

Risk - You can't manage what you can't measure

Jack Jones, CISSP, CISM, CISA

68775-3

What we'll cover...

- Why quantify?
- Why is it so hard?
- There's quantitative and then there's "quantitative"
- Common concerns
- Steps to practical application
- Q&A

Why quantify?

To answer the key questions...

- How much risk do we have?
- If I spend this money, how much less risk will I have?
- What benefit am I getting from the money I'm already spending?
- Which are my most cost-effective options?

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...

Why is it so **hard**?

You can't manage what you can't measure...
...and you can't measure what you haven't defined

Asset, Threat, Vulnerability, or Risk?

- A weak password
- A disgruntled employee
- A poorly trained employee
- An unencrypted backup tape
- An unpatched Internet-facing server
- A database full of sensitive information

Risk Scenarios - Things that can go wrong

- Smoke detector battery fails
- Failure to change smoke detector batteries
- House catches on fire

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

Getting Risk Right

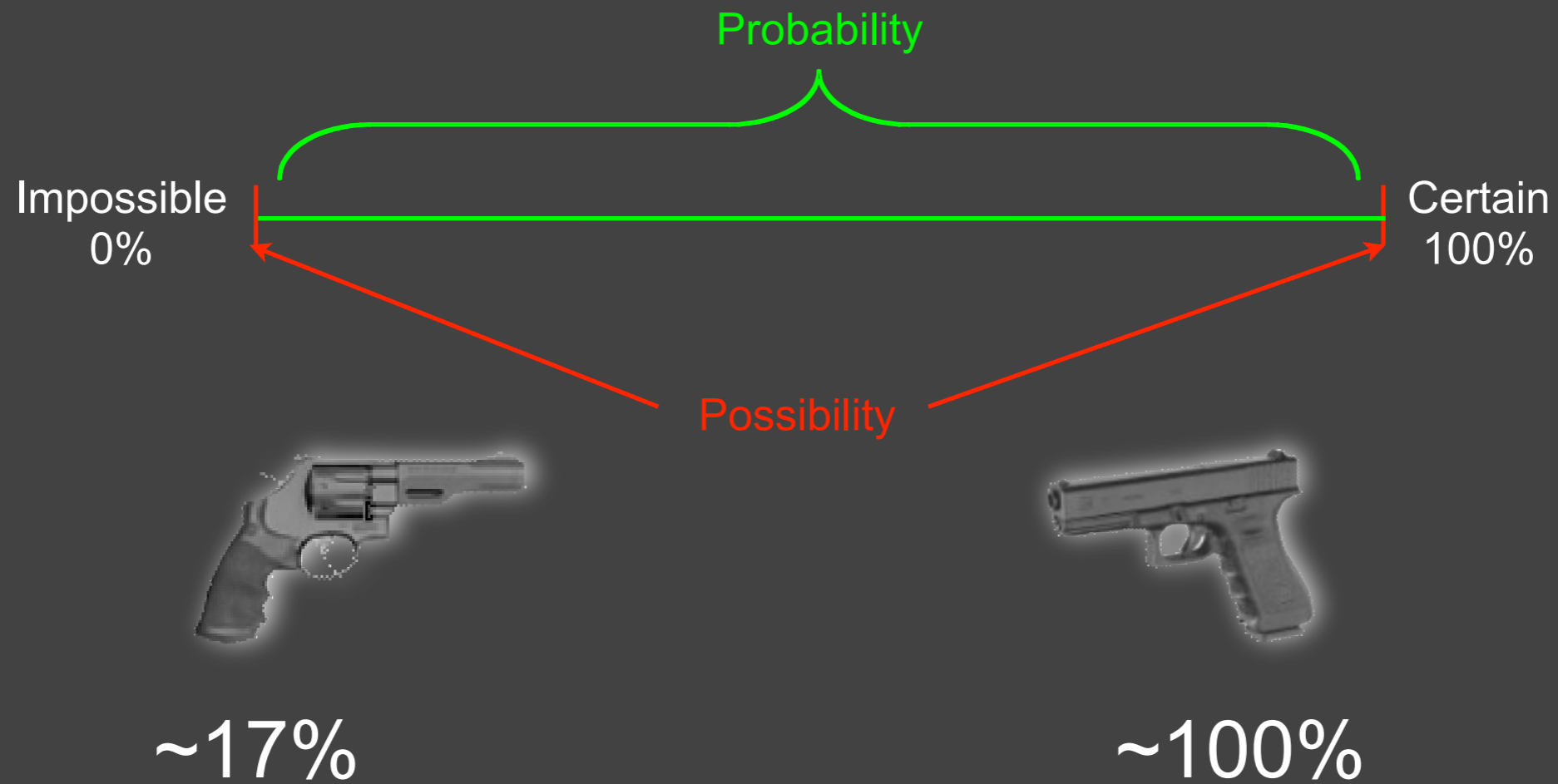
Risk...

The probable frequency and probable magnitude of future loss

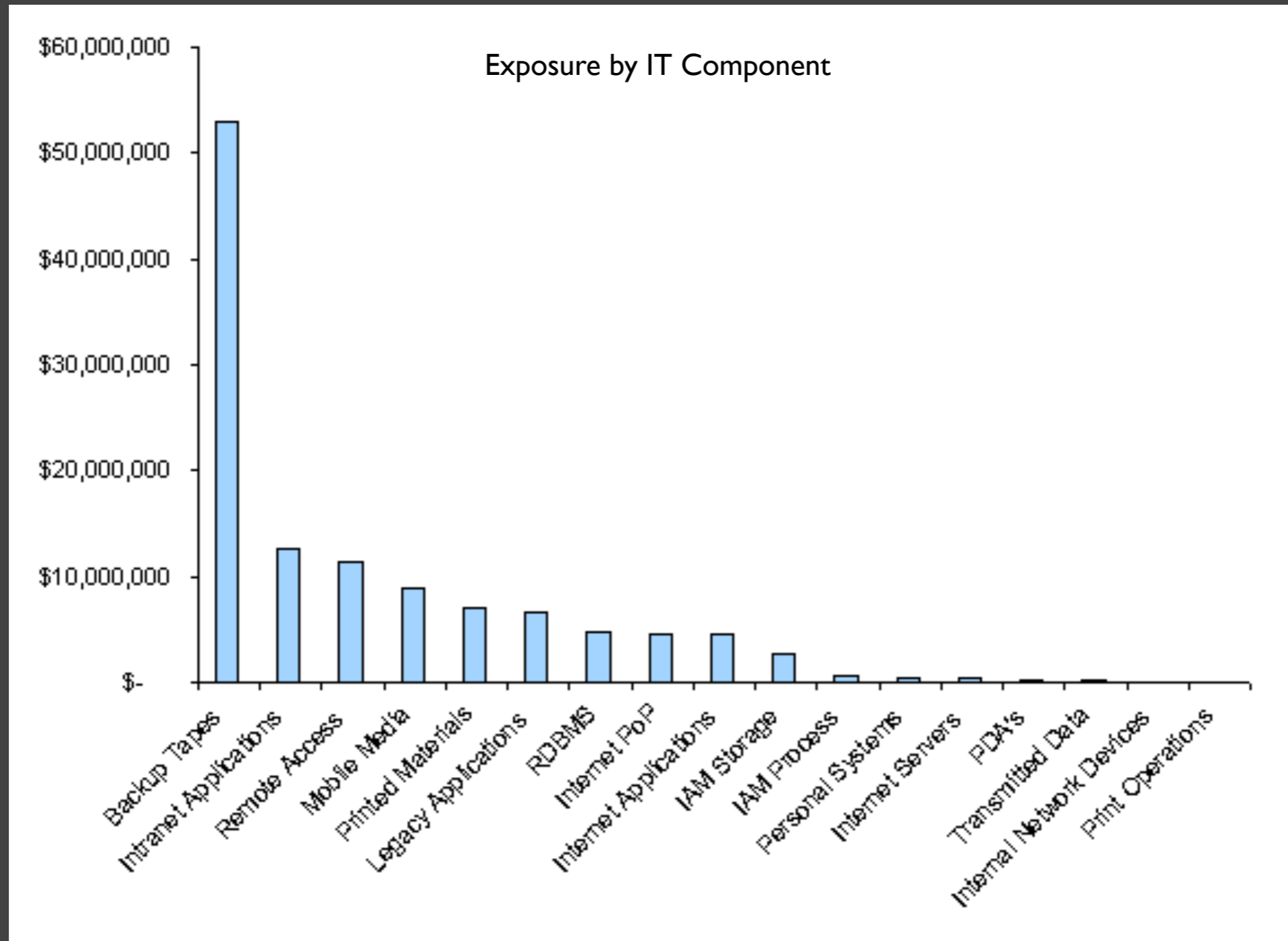
In other words...

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

Probability vs. Possibility



Ability to Focus



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?



Steps to Legitimate Quantification

- Use “real” numbers
 - ▶ Frequencies, probabilities, monetary values
- Aim for accuracy vs. precision
 - ▶ You can be precisely wrong...
- Account for uncertainty
 - ▶ Express estimates using distributions
 - ▶ Leverage monte carlo analysis
- Avoid garbage in, garbage out -- Calibrate
 - ▶ Most people are bad at estimation
 - ▶ People can be trained to estimate well

Common Concerns

- Prediction
- Subjectivity vs. objectivity
- Accuracy vs. precision
- Practicality

Prediction

“Prediction is very difficult,
especially about the future.”

(Niels Bohr, Nuclear Physicist and Nobel Laureate)



The dirty word of measurement: **SUBJECTIVITY**

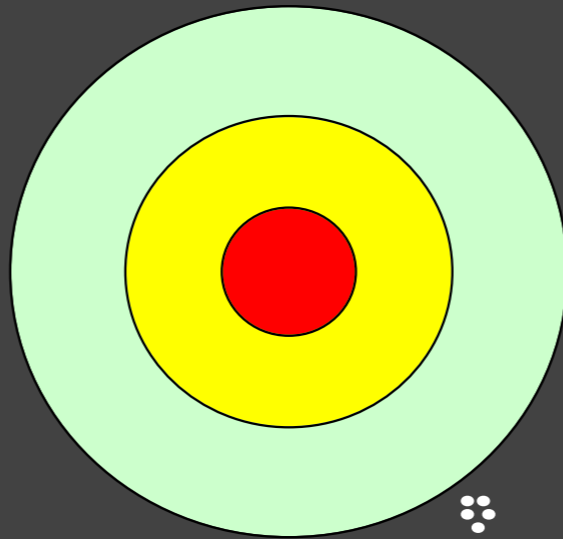


Subjectivity and Objectivity

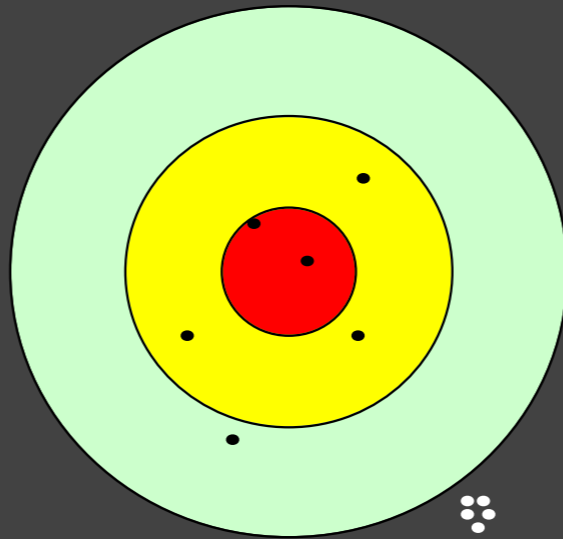
They're not binary. It's a spectrum!

- How tall am I?
 - ▶ Is that subjective or objective?
- What's your favorite flavor of ice cream?
 - ▶ Is that subjective or objective?
- If you're approaching a stoplight that's turning yellow, should you slow down or speed up?
 - ▶ Is that subjective or objective?

Precision



Accuracy



Management invariably prefers (and expects)
accuracy rather than precision

Steps to Practical Application

- Define or adopt a framework that makes sense
- Educate, educate, educate
 - ▶ This represents a paradigm shift for many professionals
- Get stakeholders on-board
 - ▶ Apply risk analysis where it matters
 - ▶ Show value

Steps to Practical Application

- Start simple - for example
 - ▶ “How much risk does this policy exception represent?”
 - ▶ “Which of these audit findings truly represents high risk?”
- Perform peer reviews
 - ▶ Requires people to explain their analyses
- Leverage external expertise
 - ▶ Selective use, where it matters most

Good Risk Resources

- Factor Analysis of Information Risk (FAIR)
 - ▶ <http://riskmanagementinsight.com>
- ISACA RiskIT Framework
 - ▶ <http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx>
- The Open Group
 - ▶ <http://www.opengroup.org/bookstore/catalog/c081.htm>
- How to Measure Anything
 - ▶ <http://www.howtomeasureanything.com/>

Questions?