Making Better Cyber and Technology Risk Decisions: Part 1

Jack Jones
Chairman
FAIR Institute

The risk landscape in a nutshell…

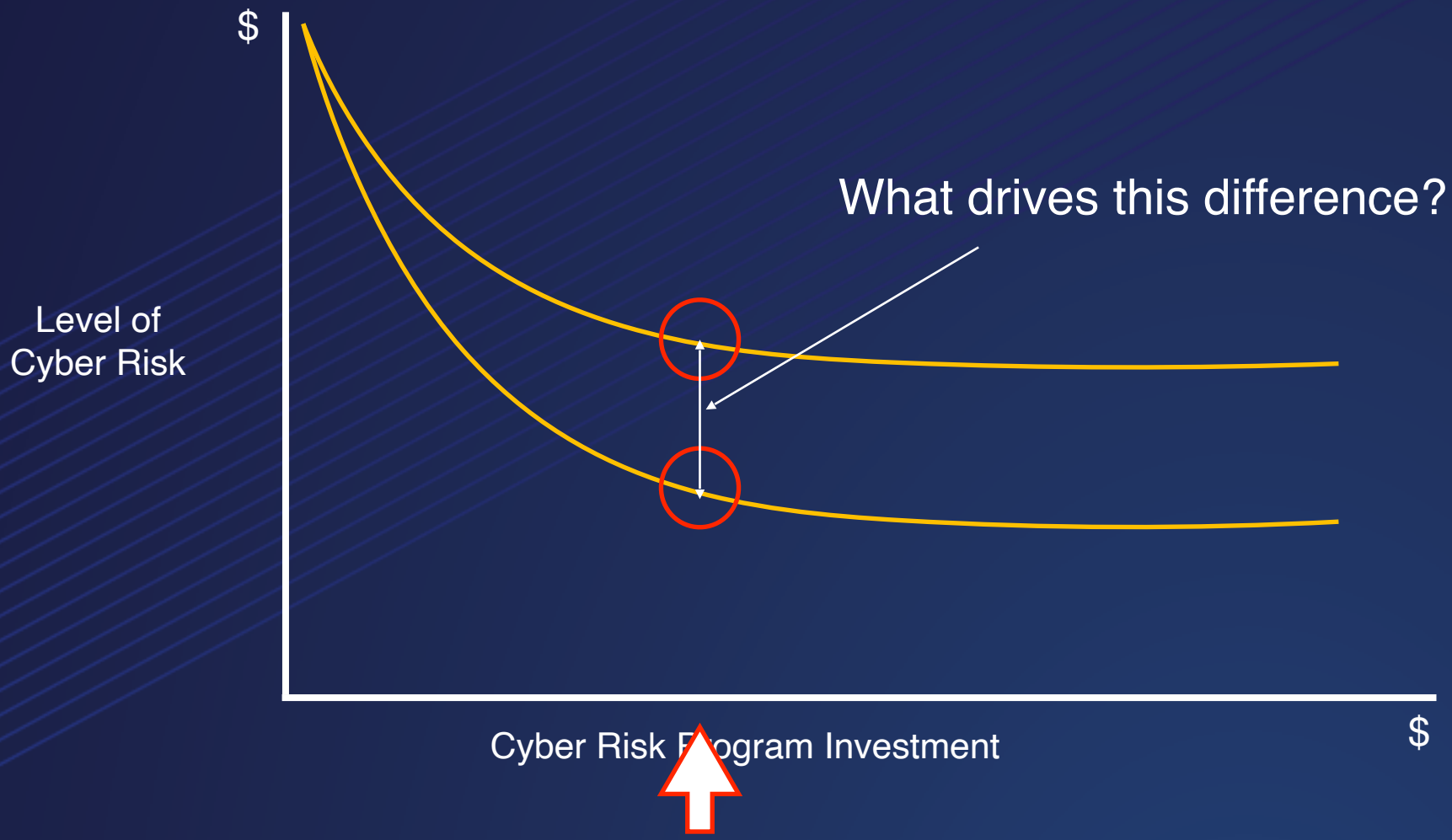
Complex

Dynamic

Limited Resources

Makes effective prioritization an absolute necessity.

The importance of being cost-effective



Decisions

Prioritization and solution choices.

How much do they really understand?

Two fundamental truths about prioritization…

Prioritization is always based on some form of comparison

Comparisons are always based on some form of measurement

The more normalized the measurement, the better comparisons and priorities will be.

Prioritizing Effectively

Three criteria for reliable risk measurement…

1. Clarity about what's being measured
2. An accurate risk model
3. Data

Getting clarity

Which of the following are risks?

- Disgruntled insiders
- Reputation
- Untested recovery process
- Network shares containing sensitive consumer information
- Weak passwords
- Cyber criminals

Actually, none of them are risks

- Disgruntled insiders — Threat community
- Reputation — Asset
- Untested recovery process — Deficient control
- Network shares containing sensitive consumer information — Assets
- Weak passwords — Deficient control
- Cyber criminals — Threat community

The classic formula for risk

Risk = Likelihood x Impact

Likelihood and Impact of what?

Loss Event Scenarios

These aren't loss events

You can only assign likelihood and impact to loss event scenarios.

- Disgruntled insiders
- Reputation
- Untested recovery process
- Network shares containing sensitive consumer information
- Weak passwords
- Cyber criminals

A measurement example

How fast are they going?

Qualitatively

Challenges…

- Is your “Fast” the same as mine?
- Which car am I referring to?
  - One in particular? (Slowest? Fastest?)
  - An average for all of them?
- Which part of the track am I referring to?
  - Corners?
  - The straightaway?
  - Average over the entire track?
  - This lap, or an average for the entire race?

Measuring speed

Requires three elements:

1. The scope of what's being measured
   - Which car(s)?
   - Which part of the track?
   - Which lap(s)?
2. An analytic model
   - What data? (time, distance)
   - How to apply the data? (speed = distance/time)
3. Data

Measuring risk

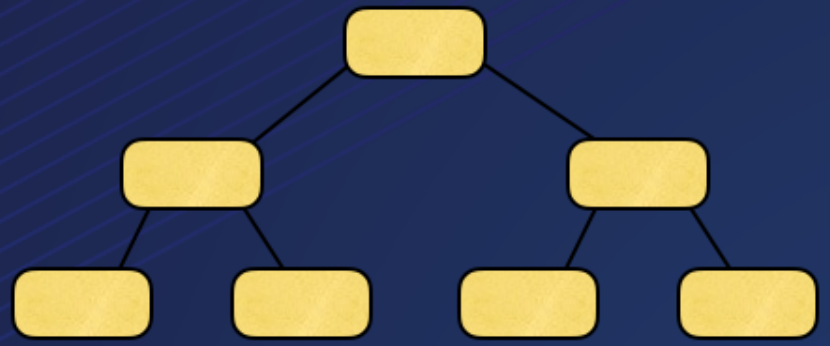
Every risk measurement involves three elements:

1. The scope of what's being measured
   - What asset?
   - What threat?
   - Which vector?
   - Which controls are relevant?
   - What type of event (e.g., C, I, A)?
2. An analytic model (e.g., FAIR)
   - What data?
   - How to apply the data?
3. Data

Without clear scoping, the odds of measuring risk accurately are much lower…

…regardless of whether you're doing qualitative or quantitative measurement

Models



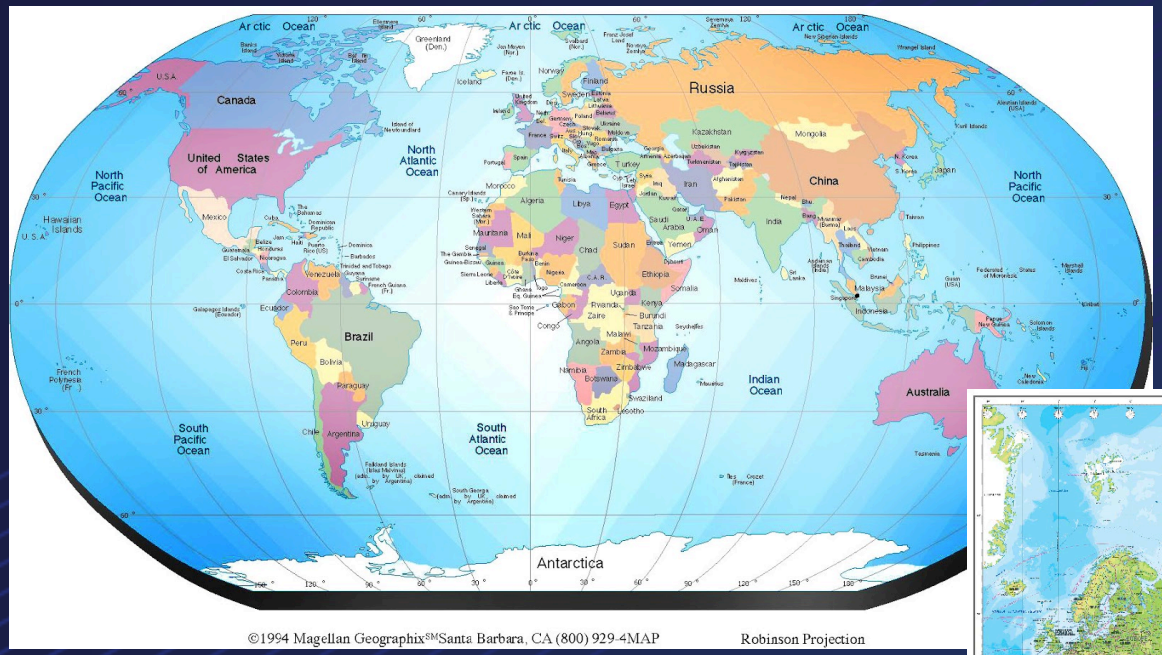
A model is a simplified representation of reality used to simulate, explain, and make predictions.

"All models are wrong, but some are useful."

George Box

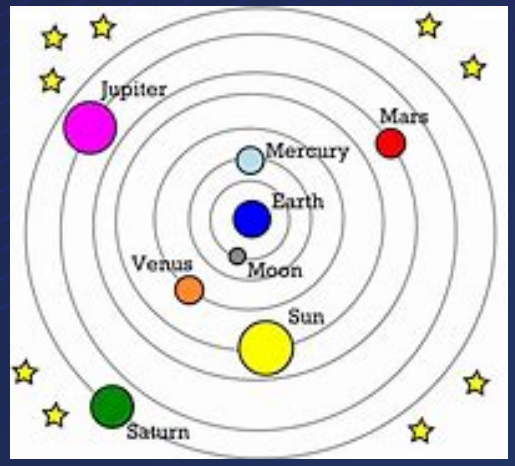
But there are different types and degrees of "wrongness"…

“Wrong” models…



Wrong, in that they aren’t perfect replicas.

A different kind of wrong…



A broken risk model (half of one, anyway)

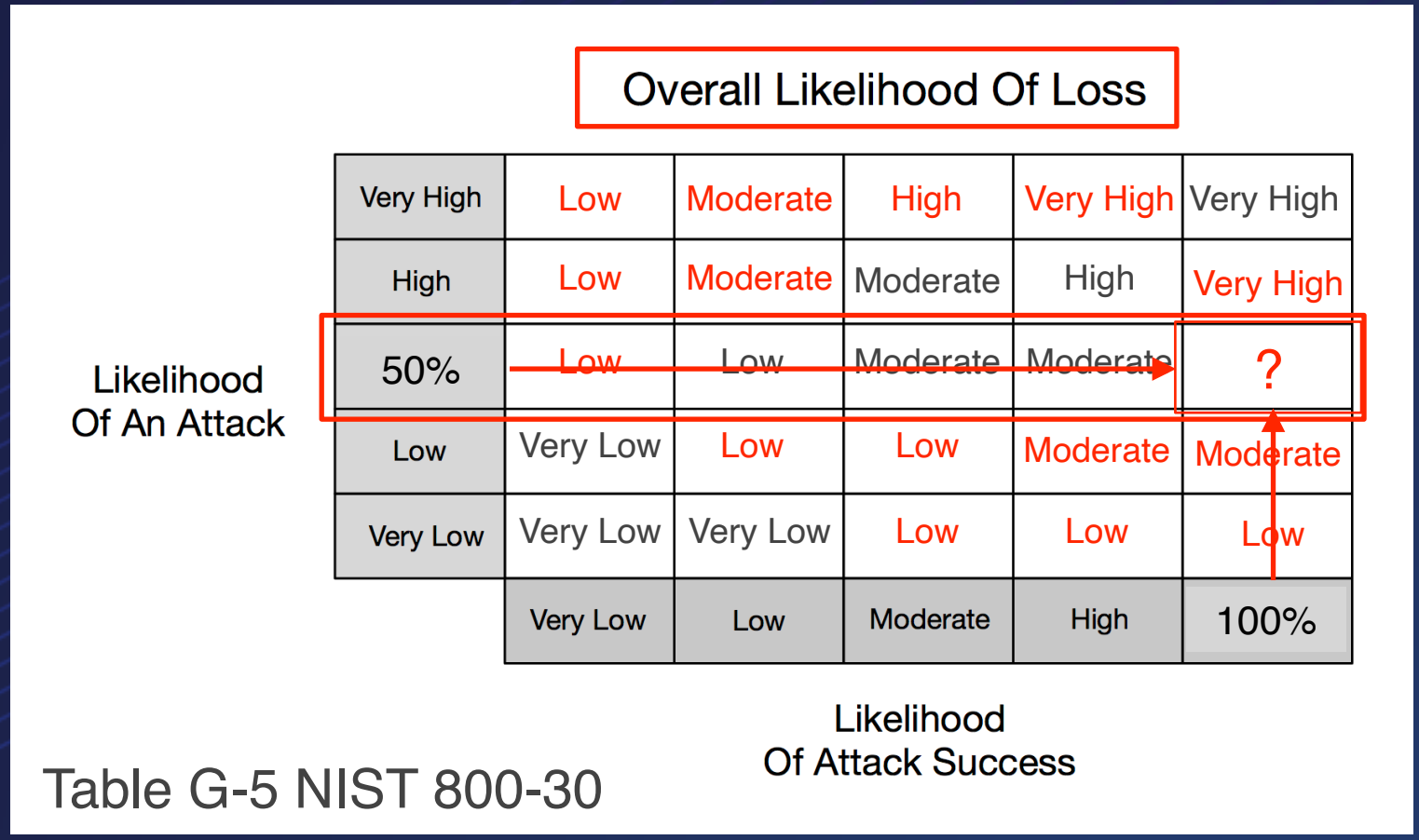
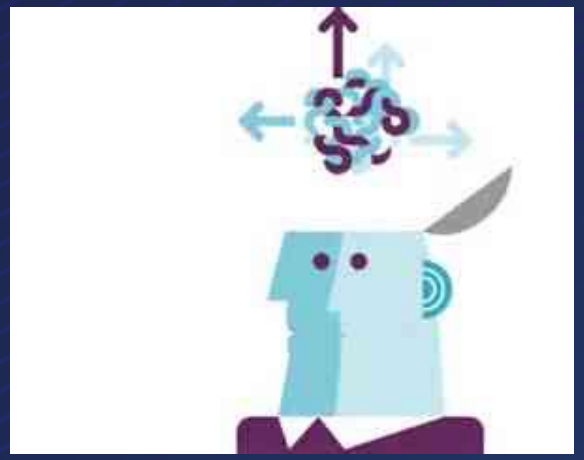


Table G-5 NIST 800-30

What is the most commonly used cyber risk measurement model?



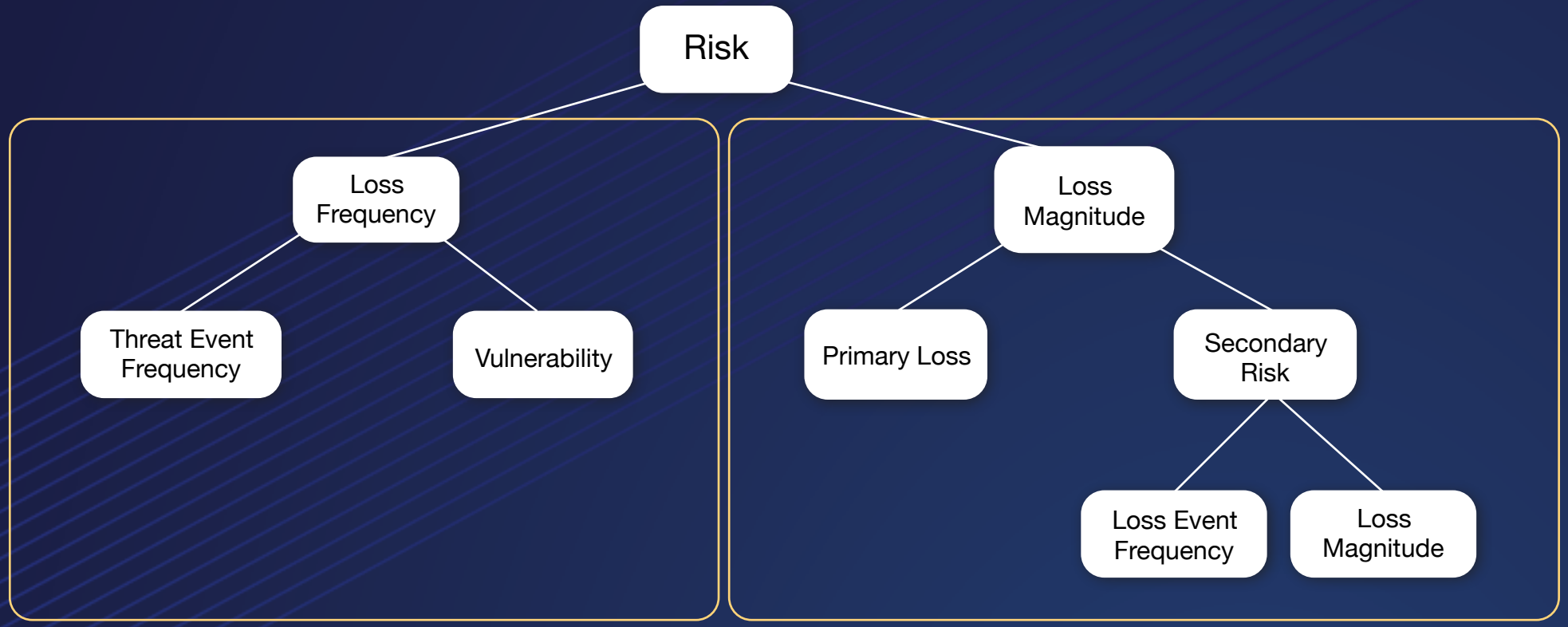
Mental models

What assumptions?

What data?

What formula?

The FAIR Model



Loss Event Frequency

Loss Magnitude

But what about data?

“We don’t have enough data.”

- “You have more data than you think you do.”
- “You need less data than you think you do.”

Douglas Hubbard

Author of “How to Measure Anything”

Questions for any risk analysis…

- What data do we need? The risk model tells us this
- Where do we get them? The scope tells us this
- How do we apply them? The model tells us this

If the analysis is scoped clearly and you're using a well-defined model, then data will be far less challenging to gather and use.

The problem of uncertainty…

How tall am I?

Uncertainty is inevitable. It's simply a matter of whether it's accounted for in measurement inputs and outputs.

Communicating Effectively

Which of these will most executives understand?

- A marketing campaign that is expected to generate $1M to $2.5M in additional revenue over the next 12 months.
- A cost-cutting initiative that will trim approximately $1.3M in expenses this year.
- A cybersecurity initiative that will enable early detection of breaches, improving this from “High risk” to “Medium risk”.

Enabling informed comparisons

- A marketing campaign that is expected to generate $1M to $2.5M in additional revenue over the next 12 months.
- A cost-cutting initiative that will trim approximately $1.3M in expenses this year.
- A cybersecurity initiative that will enable early detection of breaches, reducing loss exposure by approximately $10M.

Weak password

Missing patch

Cyber criminals

Outdated policy

Which of the “Highs” is highest?

No monitoring

Weak encryption

Inappropriate access privilege

Highest “Medium” vs. lowest “High”?

Limited logging

Flat architecture

How much risk is there in total?

No backups

Local admin privileges

Disgruntled insiders

Unencrypted PII/PHI

Where are lines drawn, and why?

Very High (5)

High (4)

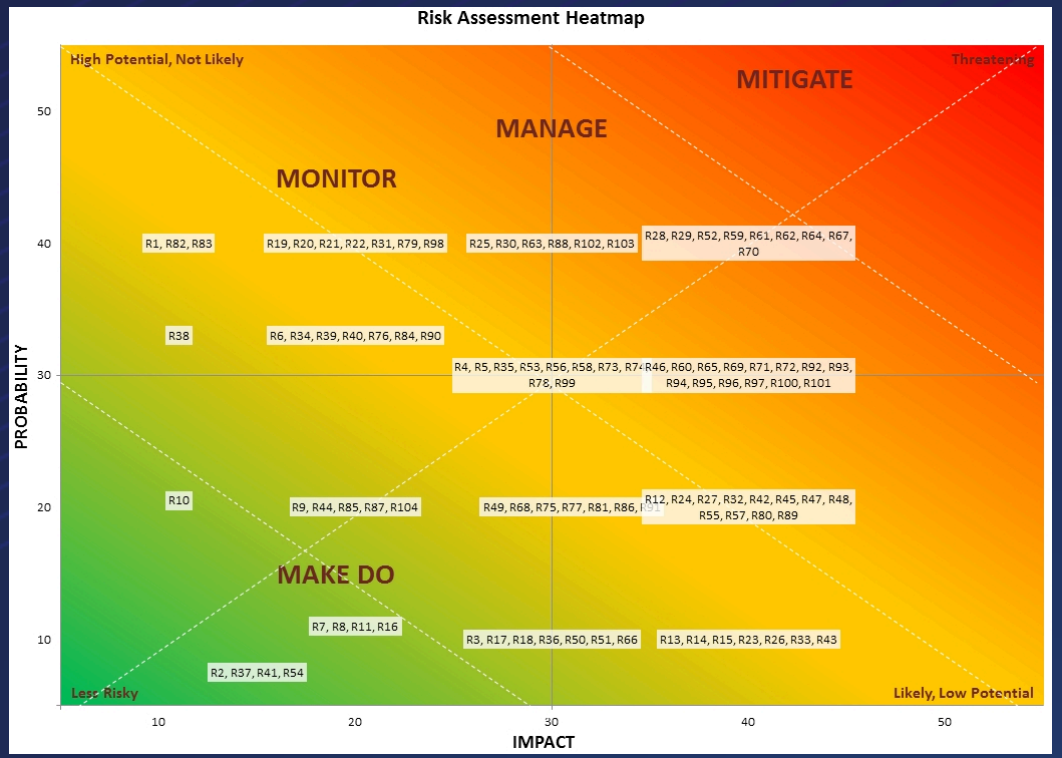
Medium (3)

Low (2)

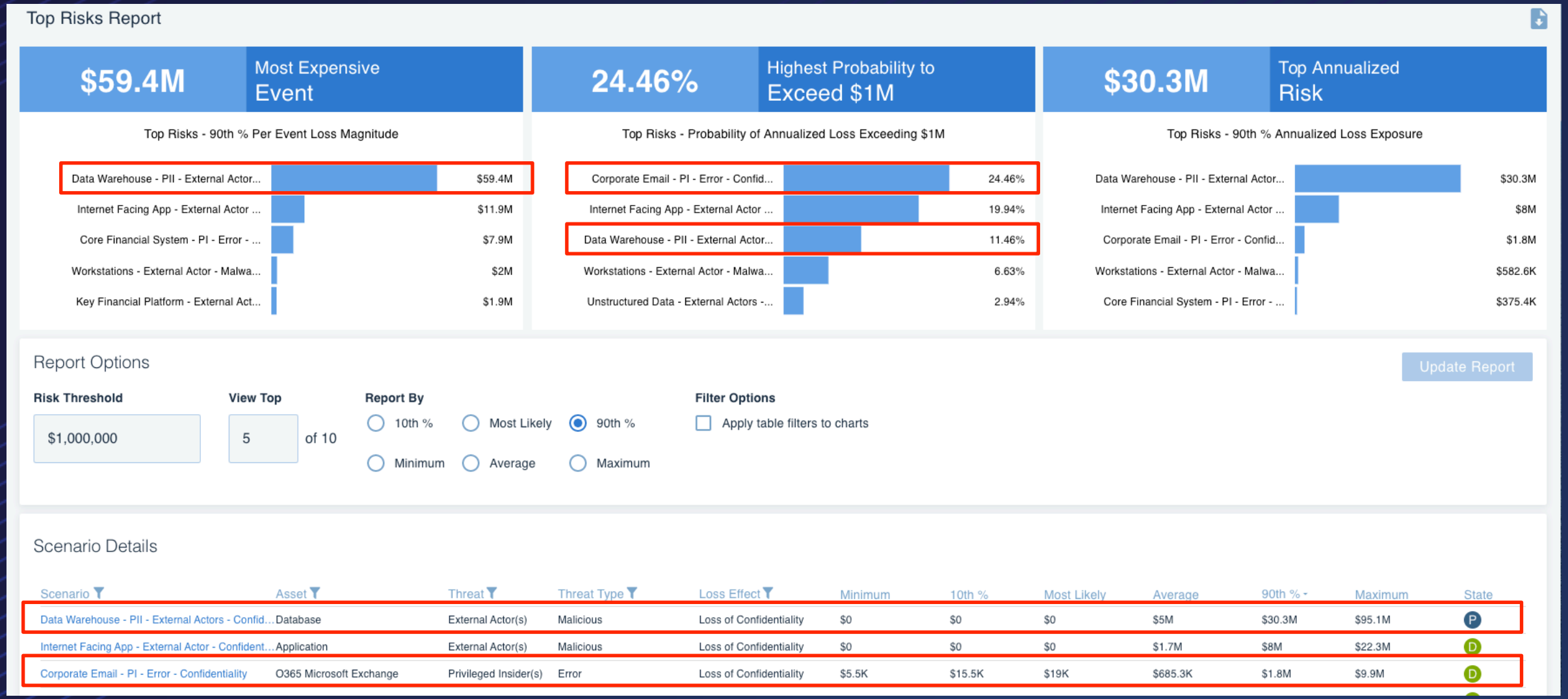
Very Low (1)

Prioritizing amongst risks qualitatively

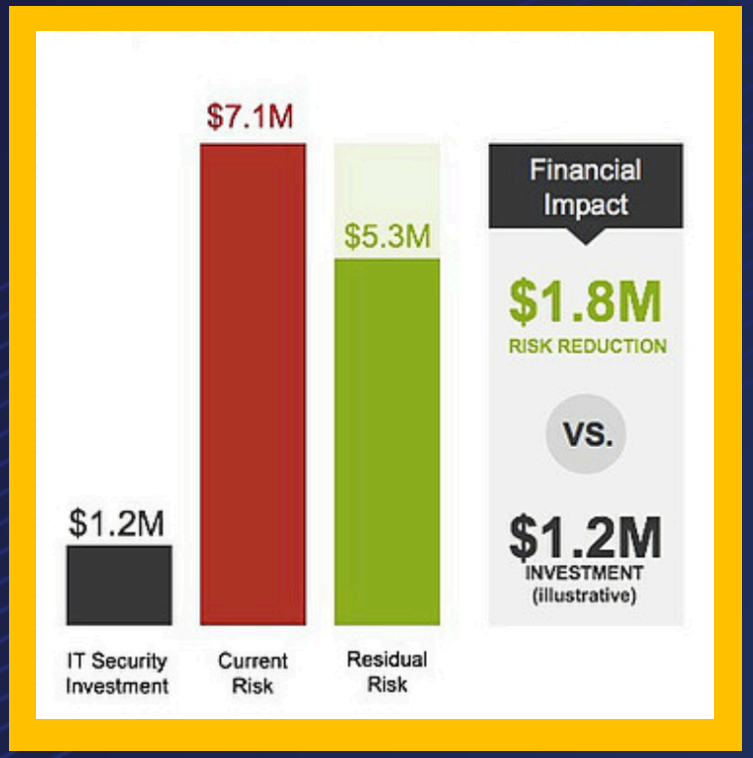
Risk Statement	Likelihood	Impact	Velocity	Score
IT projects not managed in terms of budget, scheduling, scope, priority, and delivery	3	3	3	27
No process for identifying and allocating costs attributable to IT services	3	3	3	27
Failure to make adequate plans for continuation of institutional business processes (e.g., admissions, academic, operational activities, and research) in the event of an extended IT outage	3	3	3	27
No coordinated vetting and review process for third-party or cloud-computing services used to store, process, or transmit institutional data	3	3	3	27
Failure to designate leadership (e.g., an individual or individuals) for institutional oversight and strategic direction for information security activities	2	3	3	18
No succession plan for key institutional IT leaders (e.g., CIO, CISO, CTO, CPO, etc.)	3	3	2	18
Incorrect information on public-facing institutional resources (e.g., website, social media streams)	3	2	3	18
IT management aims and directions not communicated to critical user areas	3	2	2	12
No process for managing IT problems to ensure they are adequately resolved or for investigating causes to prevent recurrence	2	2	3	12
Failure to designate leadership (e.g., an individual or individuals) for institutional oversight and strategic direction for IT operations	1	3	3	9
Relevant stakeholders not included in important IT investment decisions (e.g., priorities, technologies, new applications)	2	2	2	8
No process for measuring and managing IT performance	2	2	2	8
IT governance and priorities not aligned with institutional priorities	3	2	1	6
IT assets (e.g., hardware, devices, data, and software), systems, and services outdated, do not support institutional needs (admissions, academic, business operations, research, etc.)	3	2	1	6
Lack of shared understanding by IT and business units that affects IT service delivery and projects	3	2	1	6
IT assets (e.g., hardware, devices, data, and software) and systems not prioritized based on their classification, criticality, and institutional value	3	1	1	3

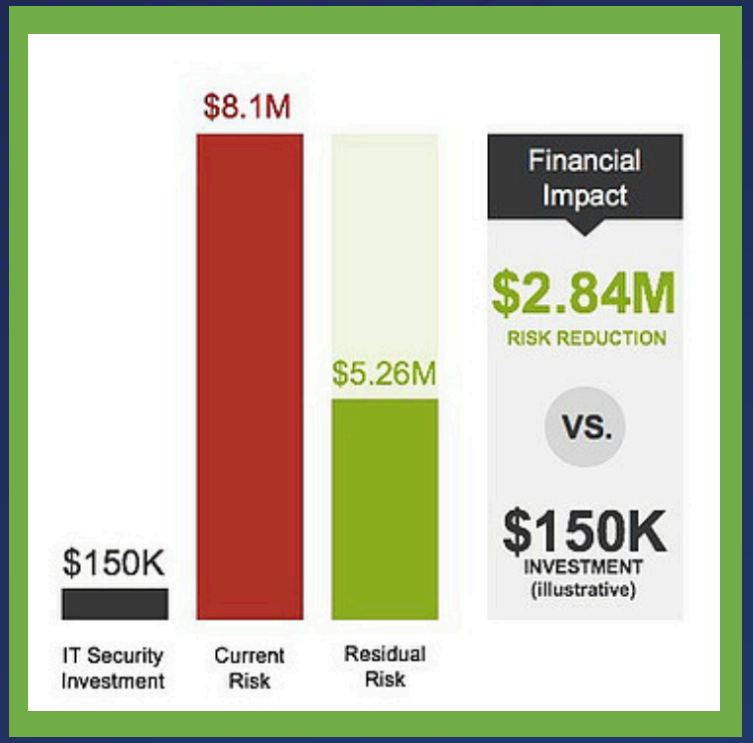


Prioritizing amongst risks quantitatively

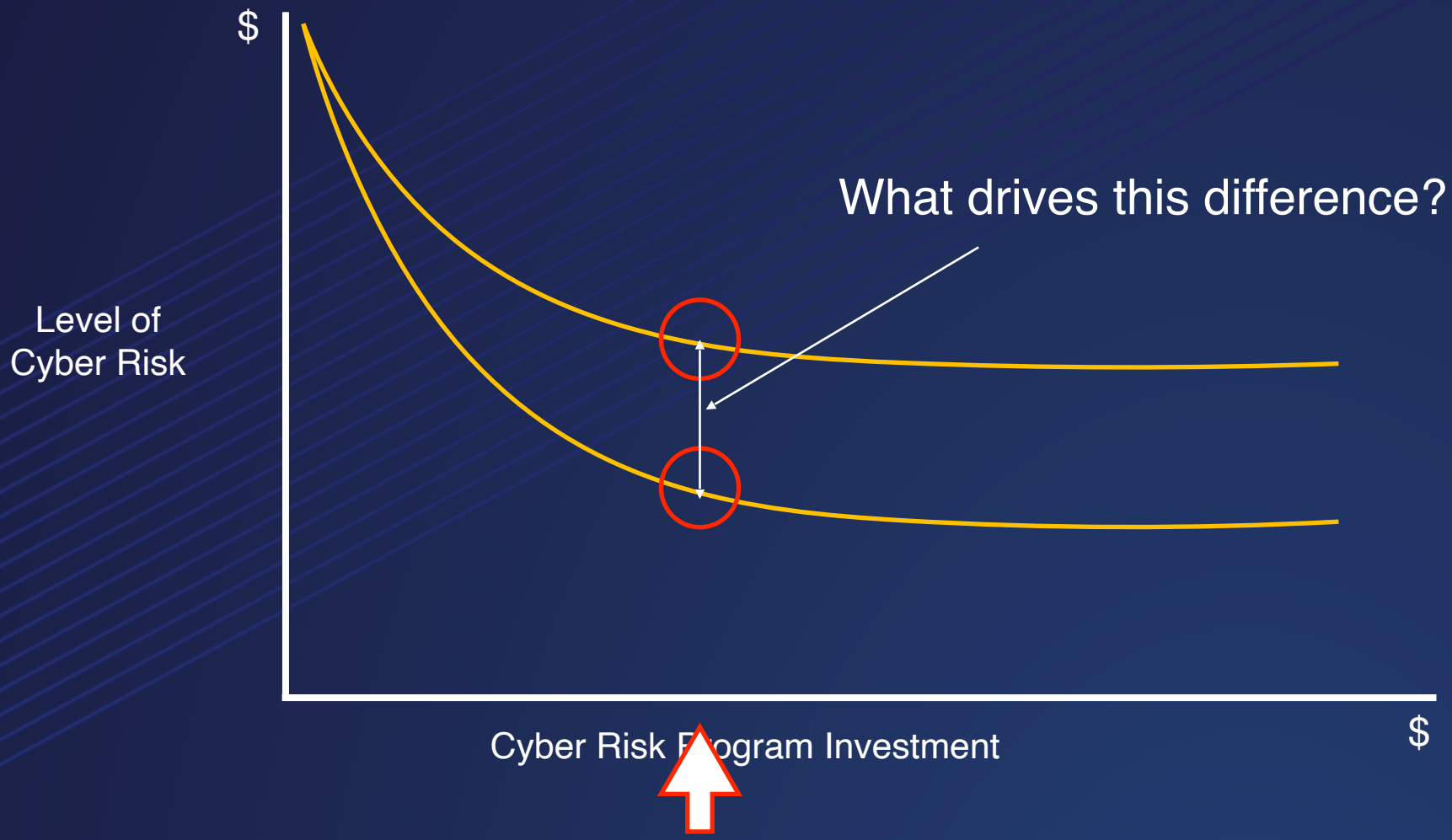


Cost-benefit comparisons





Remember this?



Wrapping up

Contributing to every breach…

Poor prioritization, wasted resources and ineffective communication

Making better cyber and technology risk decisions

- Three fundamental requirements for reliable risk measurements:
  - Clarity: You can't reliably measure what you haven't clearly defined
  - An accurate model: All models are imperfect — but some are fundamentally broken
  - Data: Data will always have uncertainty. The key is to faithfully account for and communicate uncertainty.
- Decisions are always based on priorities.
- Prioritization is always based on comparisons, which are based on measurements.
- If we want risk to be on an even playing field with other organization priorities, we have to measure and communicate risk in financial terms.

In the next webinar in this series…

…I'll walk thru an example analysis comparing and contrasting common qualitative practice vs. a quantitative approach.