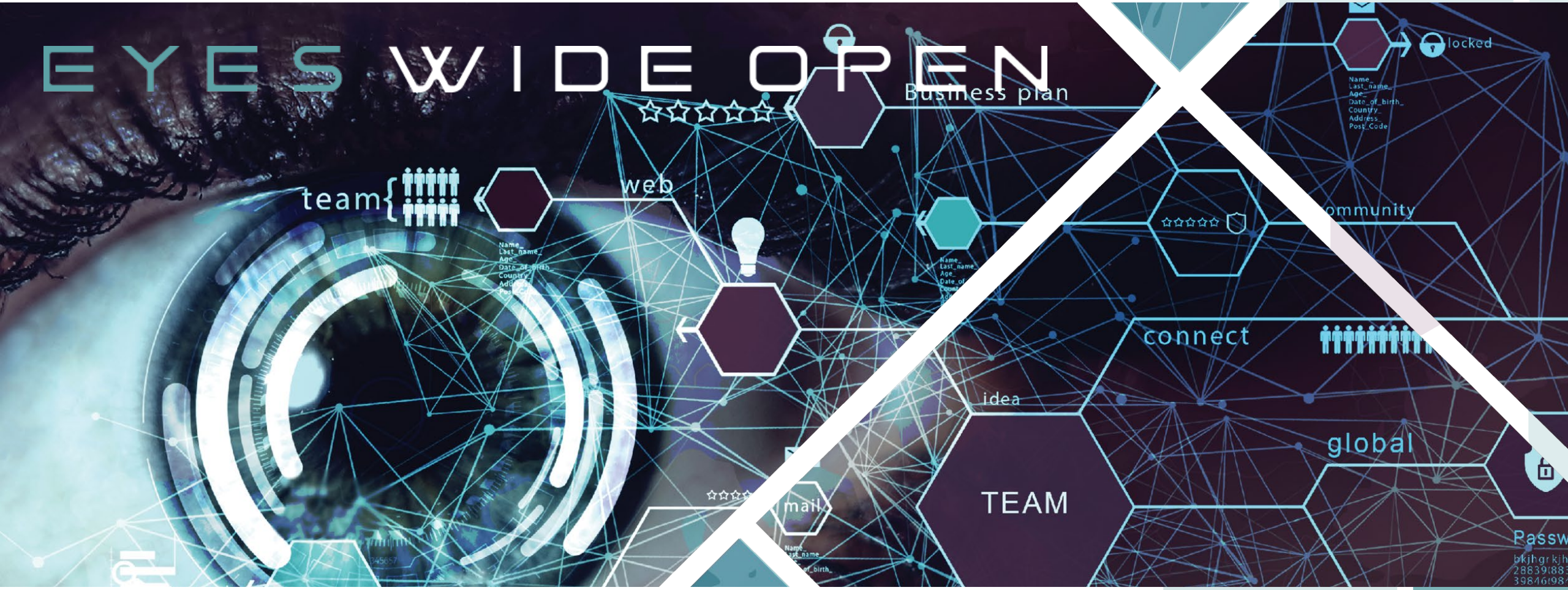
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



Cyber Risk Economics – We Can Be Better

Jeff Norem – Deputy CISO, Freddie Mac

Corey Tower – Sr. Manager, Cyber Risk Quantification, Freddie Mac

Andrew Herbert – Professional, Cyber Risk Quantification, Freddie Mac

Agenda

1. Overview of Cyber Risk Quantification
2. Gaining Buy-In and Understanding
3. 3 Questions CRQ Can Help You With
4. Passing on Lessons Learned
5. Questions

Brief Overview of Cyber Risk Quantification

Probabilistic Model

Techniques that considers modeling a range of potential adverse effects vs point values.

Factor Analysis of Information Risk (FAIR)

A framework that analyzes IT risk factors using Frequency & Magnitude

Data Inputs

Combination of consortium data, company-specific performance (e.g., controls, metrics, etc.), and industry knowledge to derive reasonable probabilities.

Monte Carlo Method

FAIR's statistical method that creates a frequency distribution by using randomly selected "what-if" scenarios for each calculation.

Challenges Building CRQ Program

This Will Be a Culture Change

We don't have enough data or cyber is to dynamic to measure

I am not a mathematician

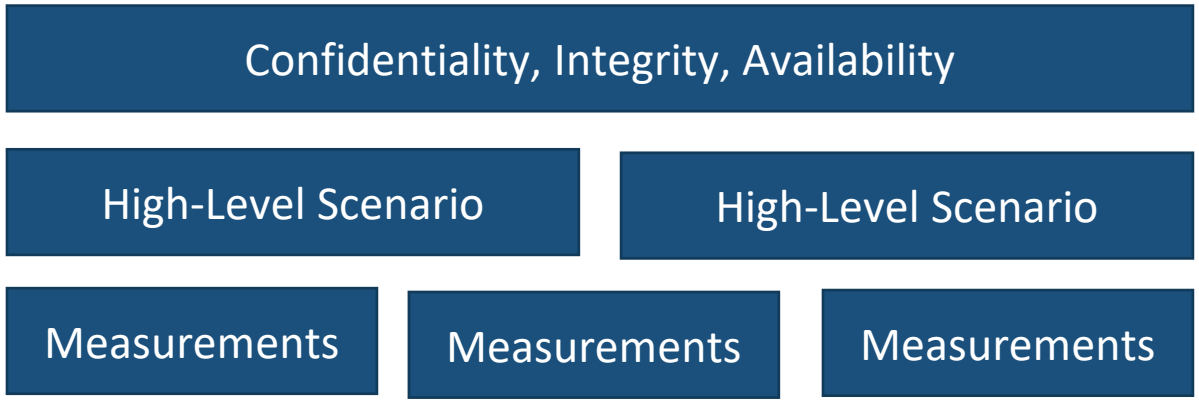
Its too subjective

Leverage the Community: fairinstitute.org

Three Questions CRQ Can Help You With

"How much risk do I <u>actually</u> have?"

Risk Reporting vs Measurements



How You Report Risk

Applicable Risk Scenarios

Tactical Control Measurements

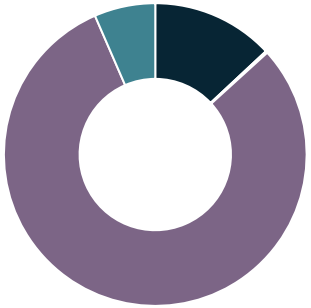
*Mock Example

Availability Loss

Aggregate Risk

Average Annualized Loss Exposure

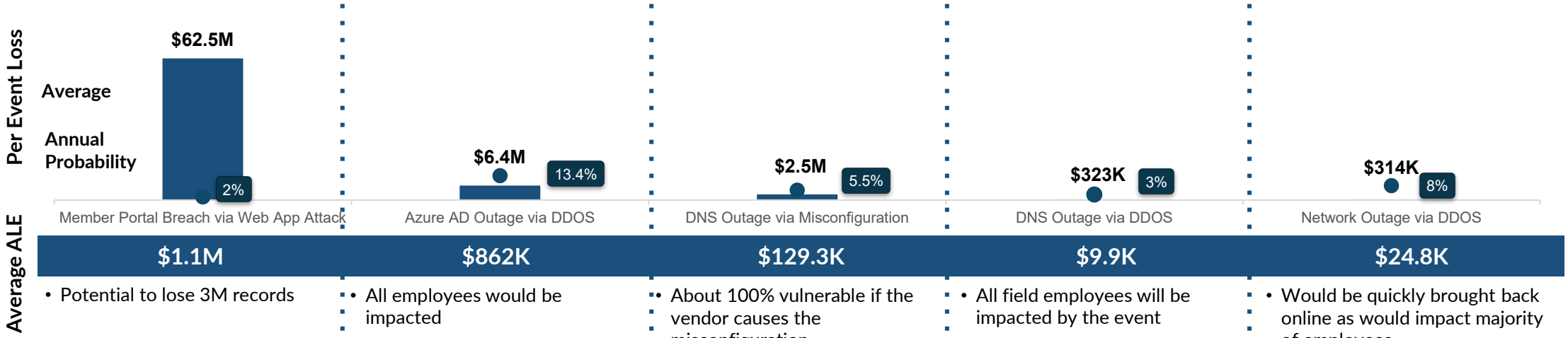
Min – Average - Max



- Inability for clients to access their accounts as well as employees unable to complete their job duties
- Fines and Judgements associated with missed SLAs
- Significant losses associated with responding to clients or reporting to regulators

Aggregated average loss by effect

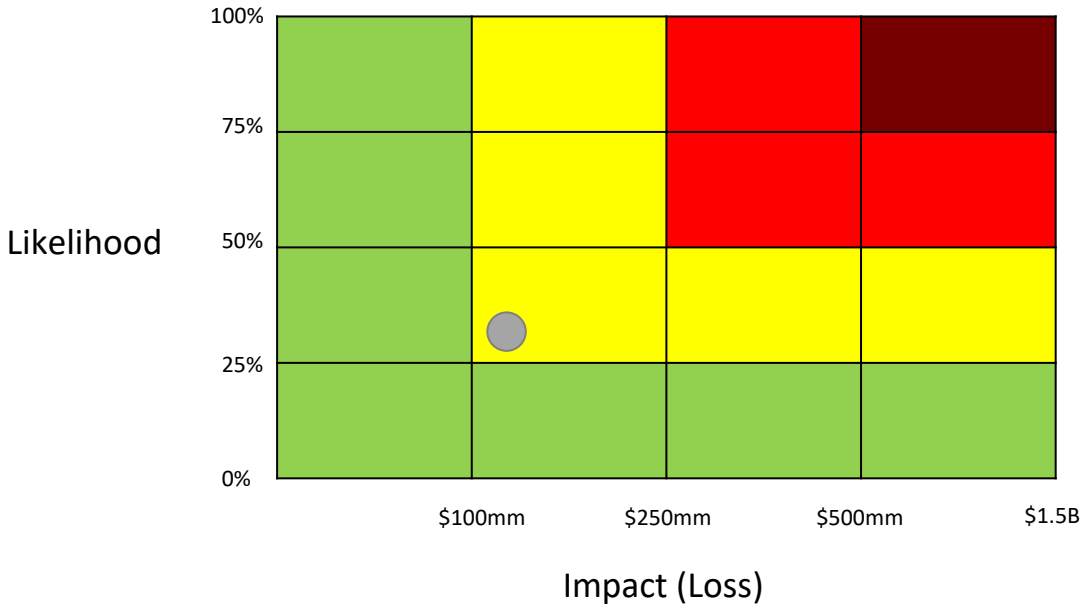
Top 5 Risk Scenarios

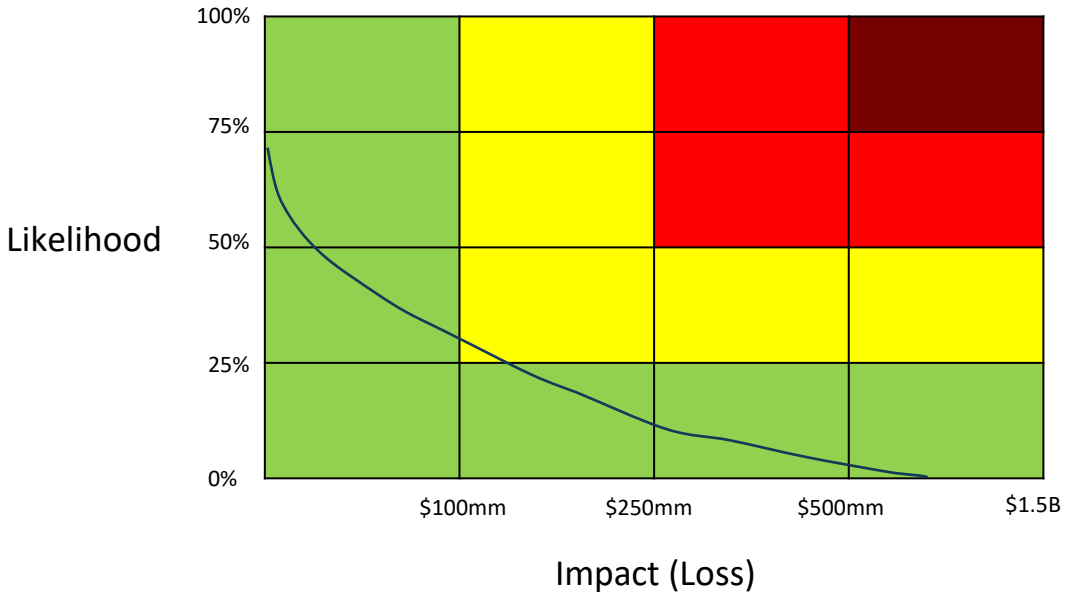


- Potential to lose 3M records
- All employees would be impacted
- About 100% vulnerable if the vendor causes the misconfiguration
- All field employees will be impacted by the event
- Would be quickly brought back online as would impact majority of employees

Point Value vs Loss Exceedance Curve

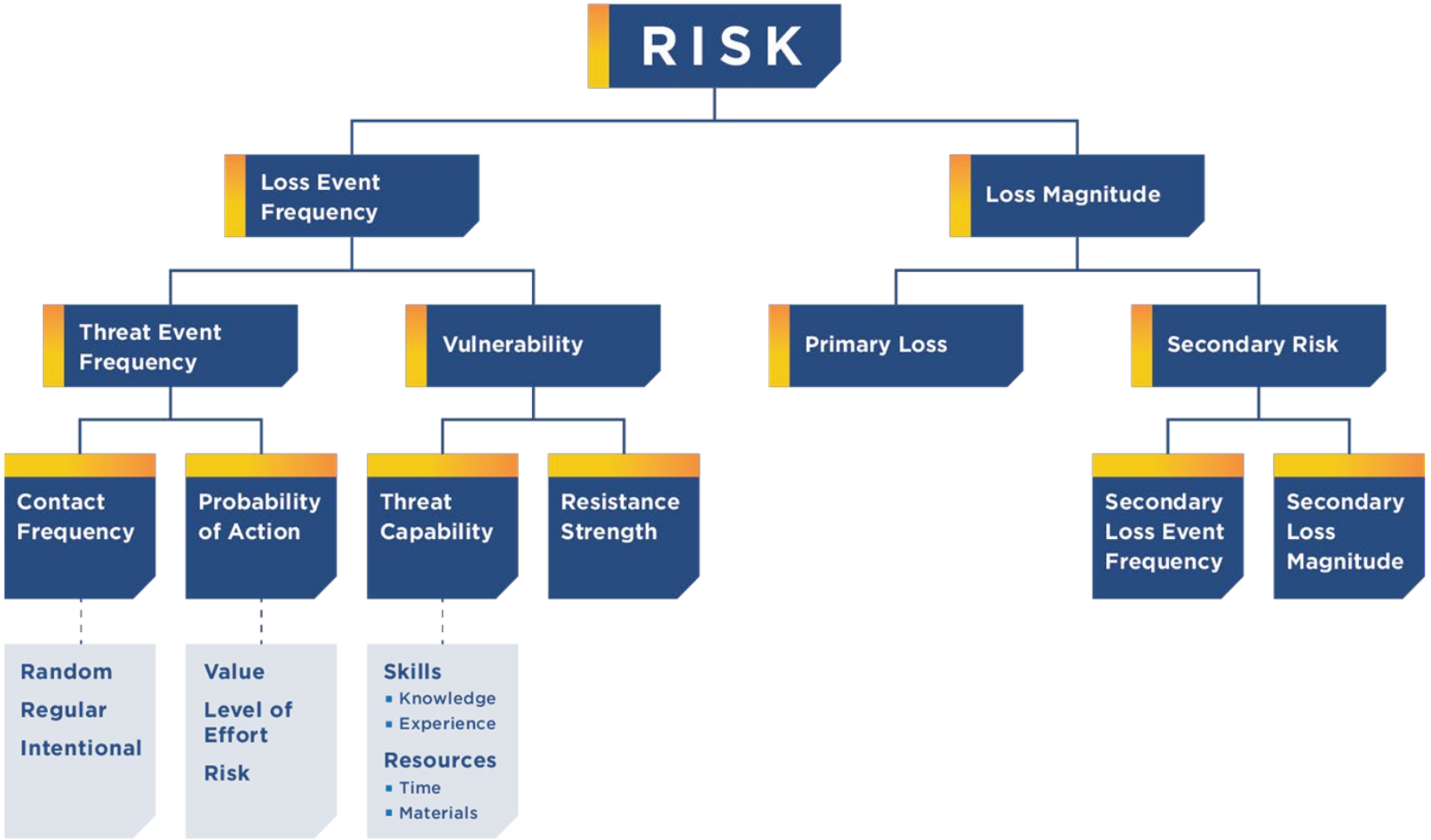
Same Risk – Two Different Views



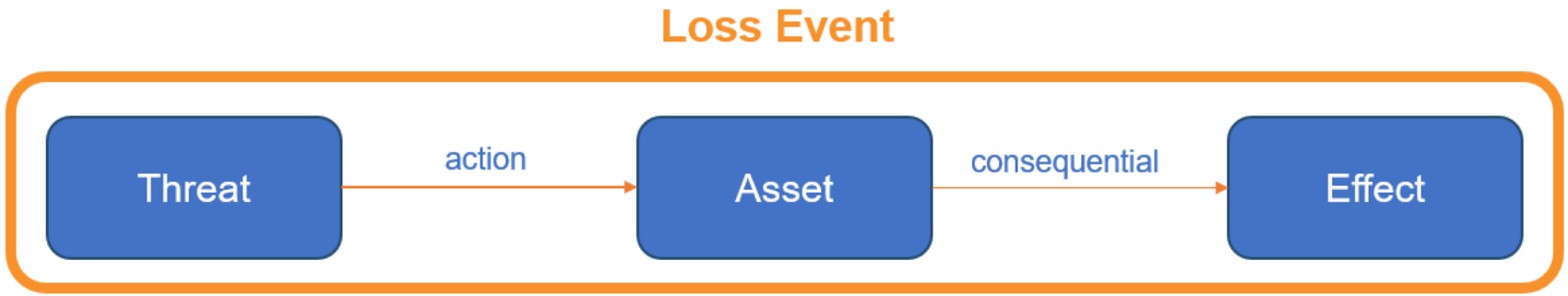


“Everyone at my organization thinks about risk differently”

Using a Quantitative Risk Taxonomy



Scoping Scenarios



Anything, actor or agent, capable of acting against an asset in a manner that can result in loss

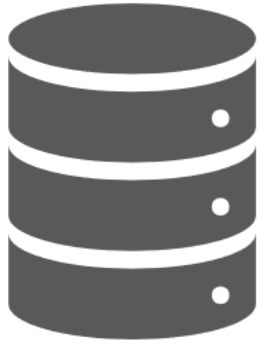
Anything of value that can be affected in a manner that results in loss

How loss materializes within a given asset

Scoping Scenarios

External Malicious

Breaches PII
(**Confidentiality Effect**)
from



Database X

How much risk do we face from
cybercriminals breaching the **confidentiality**
of sensitive data **(PII)** in **Database X**

“I have a limited budget and not everything can be fixed”

Roadmap vs Budgeted Roadmap

Security Roadmap	**Budget**
$68mm	$6.8mm

Question: Which of the $68mm in Control Efforts Do You Spend $6.8mm?

Common answer: *“The ones that get me the most amount of risk reduction”*

*Mock Example

Comparative Analysis

DNS – Risk Comparison (EXAMPLE ONLY)

Compares how risk changes based on different levels of remediation

Comparison Insight
Risk is significantly reduced upon implementation of Brand Protection

	Current Exposure	Implementing Brand Protection	Zscaler (example)
Average Per Event Loss	$2.4M	$2.3M	$1.8M
Average ALE	$130.4K	$17.6K	$43K
Annualized Risk Reduction	-	-$112.8K	-$86.9K
Estimated Cost	-	$101K	$10K
Return on Investment (per $ spent)	-	$1.30	$1

Figures shown in Annualized Loss Exposure

Lessons Learned from Deploying CRQ

Start slow, just start doing assessments and show the value, find a key stakeholder and help them solve a problem

Don’t over think it. People, Process, Technology just like everything else. Build your culture.

Manage expectations early and often. Take a pragmatic approach (qualitative isn't perfect and neither is quantitative).

Questions?