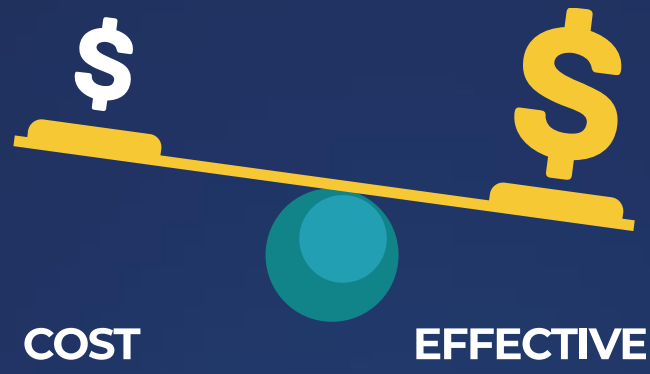
FAIR CONFERENCE 2019

Enabling Risk Management Programs That Actually Work

JACK JONES
Chairman,
The FAIR Institute



FAIR CONFERENCE 2019

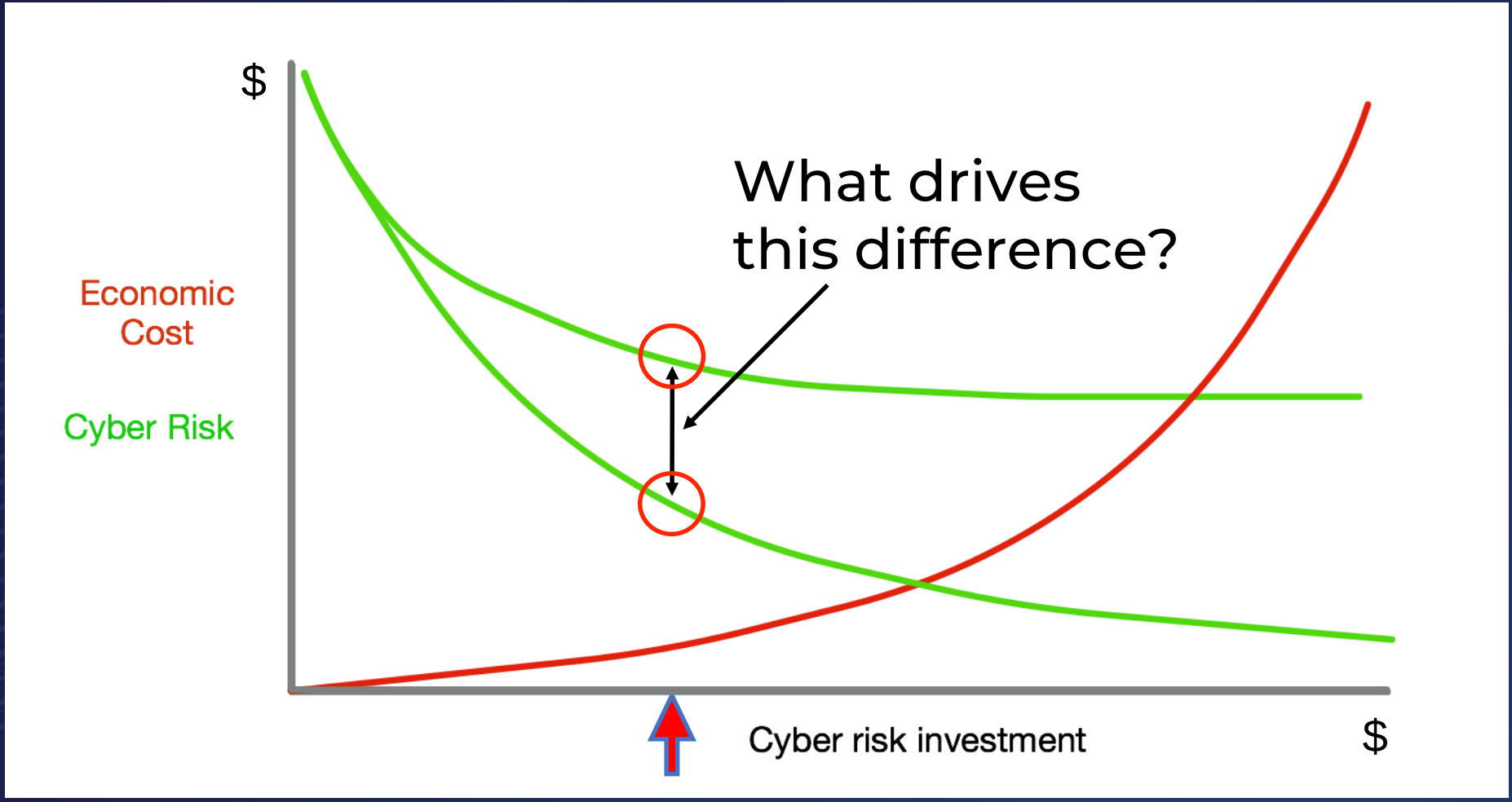
...cost-effectively

FAIR CONFERENCE 2019

What is the cost of a $5,000,000 risk management program*?

*Salaries, benefits, services, technologies, etc.

Why it matters...



FAIR CONFERENCE 2019

Decisions

How cost-effectively we apply our risk management resources.

Prioritization

FAIR CONFERENCE 2019

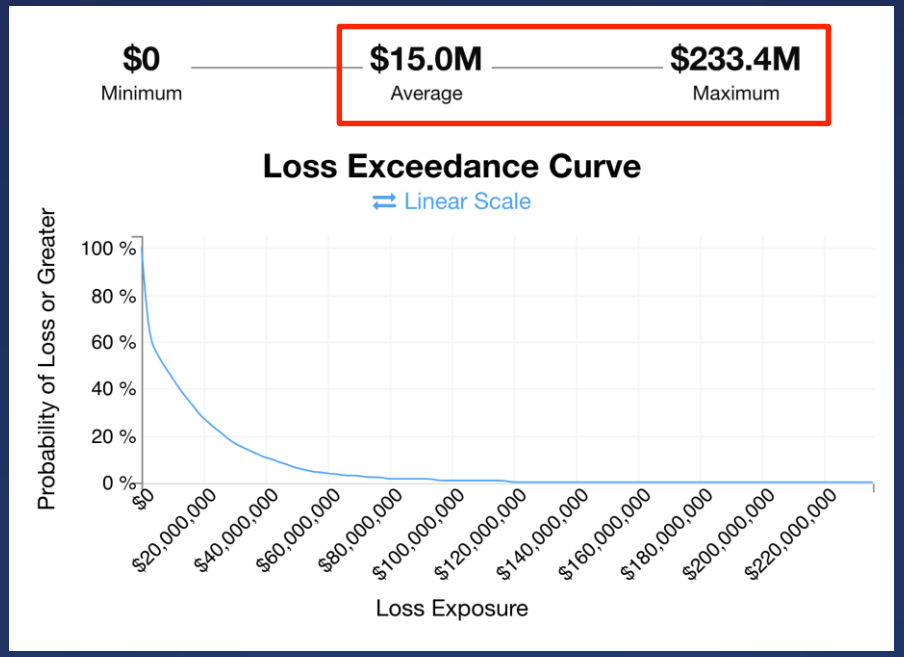
- A vulnerability scanner identifies a web application with a SQL injection weakness. The scanner's scoring model (CVSS) labels the weakness as "critical".
- Software development resources are redirected from other work to correct this weakness.
- However, this application is: a) not Internet-facing, b) requires authentication in order to find and exploit the SQL injection flaw, and c) doesn't have access to sensitive information.
- If the organization had postponed remediation, it is extremely unlikely to experience a significant loss event. Therefore, resources could have been better applied to other, higher-risk concerns.

Prioritization

FAIR CONFERENCE 2019

An audit discovered that privileges are not consistently being updated for user accounts with access to a customer service application containing credit card numbers.

A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.

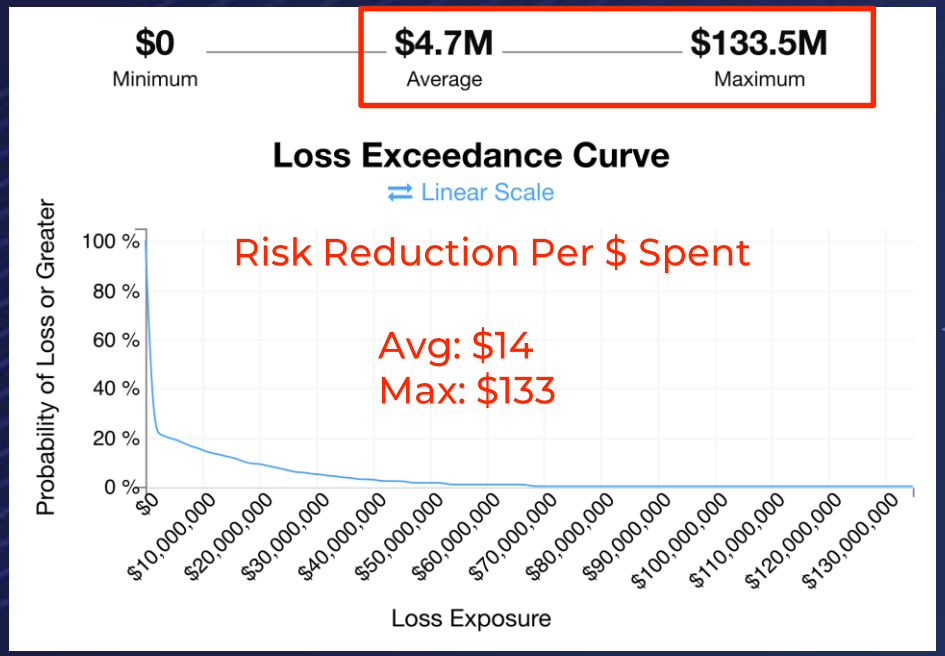


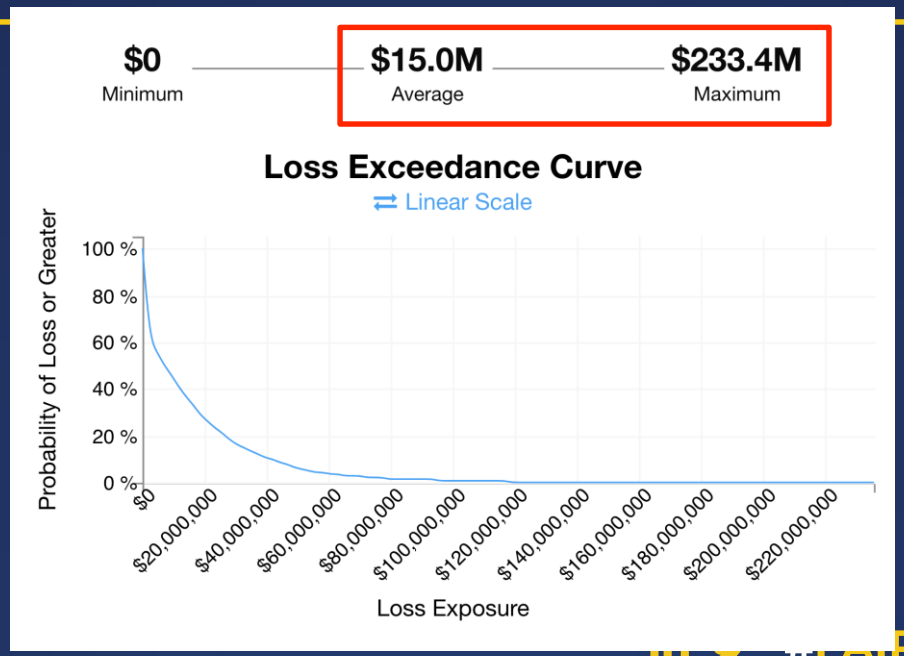
What's the ROI for "fixing" it?

FAIR CONFERENCE 2019

A risk reduction solution was identified that was going to cost $750k in year 1, and approx. $300k yearly thereafter.

A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.





#FAIRCON19

Top risks…

- The “cloud”
- E-mail
- Reputation
- Phishing
- Ransomware
- Internet of things (IoT)
- Insiders
- Patching
- Shadow IT
- Technology debt

What is expected to happen when top risks have been identified?

FAIR CONFERENCE 2019

The problem is fairly obvious, but…

Culture — The Biggest Hurdle?

FAIR CONFERENCE 2019

- Culture boils down to beliefs, which drive values and behaviors
- If stakeholders believe…
  - Quantitative analysis is too hard (or impossible), and/or
  - Qualitative measurement has been working well enough so far

…then you have to overcome those beliefs

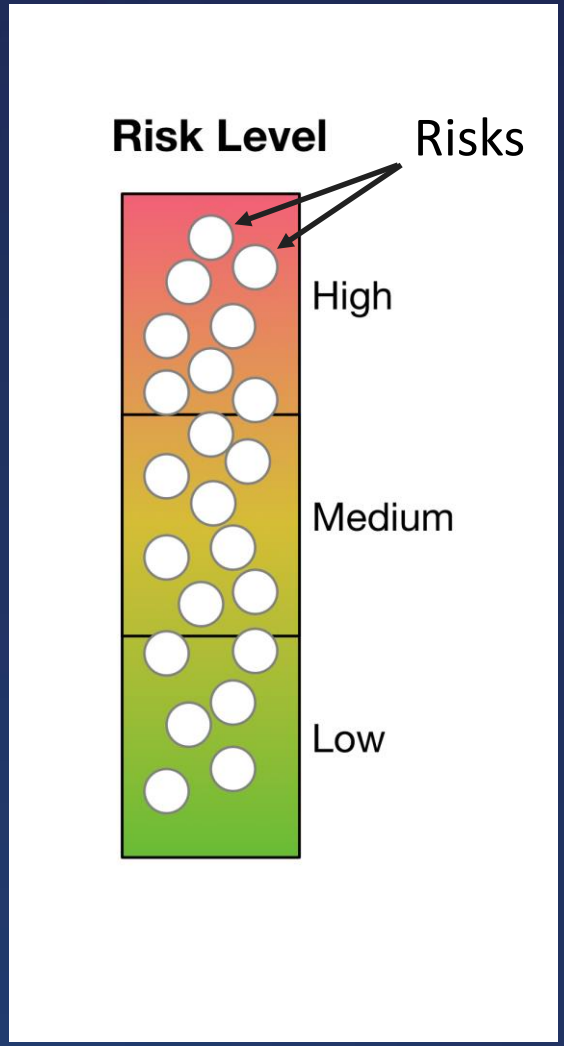
Education Regarding Qualitative Limitations

FAIR CONFERENCE 2019

- How much more risk does the highest “high” represent than the lowest “high”? (And do we even agree on which one is highest?)
- How much more risk does the lowest “high” represent than the highest “medium”?
- How much risk is there in aggregate?
- Why are the lines drawn where they are?

Are these reasonable questions?

How would you defend your responses?



But Logic Often Isn't Enough…

FAIR CONFERENCE 2019

You have to demonstrate meaningful value at an acceptable cost

Keep in mind you're competing against a zero-cost current state (zero accounting cost)

Elements of a Roadmap

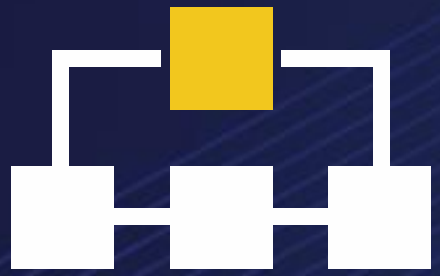
FAIR CONFERENCE 2019

Quantitative Risk Management Continuum

FAIR CONFERENCE 2019

Risk Landscape Clarity	Operational Decision Support	Strategic Decision Support	Automated Operational Decision Support
Top risk identification	Top risk measurement	Risk aggregation	Patch prioritization
Risk register cleanup	Cost-benefit analysis	Risk appetite definition and trending	3rd party landscape monitoring
Intra- and inter-team communication	Audit finding prioritization	Portfolio analysis	Near real-time risk landscape dashboard
Reduction in religious arguments	Policy exception request reviews	Board reporting	NOTE: Not yet a reality
	Zero-day analysis	M&A analysis	
	High value 3rd party analysis		

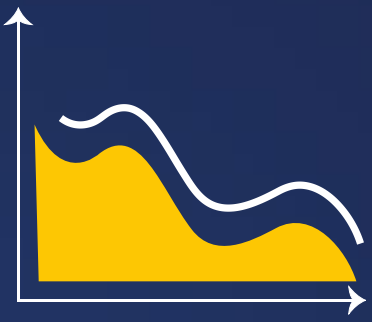
What Capabilities Enable Improvement?



Models

Skills

Data



Tools

Models

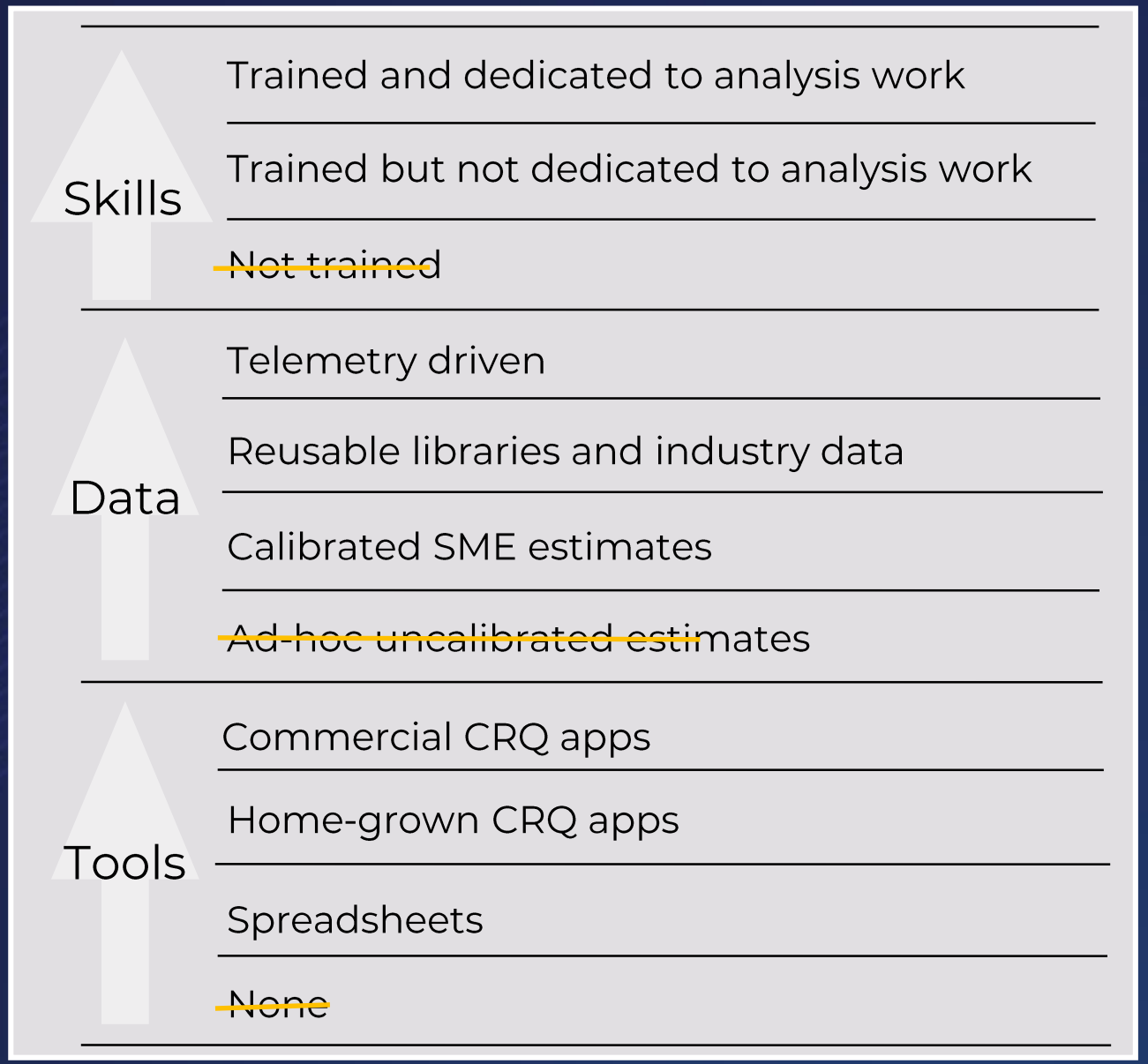
FAIR CONFERENCE 2019

TESTED

vs.

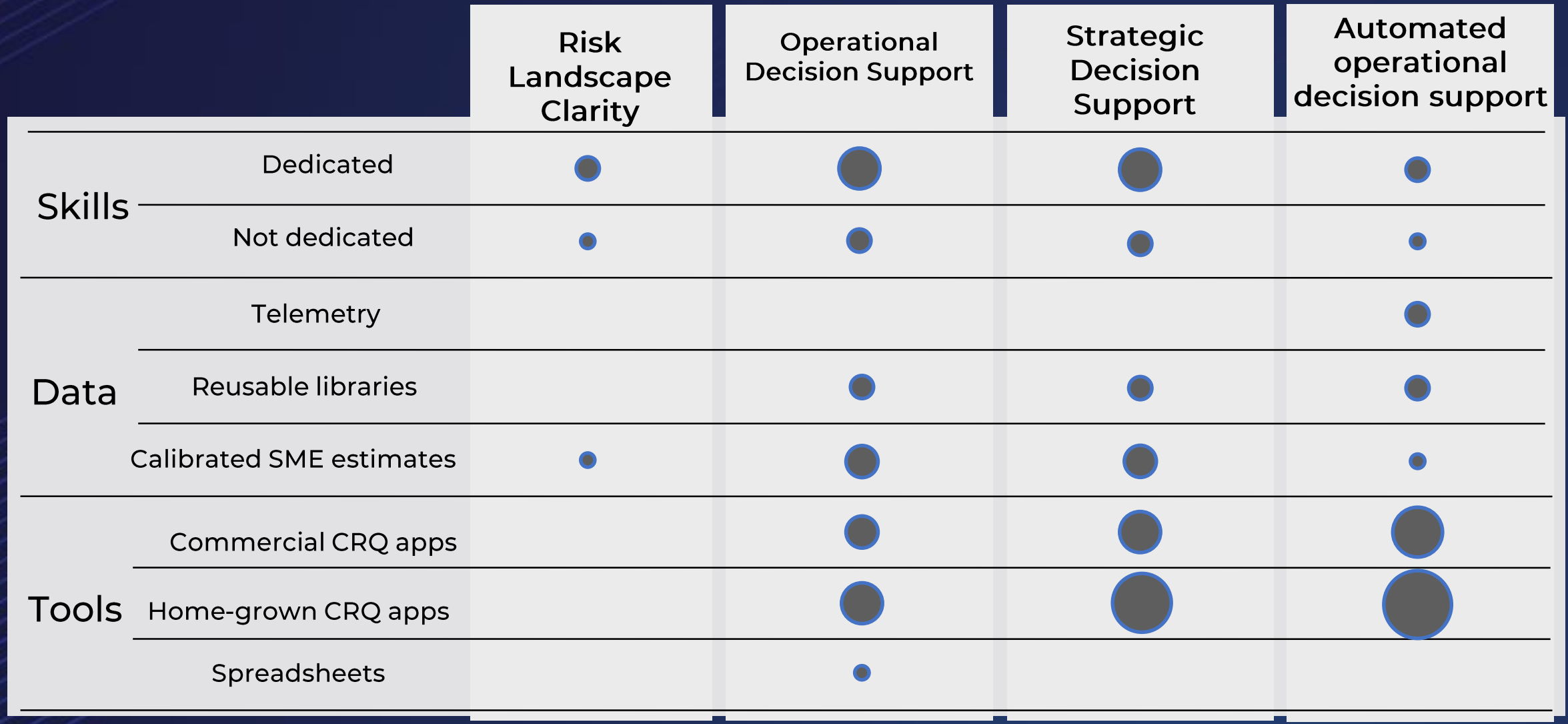
Mental Models

Capability Levels



Cost Implications

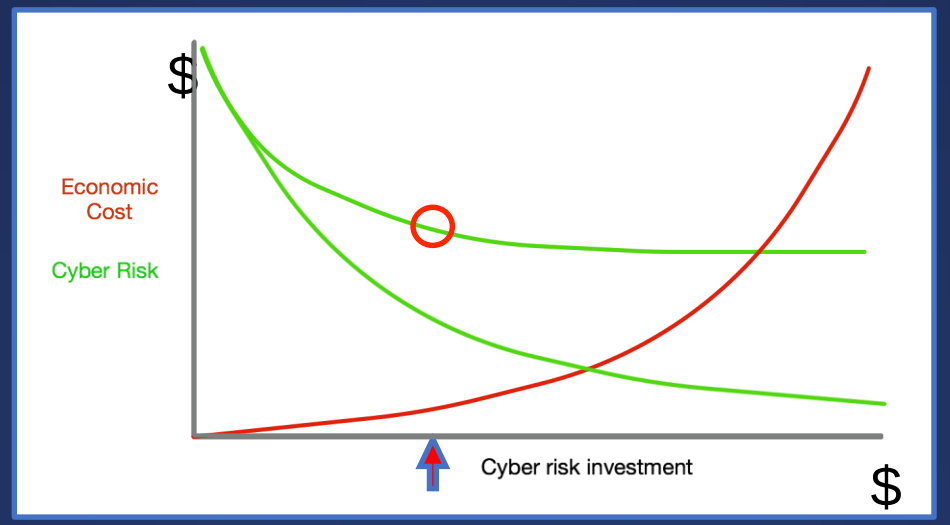
(Circle size reflects relative cost levels)



The Usual Starting Point…

- Mental models
- Uncalibrated ad-hoc estimates
- Untrained personnel
- No analysis tool

Low Cost
Low Efficacy



Roadmap Considerations

- Do you have executive support?
  - If not, where can you rapidly demonstrate obvious benefit at the lowest possible cost?
  - If so, identify their pain
- Budget?
- Available skills? (critical thinkers)
- Potential allies (and obstacles)

All Roadmaps Begin with…

Critical thinking skills

Risk analysis training

A clearly defined initial objective

An Example Starting Point

Evolving to…

The First Steps are the Hardest

FAIR CONFERENCE 2019

Start doing analyses

FAIR CONFERENCE 2019

Wrapping up…

- We have a responsibility to help our organizations and industry manage risk as cost-effectively as possible.
- This requires that we continually evolve our ability to measure risk.
- Every organization will need to define a roadmap that fits its risk management objectives and constraints.
- As leaders in our profession, our ability to drive cost-efficacy into our programs will differentiate us from those who are driven by checklists and mental models.

FAIR CONFERENCE 2019

Questions?

FAIR CONFERENCE 2019

Enabling Risk Management Programs That Actually Work

JACK JONES
Chairman,
The FAIR Institute