Risk Management Maturity Benchmark Review

WEBINAR - DECEMBER 5TH, 2017

Presenters

- Jack Jones - Chairman, FAIR Institute, and EVP R&D RiskLens

- Steve Schlarman - Director, Product Marketing and GRC Strategist, RSA

Agenda

- Does the world really need yet ANOTHER cyber risk maturity model?
- Benchmark survey results
- Overcoming challenges
- Next year's report…

Why this maturity model?

OR, DOES THE WORLD REALLY NEED YET ANOTHER MATURITY MODEL?

What does a “mature” organization look like?

- The existence of well-documented policies and procedures?
- Essential/fundamental security technologies deployed?
- Active education and awareness program?
- Personnel roles and responsibilities clearly-defined?
- Board of directors engaged and getting regular reports?
- Uses a risk register to track “risks”?
- Risk appetite defined?
- Metrics program in place?

Yes, but…

What's the purpose of a RM program?

To enable an organization to manage risk?

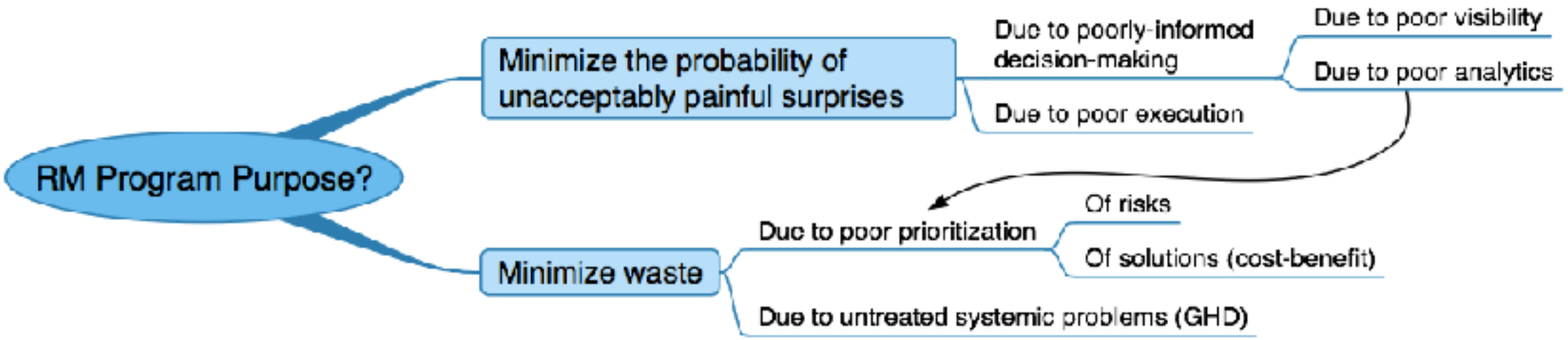
What's the purpose of a RM program?

Enable an organization to cost-effectively achieve and maintain an acceptable level of risk.

In a business and risk landscape that is complex and constantly evolving, and where resources are limited.

What's the purpose of a RM program?

Said another way…



In a business and risk landscape that is complex and constantly evolving, and where resources are limited.

Model premise

- Two dimensions to maturity:
  - The ability to make well-informed decisions
  - The ability to execute reliably
- Each of these is decomposed into the factors that drive them, which results in a Bayesian network

Do these drive, or result from, maturity?

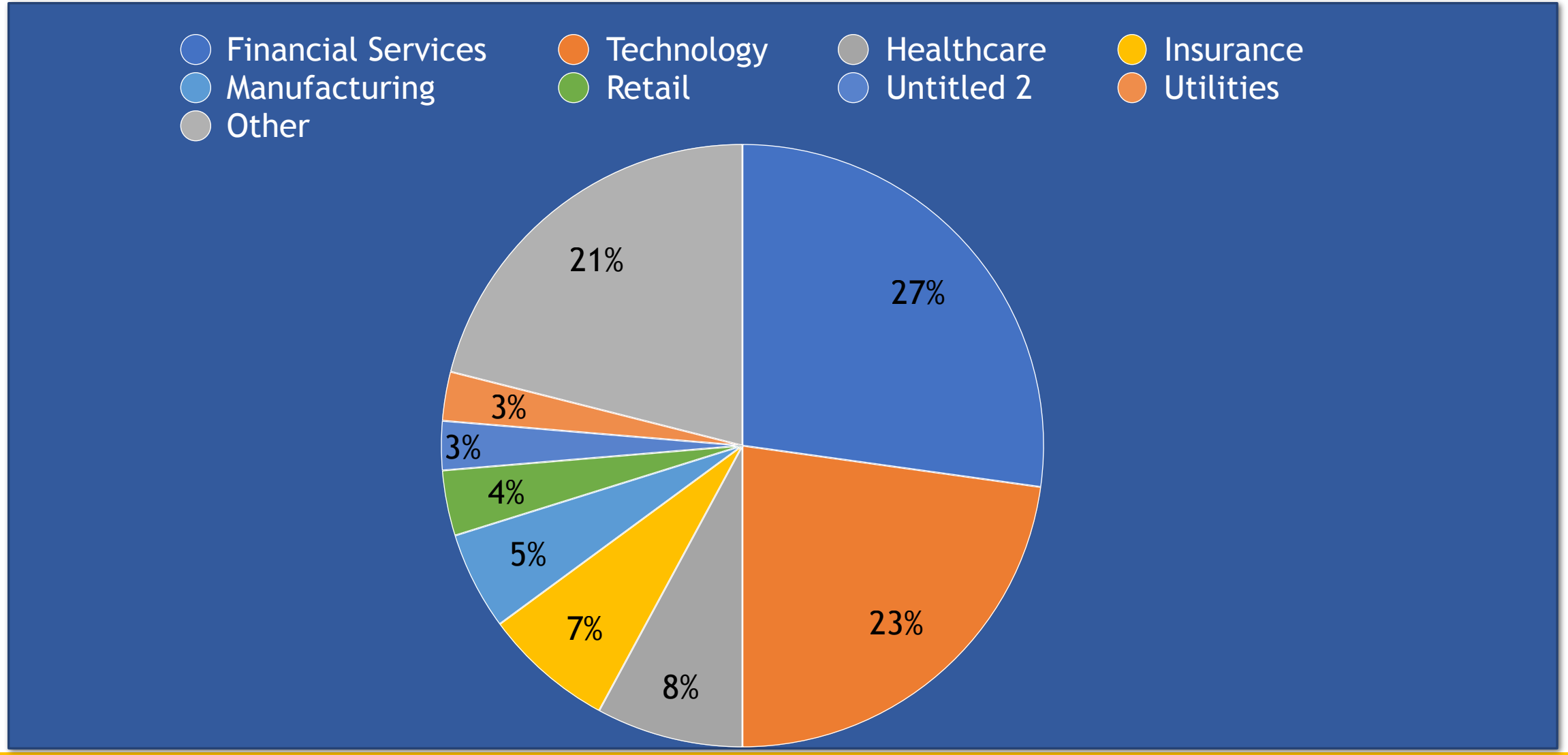
- The existence of well-documented policies and procedures?
- Essential/fundamental security technologies deployed?
- Active education and awareness program?
- Personnel roles and responsibilities clearly-defined?
- Board of directors engaged and getting regular reports?
- Uses a risk register to track “risks”?
- Risk appetite defined?
- Metrics program in place?

What’s the difference?

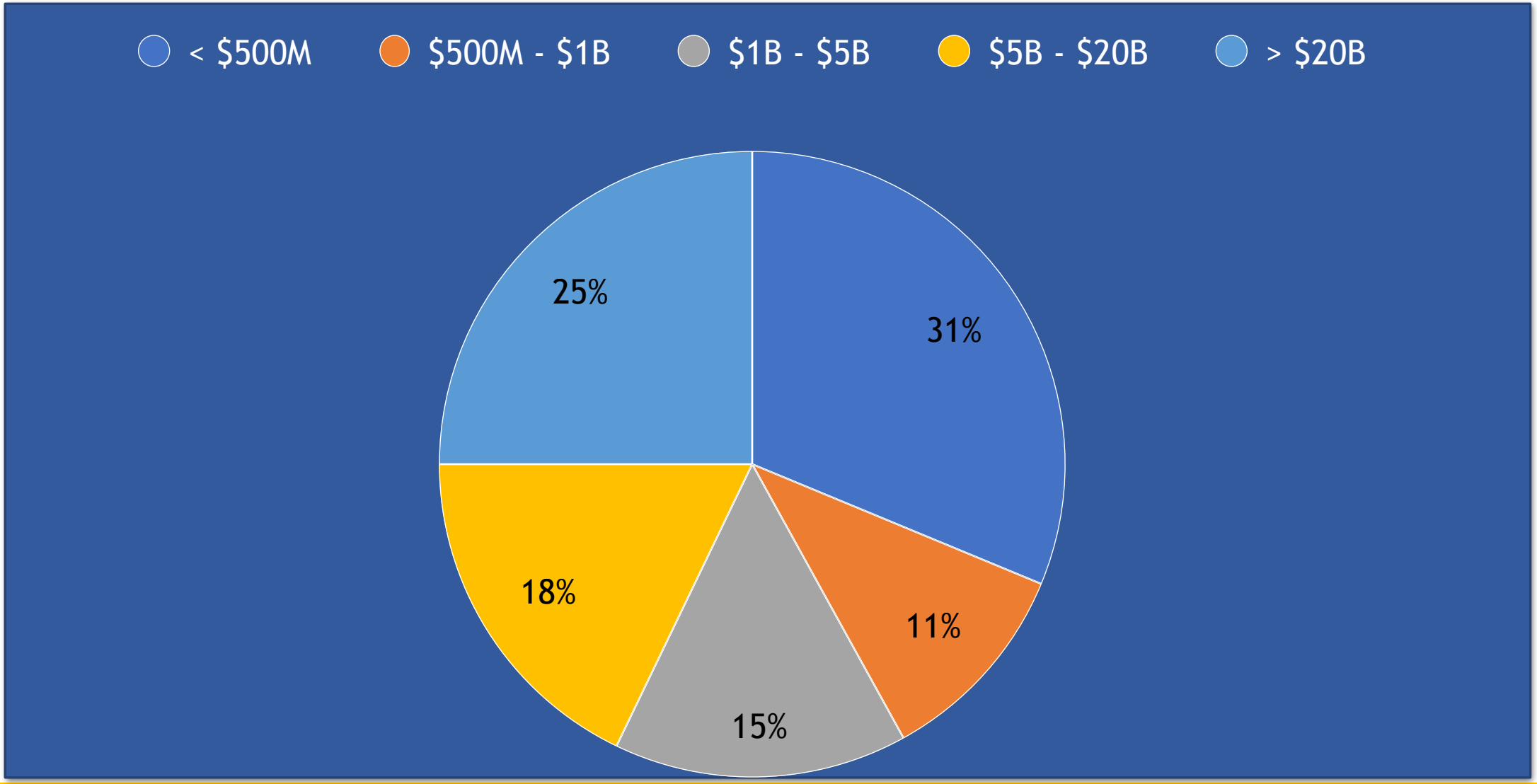
Respondent Data

114 Respondents

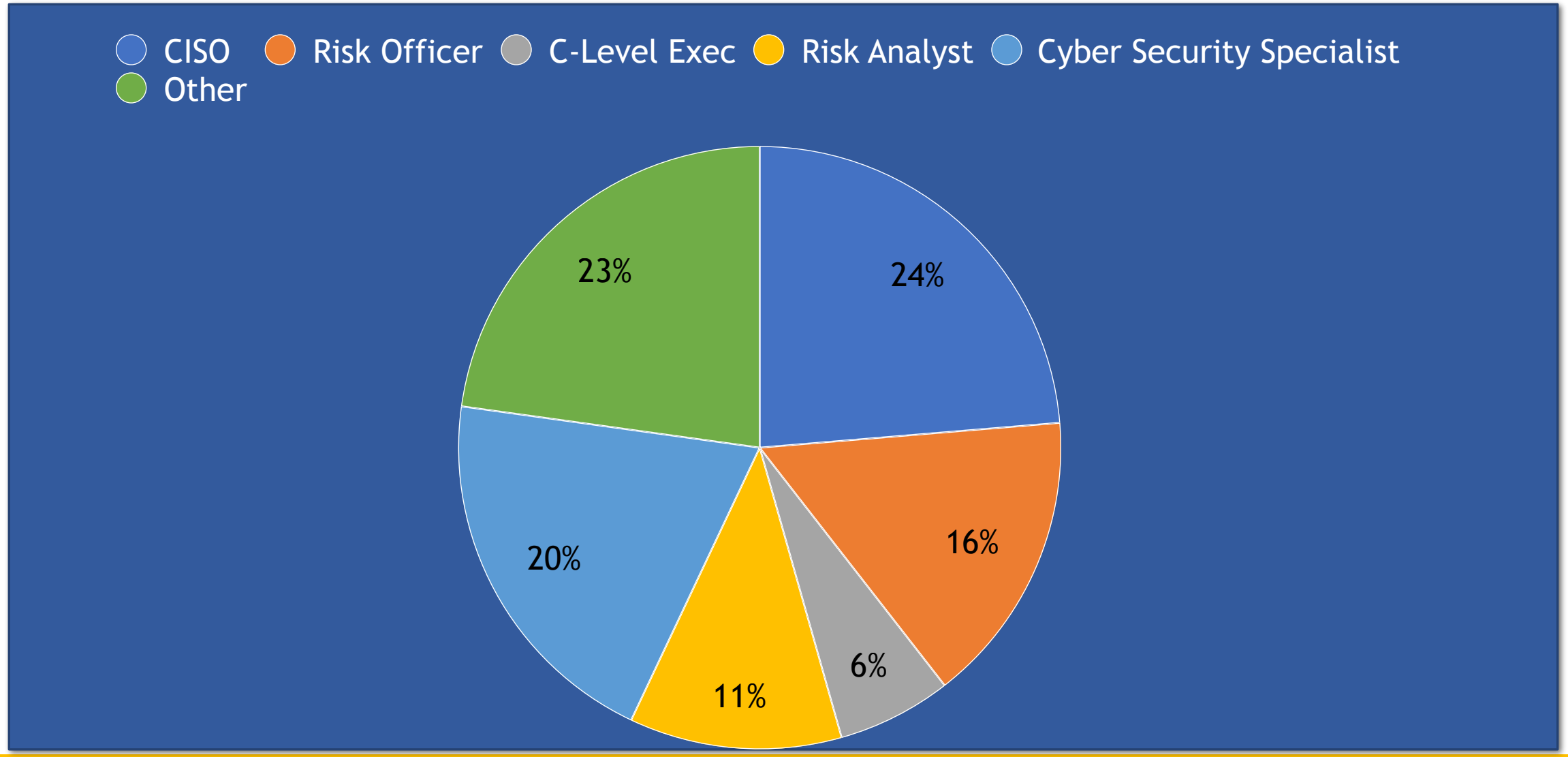
Industries


Financial Services
Technology
Healthcare
Insurance
Manufacturing
Retail
Untitled 2
Utilities
Other
27%
23%
8%
7%
5%
4%
3%
3%
21%

Organization size



Respondent roles



Inputs…

- 14 questions inform the model
- Three choices per question (“Weak”, “Partial”, “Strong”)
  - Why 3 versus 5?
  - What represents “strong”, etc.?

Caveats & considerations

- Sample bias
- Self-assessed
  - Bias?
  - Respondent visibility into their organization's program?
- Interpretation of questions and choices
- Limited granularity
- Bayesian probabilities should be considered "priors"
- Measurement uncertainty not fully represented

Survey Results

Interesting findings

- Highest score was from a $500M - $1B healthcare organization
- Top 4 scores came from 4 different industries (healthcare, insurance, banking, consultancy)

Summary data

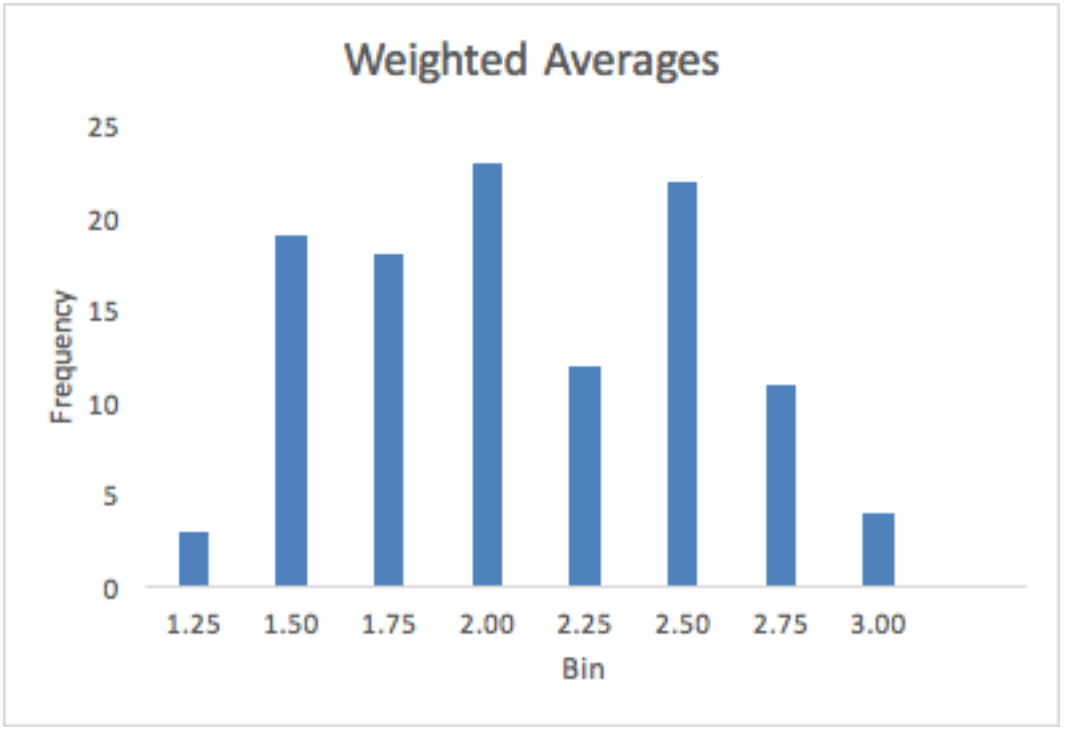
Two separate analysis approaches…

- Weighted averages
  - Assumes all variables are independent and of equal weight
- Bayesian
  - Captures variable relationships and dependencies
  - Probabilistic results
  - Index scoring for comparisons

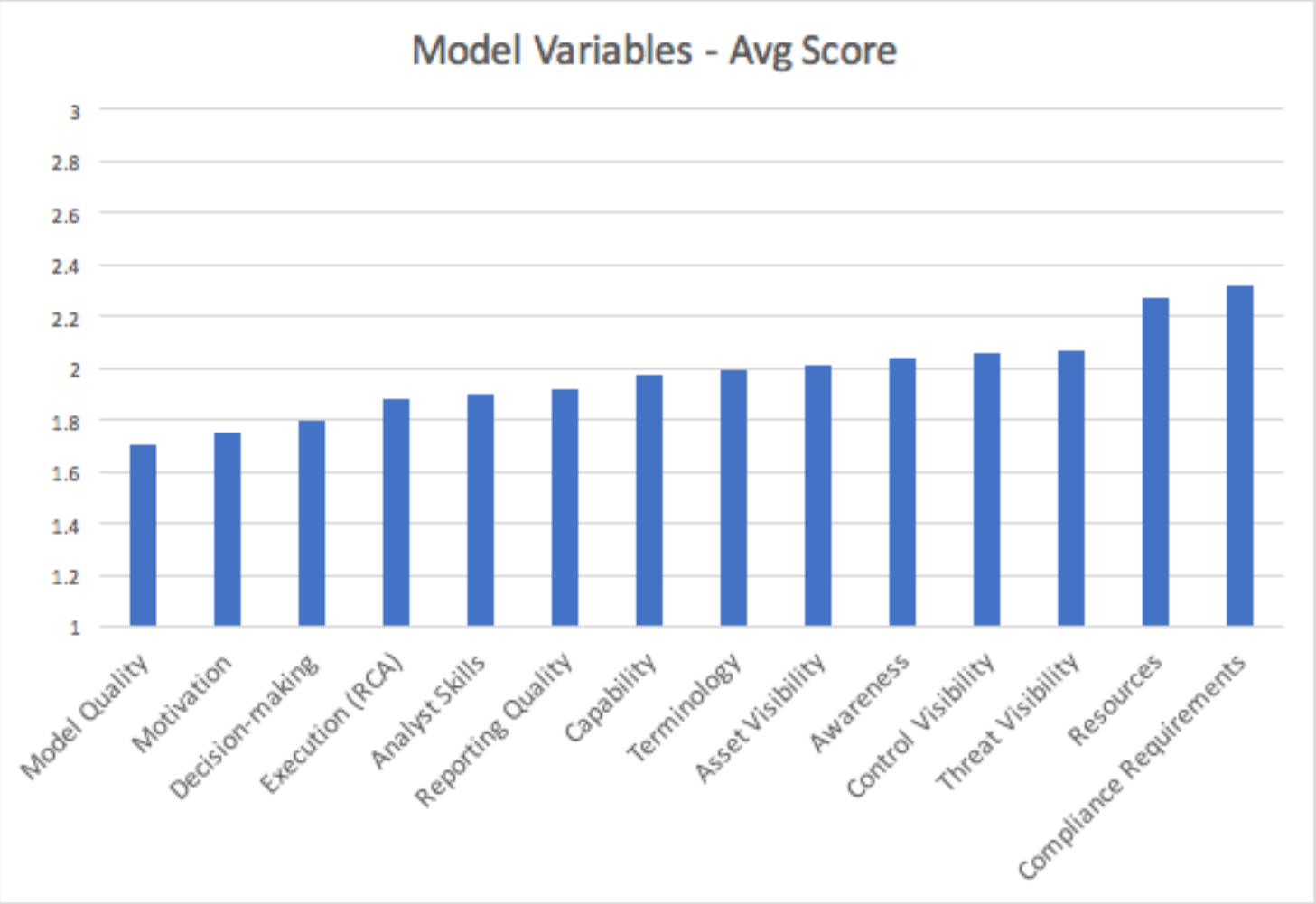
Weighted averages

- Minimum: 1.21
- Maximum: 2.93
- Average: 1.97
- Median: 1.96
- Mode: 1.86

- 75th percentile: 2.36
- 90th percentile: 2.57

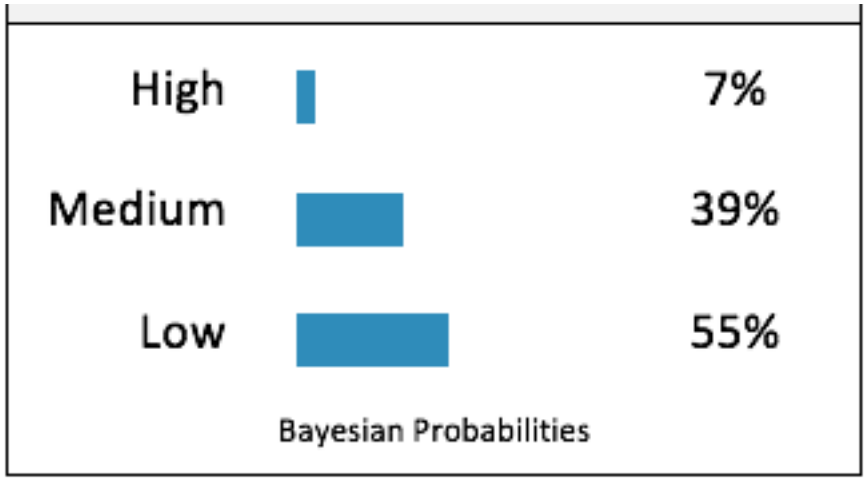


Ranking the variables…



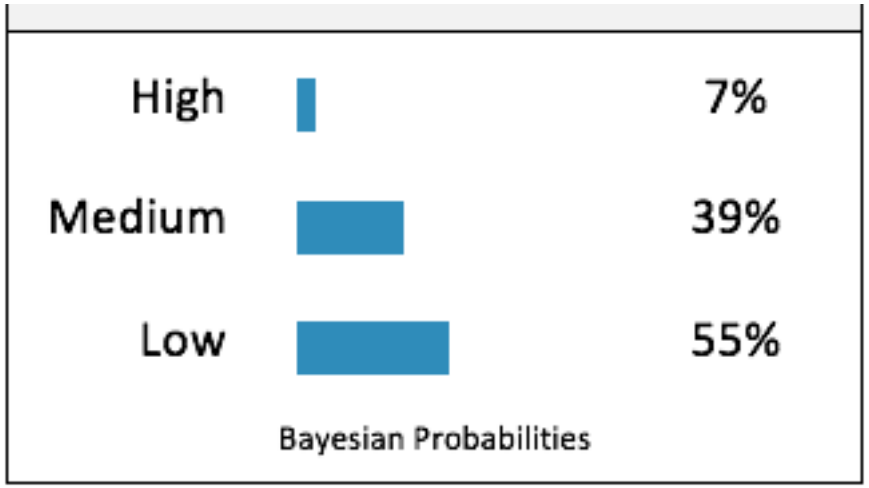
Bayesian analysis

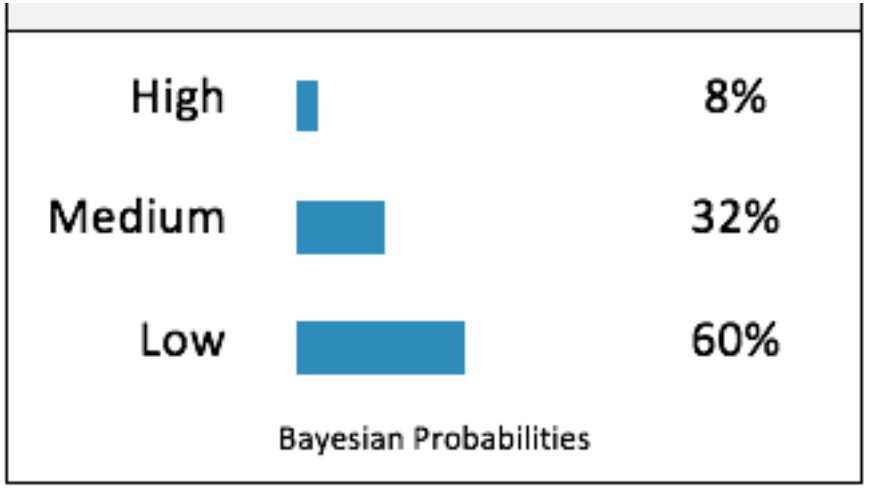
- Based on the respondent's answers, expresses the probability that an organization will perform at a "Highly Mature", "Moderately Mature" or "Low Maturity" level



Bayesian analysis comparisons…

- … are hard

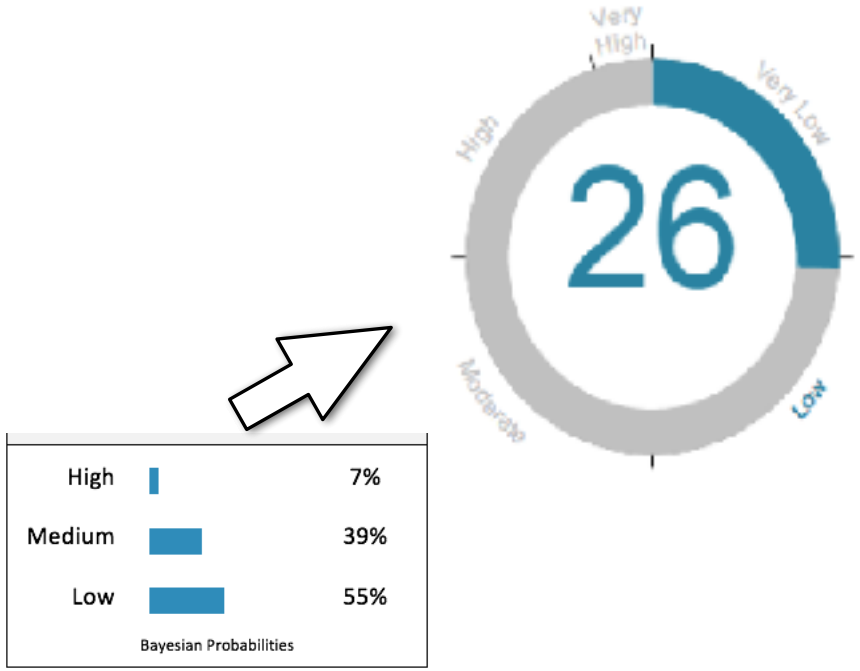


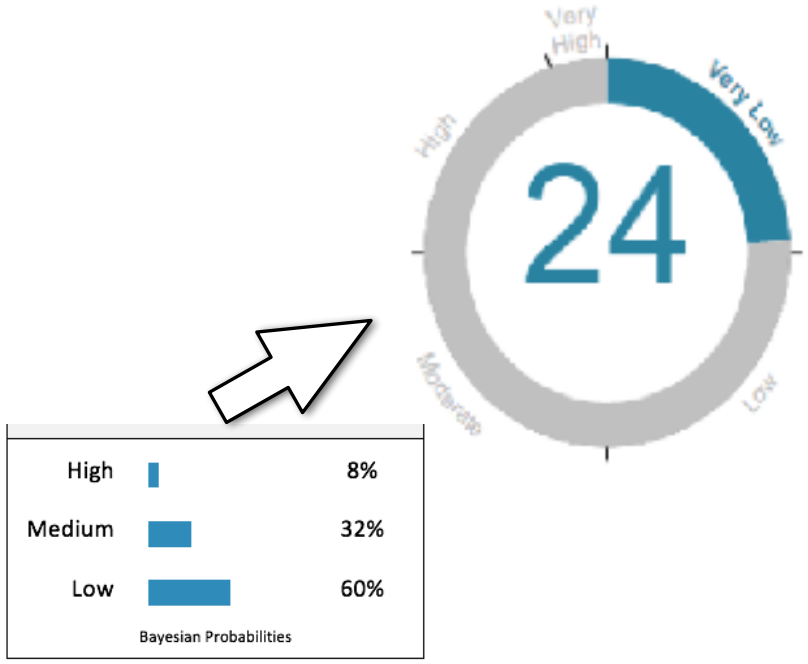


Which of these is better?

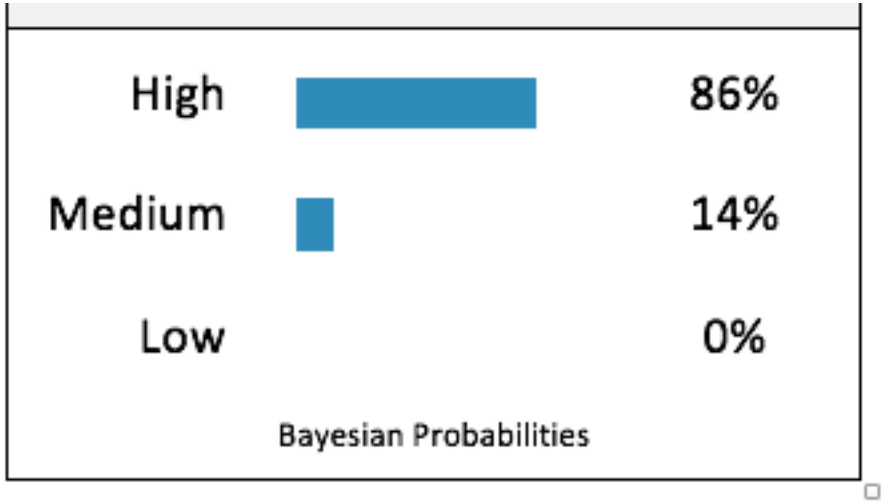
So we created an index…

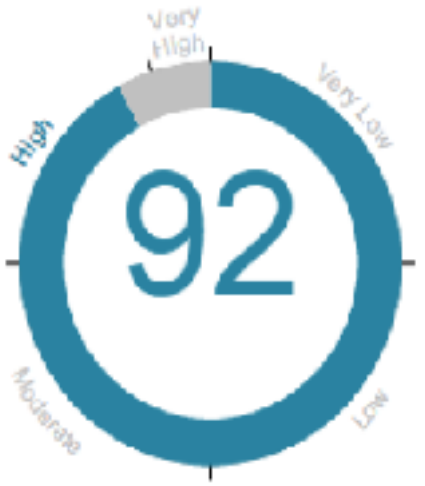
- 0 thru 100 scale



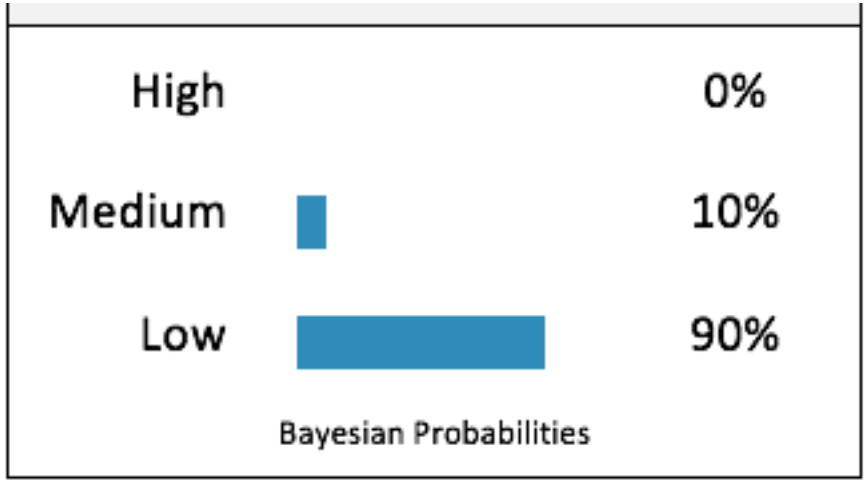


Highest score

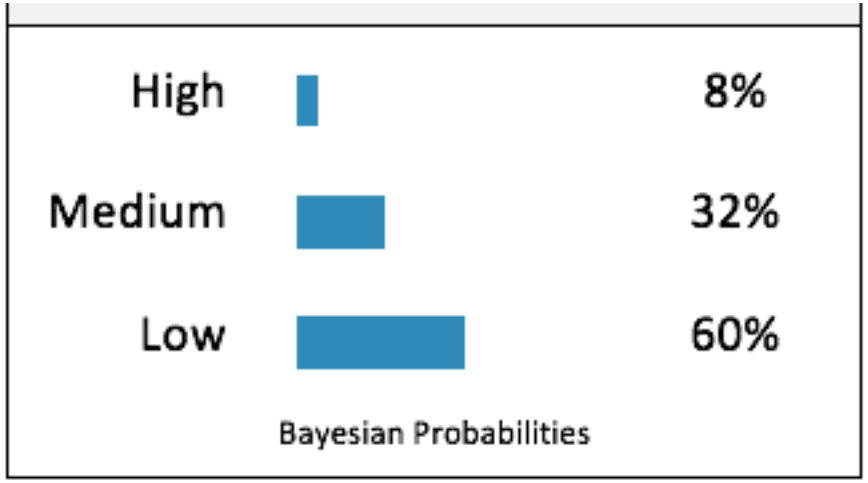




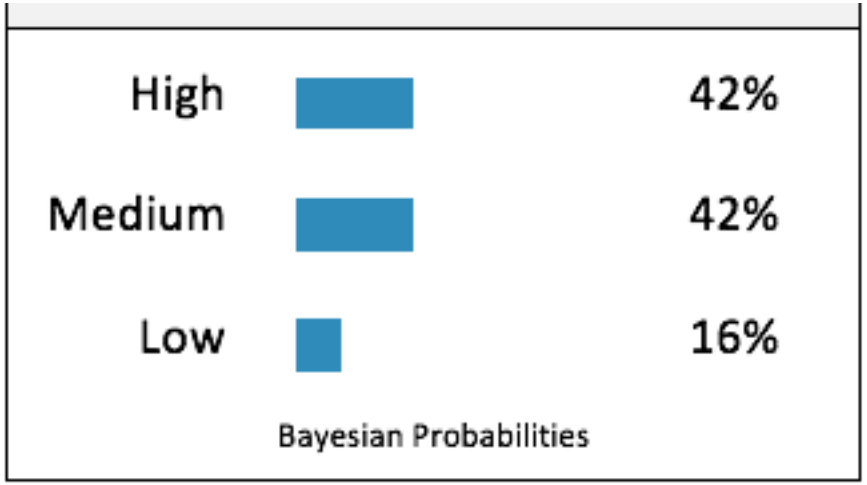
Lowest score

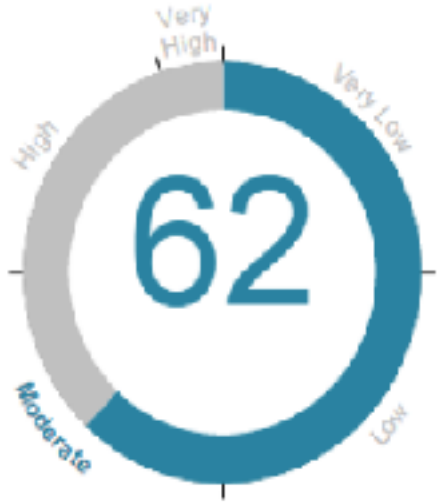


Average score

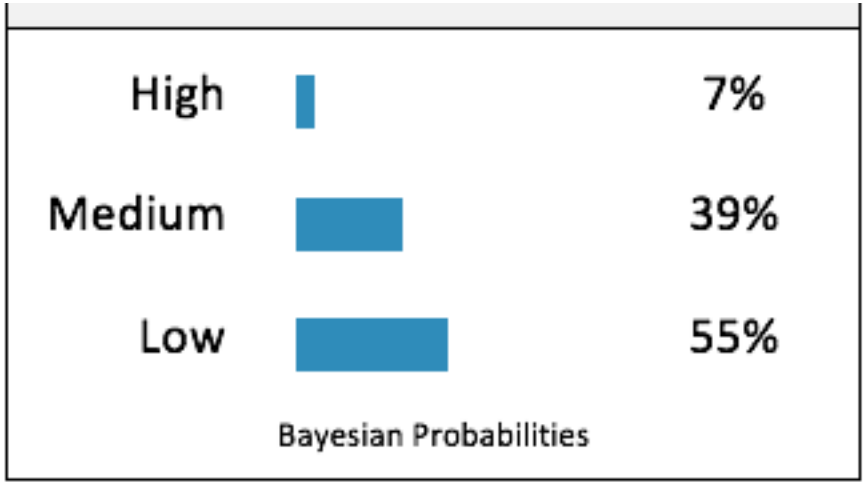


90th percentile





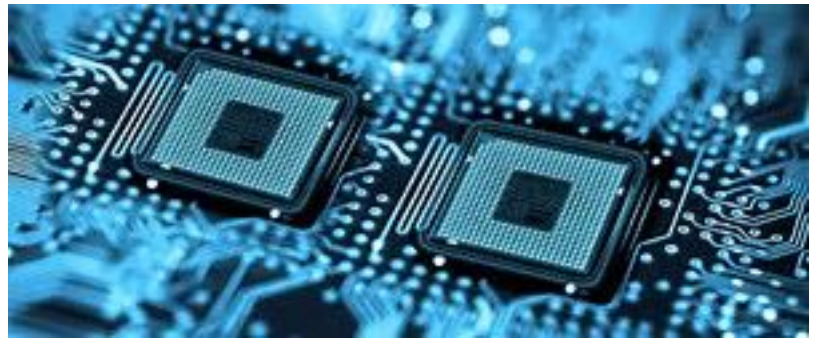
75th percentile



Implications

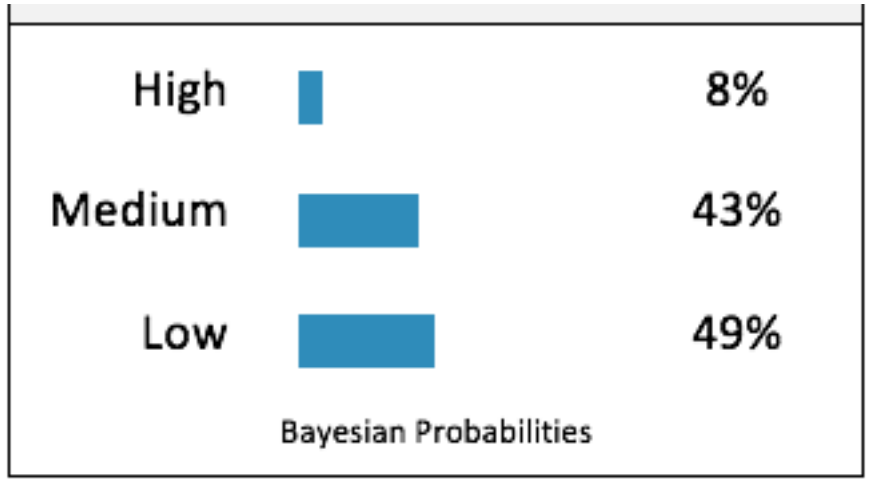
- Demonstrates difference between a weighted average (relative scoring) approach vs. Bayesian (context measurement) approach
- An organization at the 90th percentile (using wt. avg.) still isn't very mature (by our definition and using Bayesian analysis)

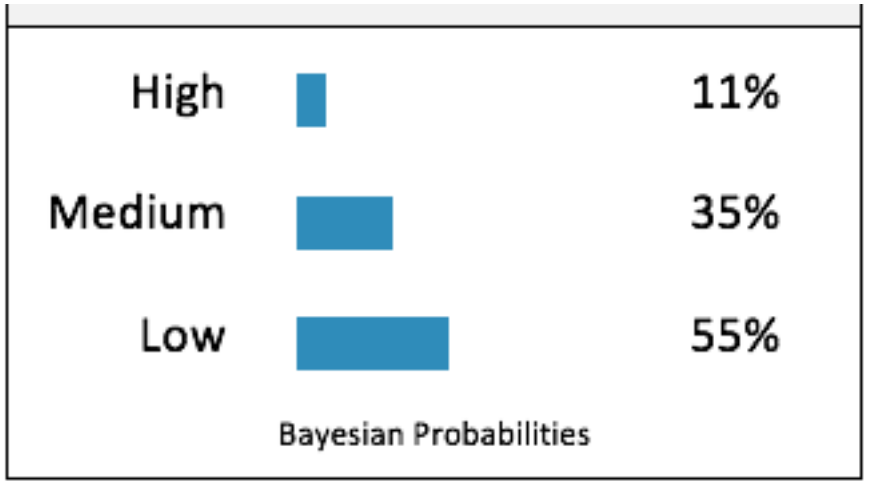
vs.



Industry comparison

Finance vs. Technology





Comparison by organization size

Resources

< $500M | $500M - $1B | $1B - $5B | $5B - $20B | > $20B

Threat visibility

< $500M | $500M - $1B | $1B - $5B | $5B - $20B | > $20B

Capability (training)

< $500M

$500M - $1B

$1B - $5B

$5B - $20B

> $20B

Overcoming challenges

Awareness

- Our profession needs to more broadly recognize the limitations of current compliance and checklist-based practices. We need to get the word out through:
  - Webinars
  - Conference presentations
  - Blog posts
  - White papers
  - Books

Expectations

- Regulations
- Big-4 adoption
- Boards of Directors
- The herd…

Credibility

- Research
- Success stories
- Broader adoption (?)

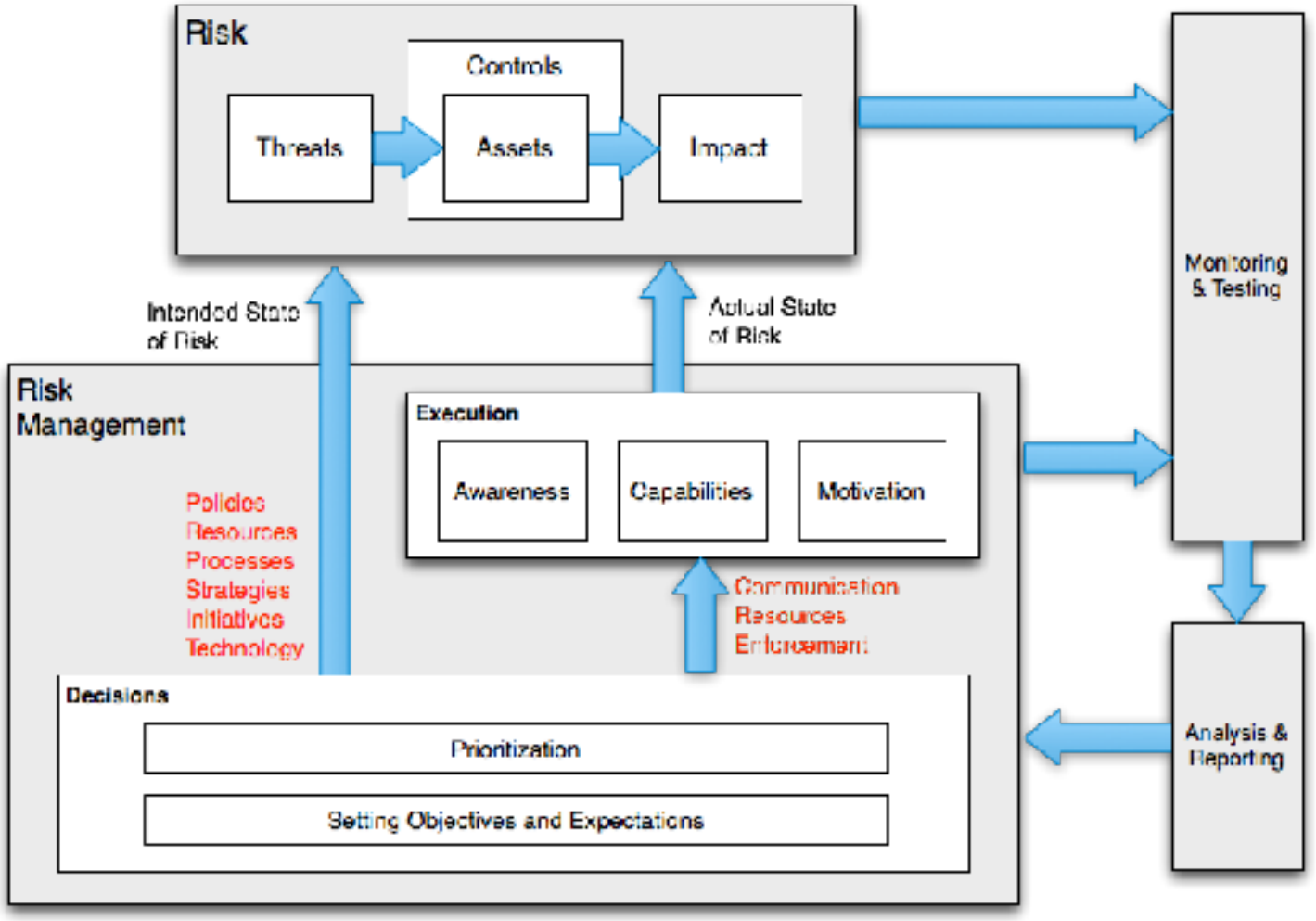
Training/resources

- Books
- Blogs (e.g., FAIR Institute)
- White papers (e.g., FAIR Institute)
- Local FAIR chapters
- Classes
  - Online (new FAIR course)
  - Onsite
  - University
    - Props to San Jose State University (Prof. Mike Jerbic)

Tools

- Have to make it accessible, but still captures the complex nature of the problem
  - As simple as possible, but no simpler
- Free
  - FAIR-U
  - Open Group
- Commercial
  - RiskLens
  - Others?

Summary


Risk
Controls
Threats
Assets
Impact
Intended State of Risk
Actual State of Risk
Risk Management
Execution
Awareness
Capabilities
Motivation
Policies
Resources
Processes
Strategies
Initiatives
Technology
Communication
Resources
Enforcement
Decisions
Prioritization
Setting Objectives and Expectations
Monitoring & Testing
Analysis & Reporting

Next year’s report

Next year

- Larger population of respondents
  - Earlier initiation
  - Stronger marketing
- Improve consistency
  - Improve verbiage (questions & choices)
  - Add a way to express confidence
  - Evolve the Bayesian network

Questions?