Myth-Busting Risk

Jack Jones
SVP IT Risk, CISO
Huntington Bank

What we'll cover...

- What do we mean by "risk"?
- Common myths
  - The dirty word of measurement...
  - My crystal ball is fuzzy...
  - Data? What data?
  - There's quantitative and then there's "quantitative"
  - Infosec professionals should decide...

What do we mean by “risk”?

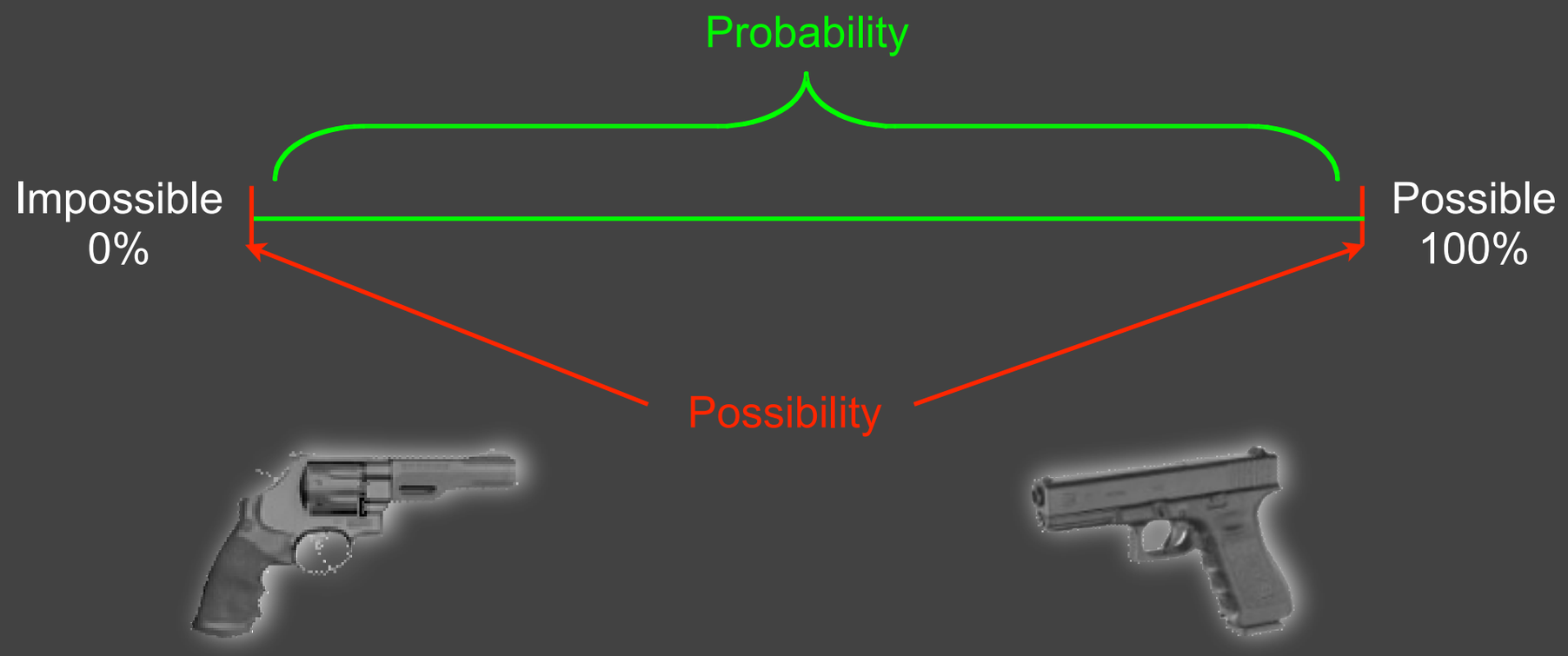
Risk...

The probable frequency and probable magnitude of future loss

In other words...

How often bad things are likely to happen,
and how bad they’re likely to be when they do happen

Probability vs. Possibility

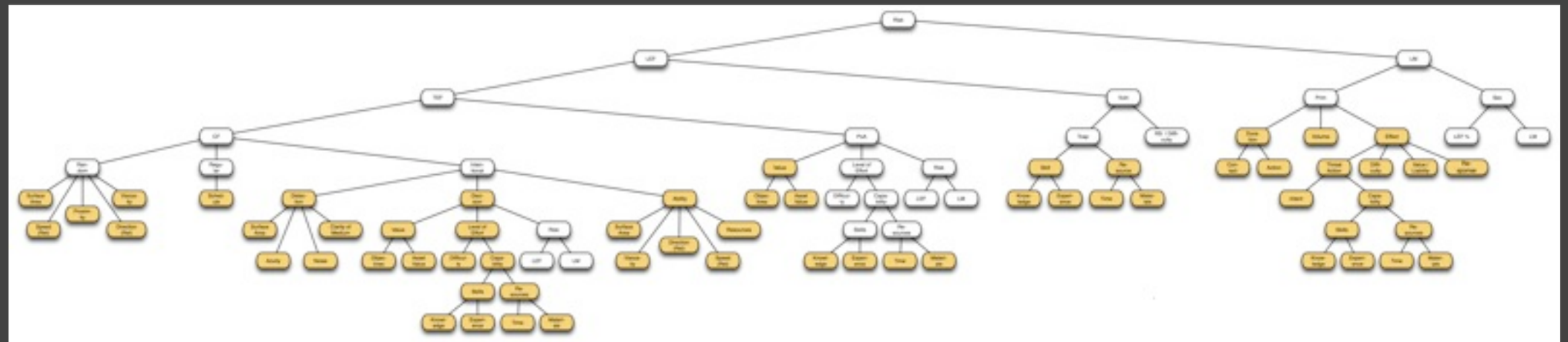


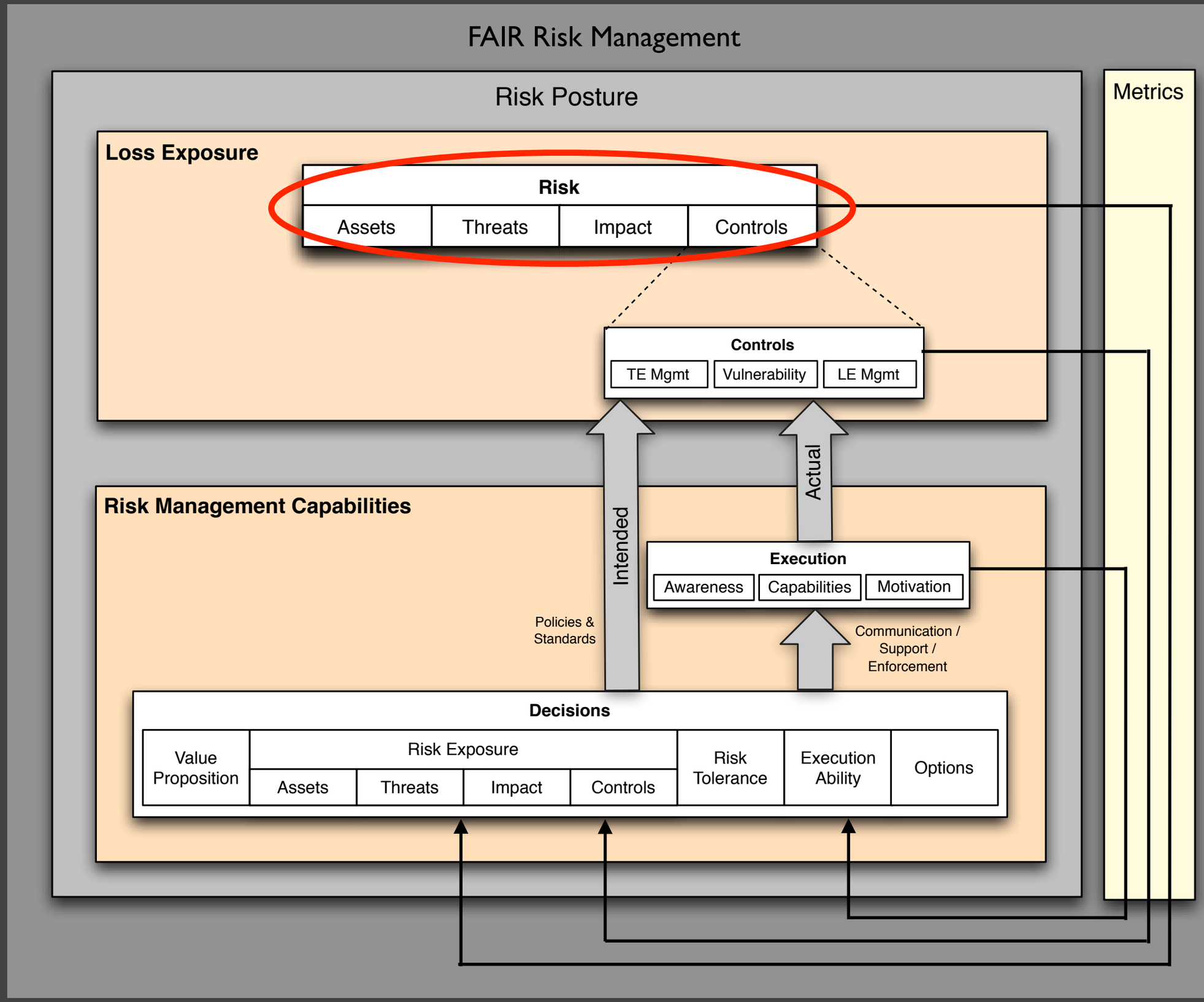
~17%

~100%

Risk Ontology...

A complex adaptive system





The dirty word...

The dirty word of measurement: **SUBJECTIVITY**

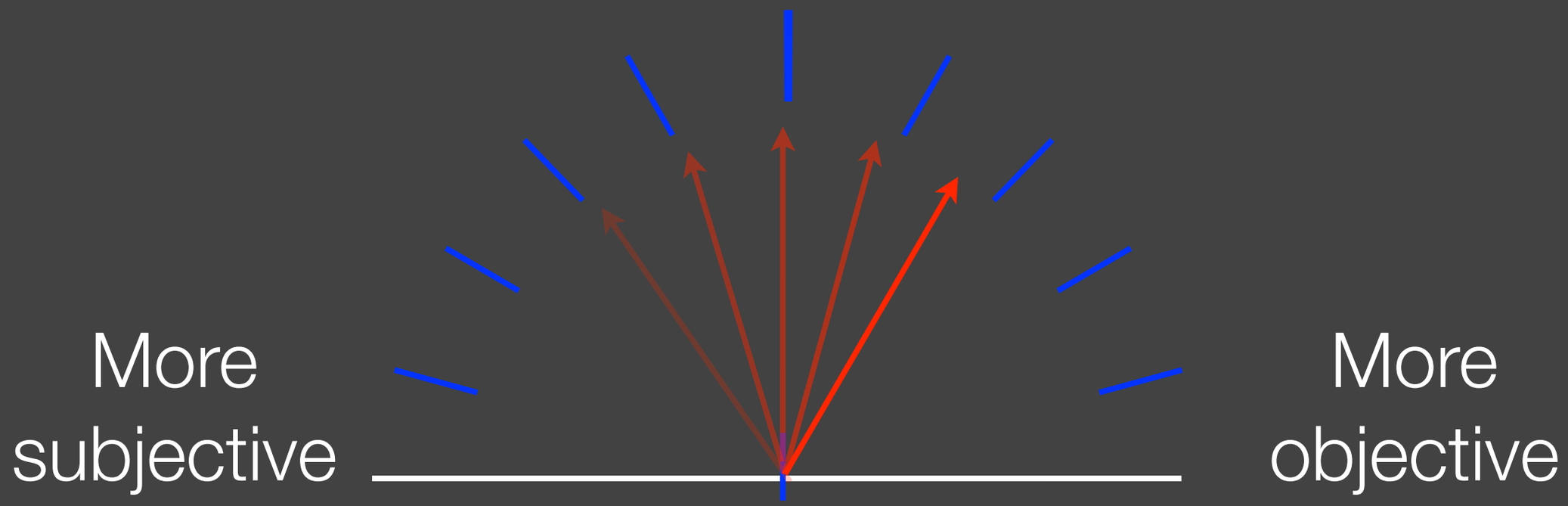
The dirty word...

- How tall am I?
  - Is that a subjective or objective measurement?

Subjectivity and Objectivity

They’re not binary. It’s a spectrum!

Increase objectivity



The dirty word...

Calling something a "subjective measurement" is just another way of saying it's a measurement with a higher degree of uncertainty and/or less precision.

All measurements have some degree of uncertainty and imprecision.

Practical example

- If you're approaching a traffic light and it turns yellow, do you step on the brake or the gas?
  - What kind of information (objective or subjective) is that based on?

The dirty word...

Myth: "Subjective" measurements are invalid

But tested!

My crystal ball is fuzzy…

My crystal ball is fuzzy...

"Prediction is very difficult,
especially about the future."

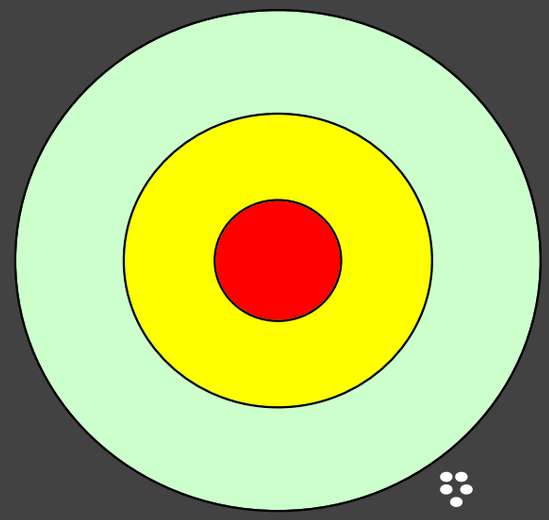
(Niels Bohr, Nuclear Physicist and Nobel Laureate)

My crystal ball is fuzzy...

Risk analysis is NOT about predicting the future.
It's about understanding the probabilities.

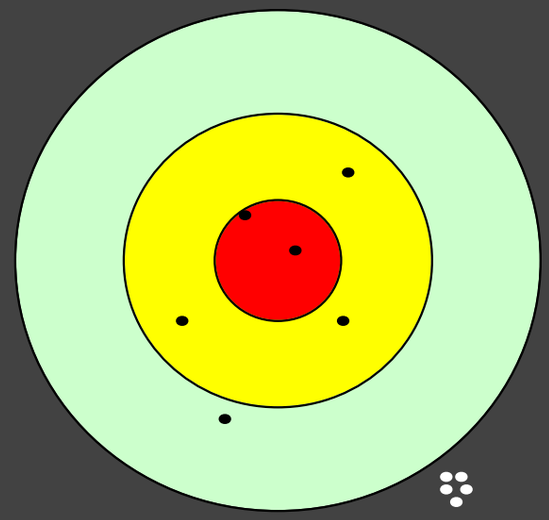
My crystal ball is fuzzy...

Precision



My crystal ball is fuzzy...

Accuracy



My crystal ball is fuzzy...

Management invariably prefers (and expects) accuracy rather than precision

My crystal ball is fuzzy...

Myth: Risk analyses are supposed to be precise

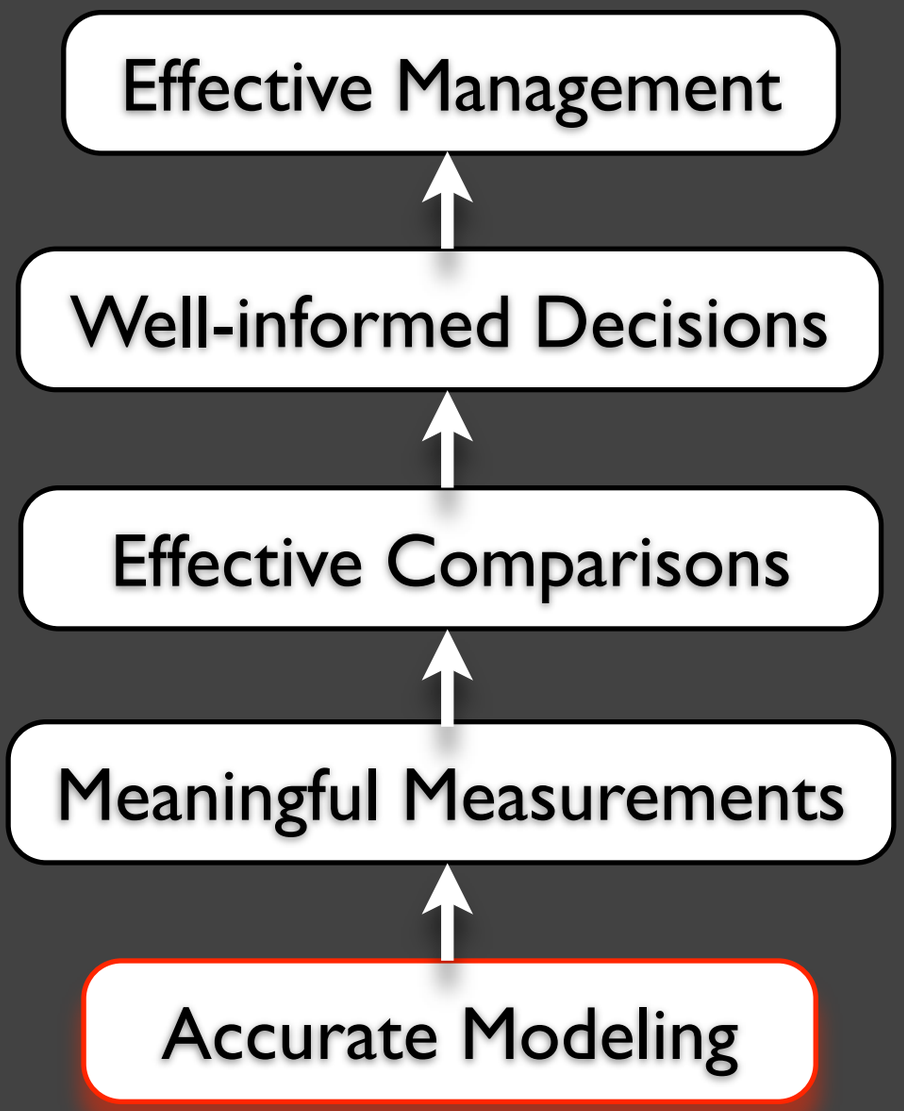
But busted!

Data? What data?

Data? What data?

- But we don't have enough good data to support quantitative analyses!! Do we?
  - Actually, much of the data is there to be had if we know where to look for it
  - Also, we don't need much data in order to make well-reasoned quantitative estimates

The missing ingredient



Example…

- Engaged a “Big Four” firm to conduct an attack and penetration exercise
  - Among their findings, several issues were rated “high risk”
  - After conducting a risk analysis, they conceded that none of those issues actually represented high risk

Example…

- Risk issue needed to be addressed
  - Evaluated three mitigation approaches
    - "Best practice"
    - And two atypical options
  - After analysis, option "B" (not "best practice") was expected to be as effective as the best practice solution, but at ~$250,000 less per year
  - Guess which one management chose…

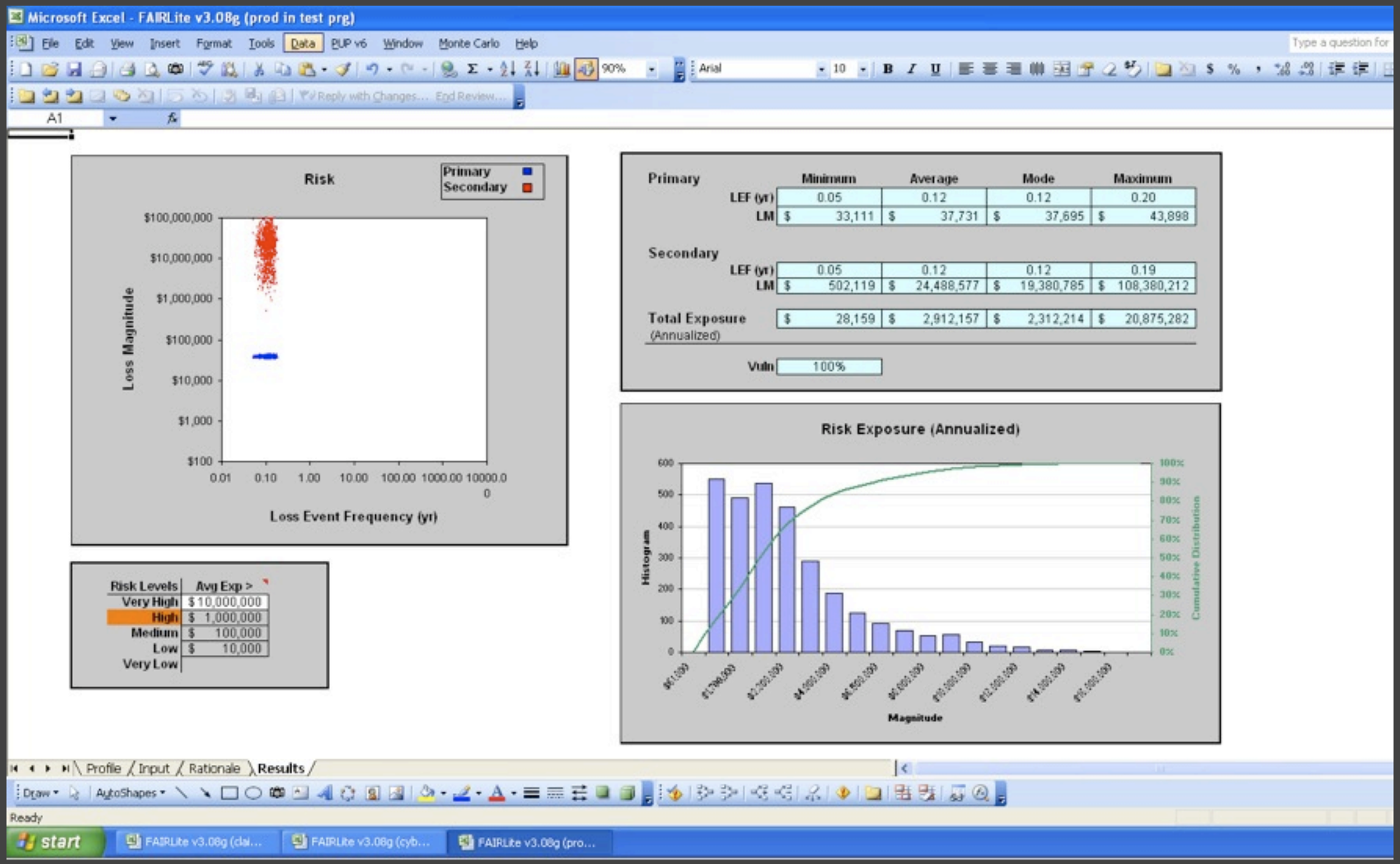
Data? What data?

- What do we mean by “good”?
  - Meaningful
  - Accurate
  - A useful degree of precision
  - Enable better-informed decisions

Data? What data?

- *How to Measure Anything*, by Douglas Hubbard
  - Talks about good data vs. bad data
  - Gives great examples
  - Provides an outstanding description of how to effectively and legitimately use subject matter expert estimates

Data? What data?



Data? What data?

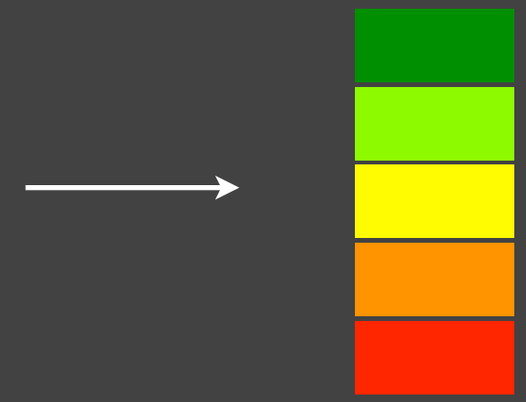
Myth: We don't have enough data to perform good quantitative analyses

Busted!

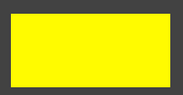
There's "quantitative" and then there's quantitative

There's "quantitative" and then there's quantitative

Qualitative Scale
(Ordinal)



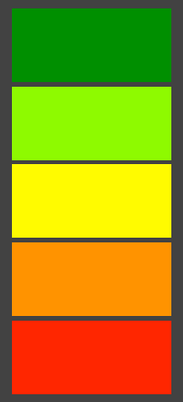
What does  x  equal?

What does  +  equal?

Ordinal scales…

What's the difference?

Scale



=

Scale

- Very Low
- Low
- Moderate
- High
- Very High

=

Scale

- 1
- 2
- 3
- 4
- 5

There's quantitative and then there's "quantitative"

Myth: Numeric ordinal scales enable quantitative measurement

Busted!

“Infosec professionals should decide...”

Infosec professionals should decide how much risk is acceptable

- Two commonly expressed concerns:
  - Do executives “get” security?
  - Will executives accept almost any amount of risk?

Do executives “get” security?

No, many of them don’t...

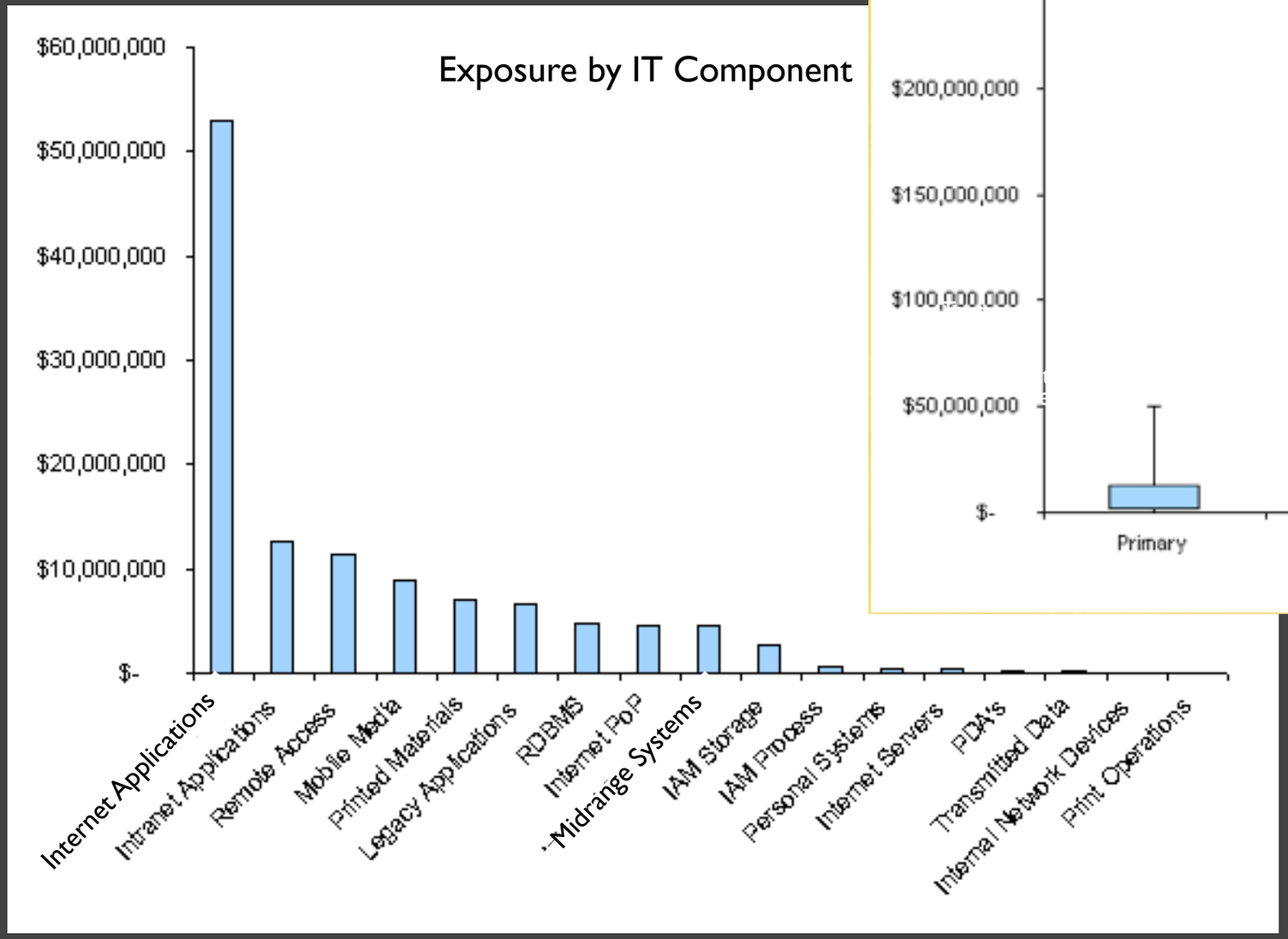
...but they shouldn’t have to.

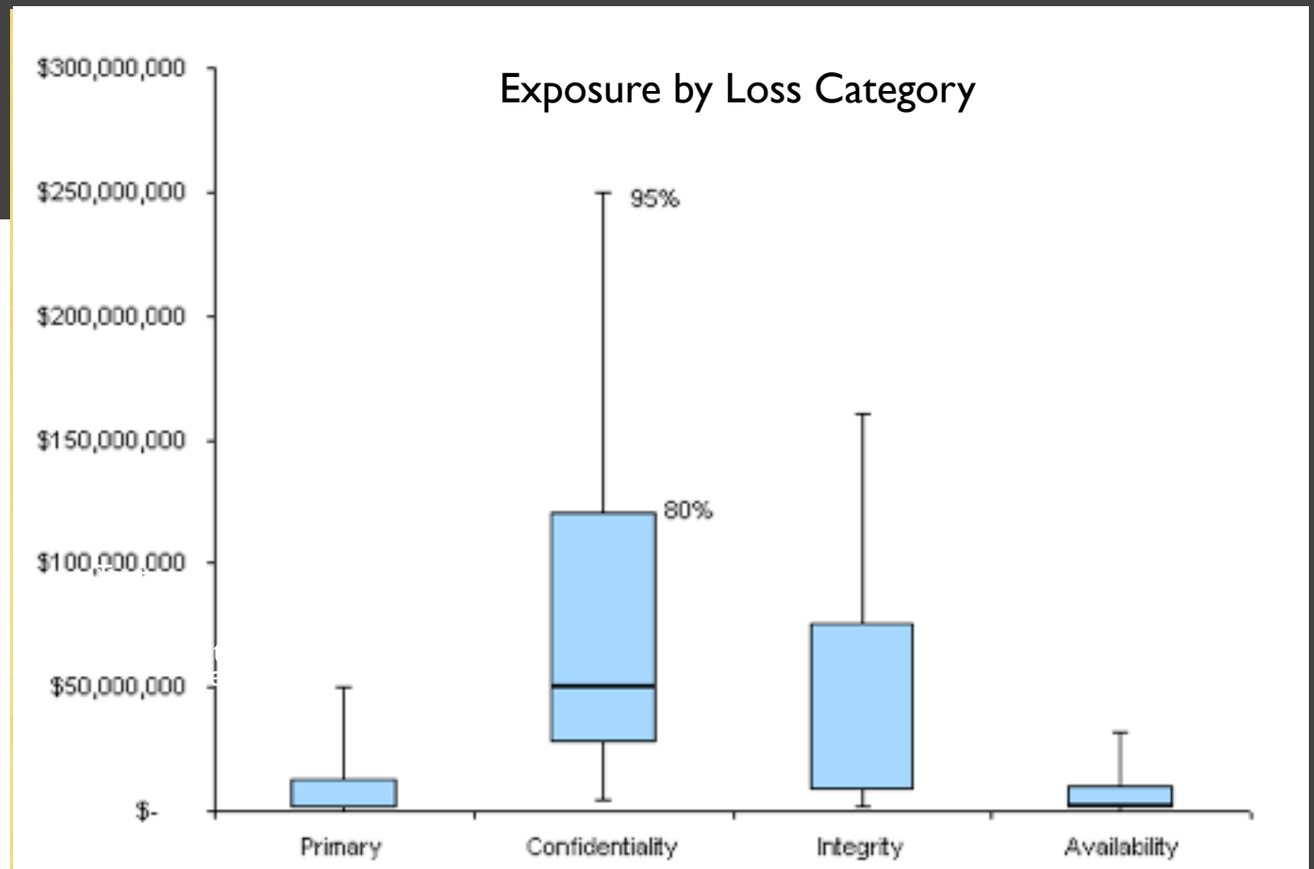
What they understand is risk. So if we want their attention and support, we need to speak in terms that are meaningful to them

Will executives accept almost any amount of risk?

- No. They're intelligent and rational. And it's THEIR JOB to balance the organization's resources against:
  - All of the opportunities they have to chase
  - All of the operational requirements that exist
  - All of the different forms of risk they're faced with, of which security is just one
  - In order for them to make well-informed decisions they must have information that is meaningful and useful

Ability to Focus





Infosec professionals should decide how much risk is acceptable

Myth: Infosec professionals should decide how much risk is acceptable

Busted!

Summary

- Management cares about risk, not security
- There are many misconceptions and myths regarding risk
- If we want to be relevant, we HAVE to understand and be able to deal effectively with risk

Questions?