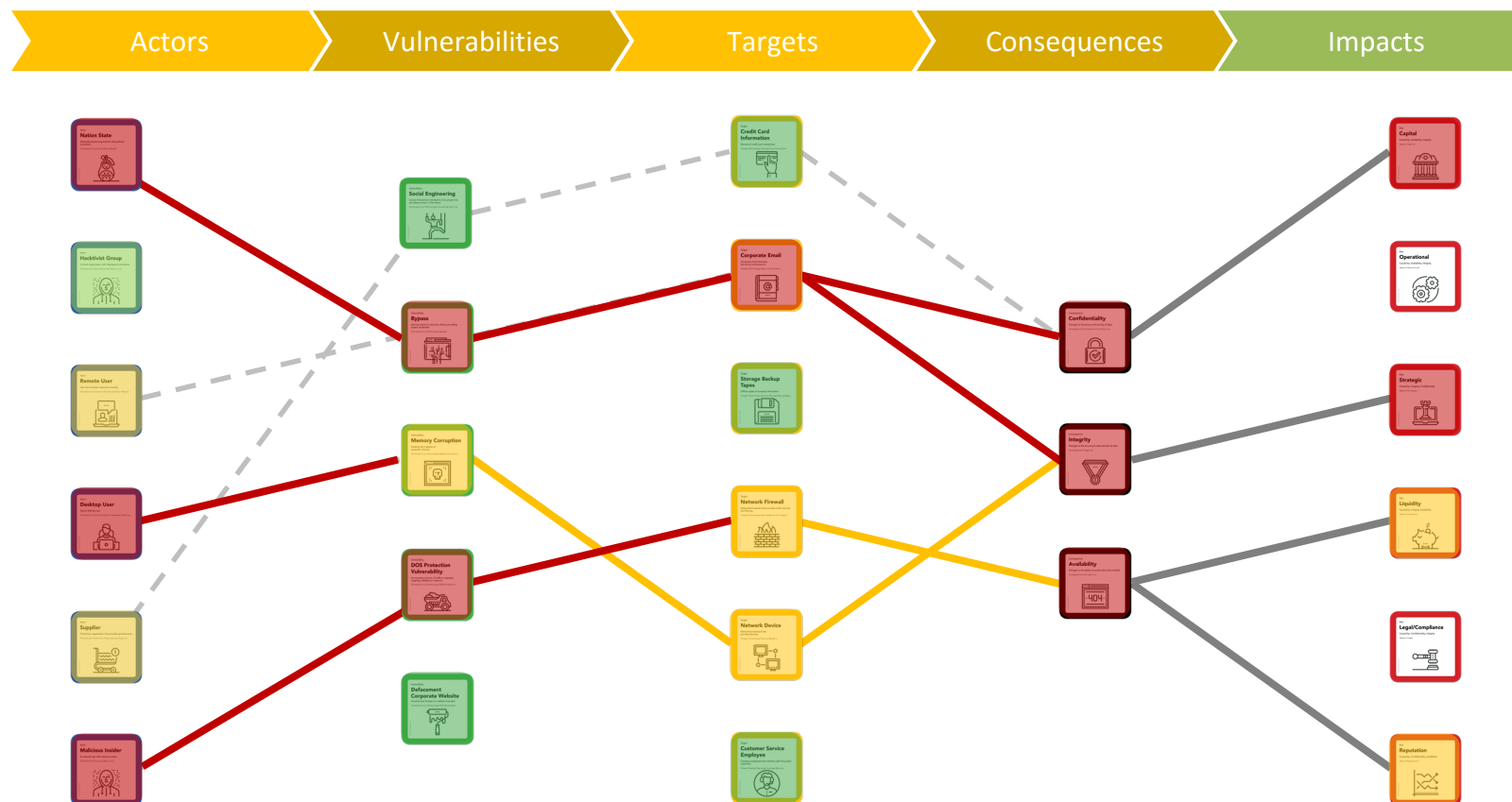
A black silhouette of a city skyline, featuring prominent skyscrapers like the Empire State Building. A large, dark silhouette of a giant monster, resembling Godzilla, is shown walking across the city from right to left. A purple speech bubble is positioned in the center of the image, containing the text 'Oh no. Someone alert the SOC!'.

Oh no. Someone
alert the SOC!

From your case study

- Use the cards to model out 2-4 scenarios that look like what happened in the case study (from the writeup or your own research.)
- Capture them at your table
- Decide on an impact (make it up. How many different ways could you determine it?)
- Use blank cards to create any objects you need

Swarm Algorithm to Discover New Scenarios

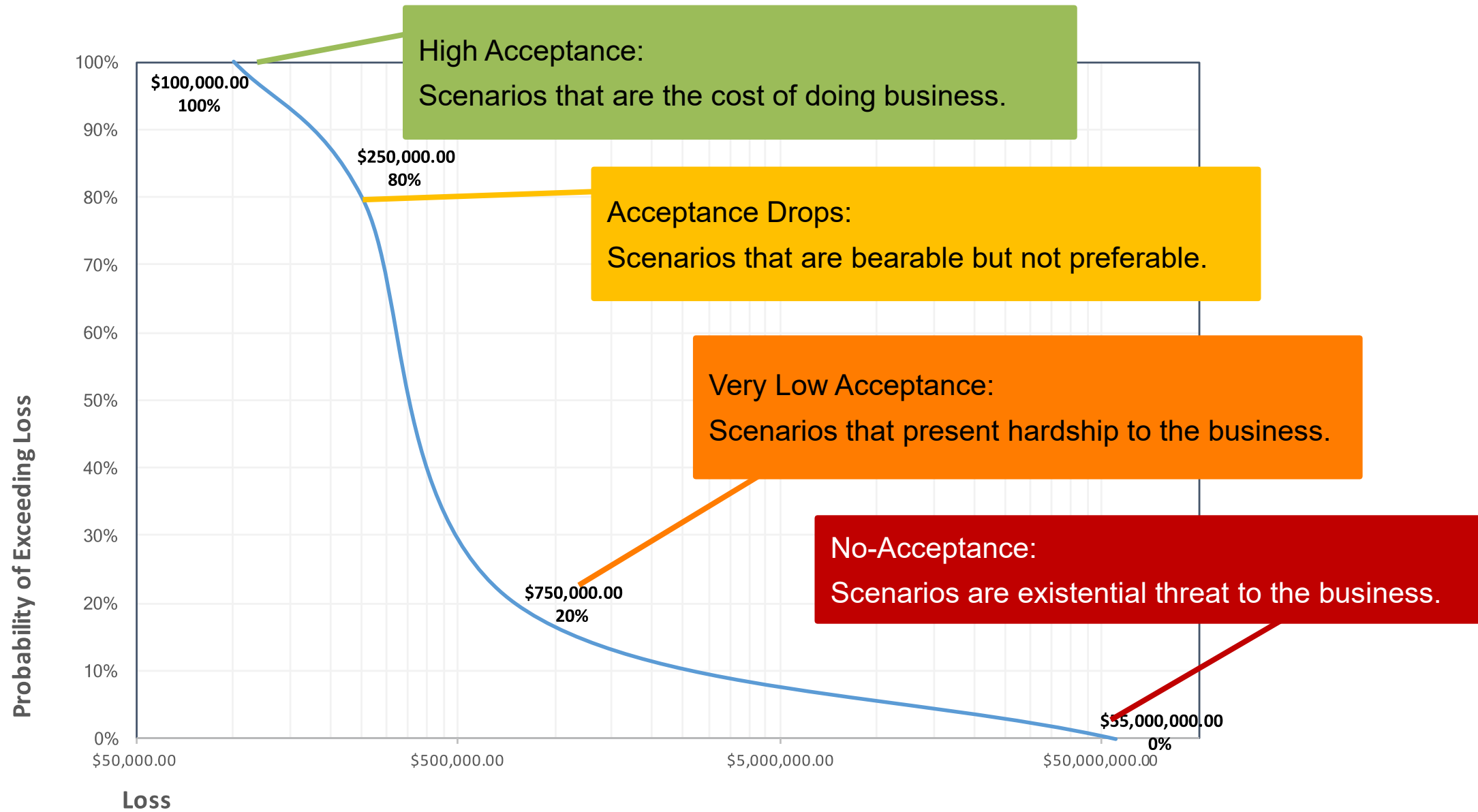


On Impact

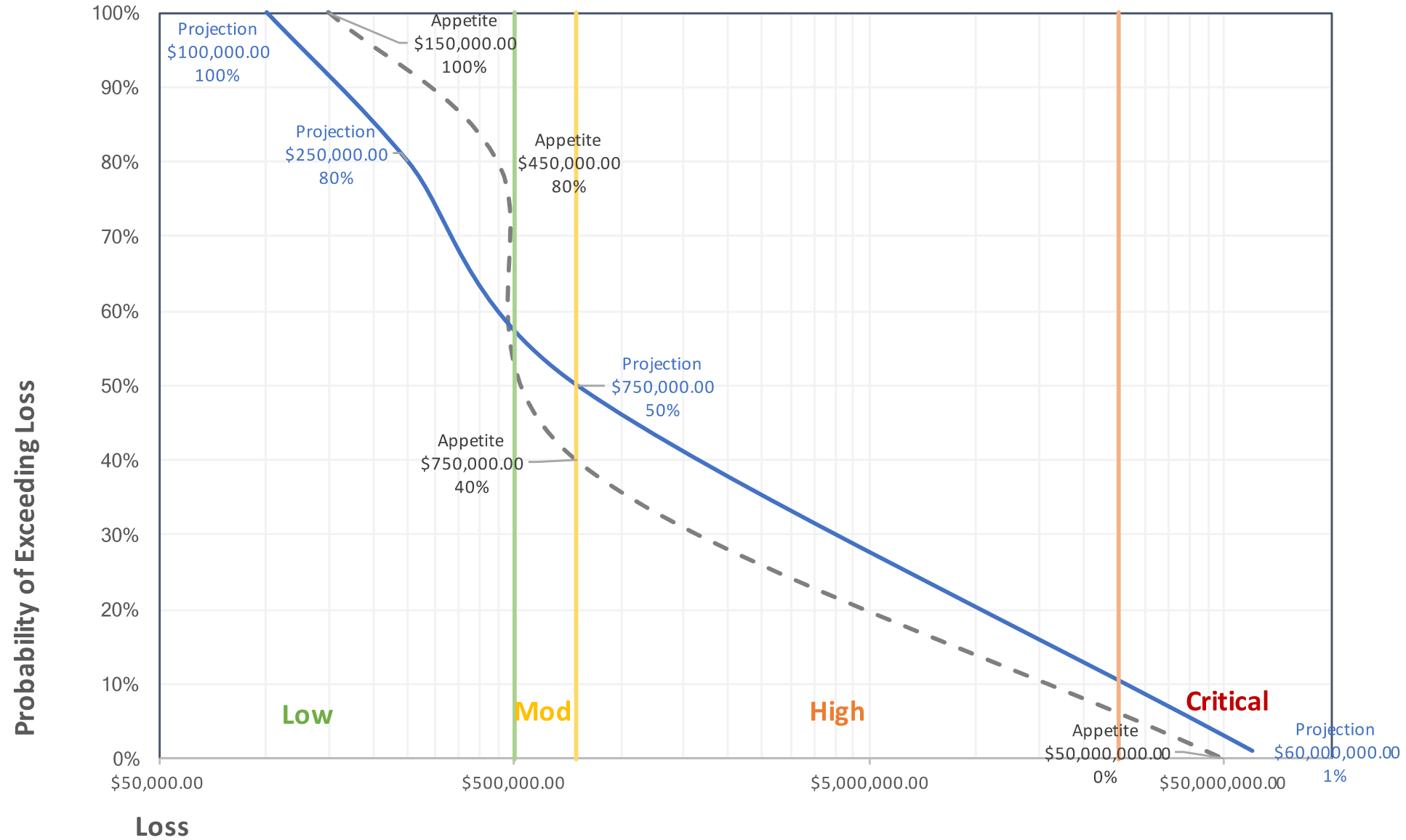
“How badly could it hurt us?”

“How much is too much?”

Business Impact & Risk Acceptance

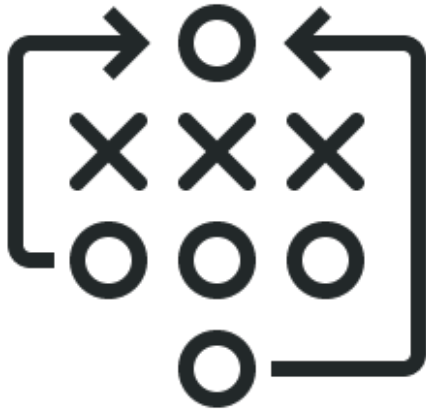


Projected Impact



Find Opportunities to

**Change your
Position**



**Change their
Mindset**



**Change the
Conversation**



RSA[®]Conference2019

Discussion/Questions?

Let's Make Risk a Game!



RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: LAB2-R10

THANK YOU!

Dr. Earl Crane



Founder, Chairman
Emergynt
@earlcranephd

Joel Benge



Strategist
ADG Creative
@joelmbenge

#RSAC