FAIR Institute Breakfast Meeting

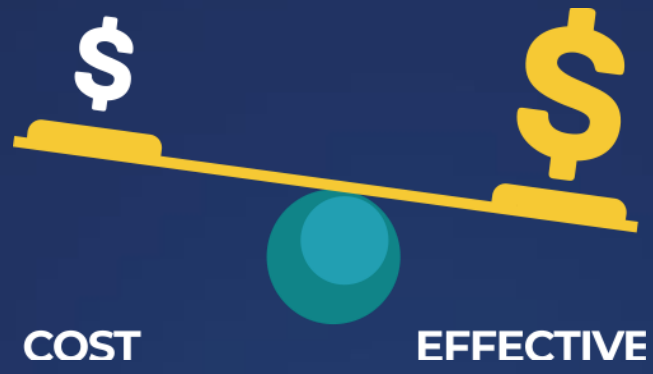
Enabling Risk Management Programs That Actually Work

February 26, 2020, 7:30 - 10:30 AM PST
Parc 55 San Francisco,
Embarcadero Room (Level Three)

@FAIRInstitute #NetworkWithFAIR

Enabling Risk Management Programs That Actually Work

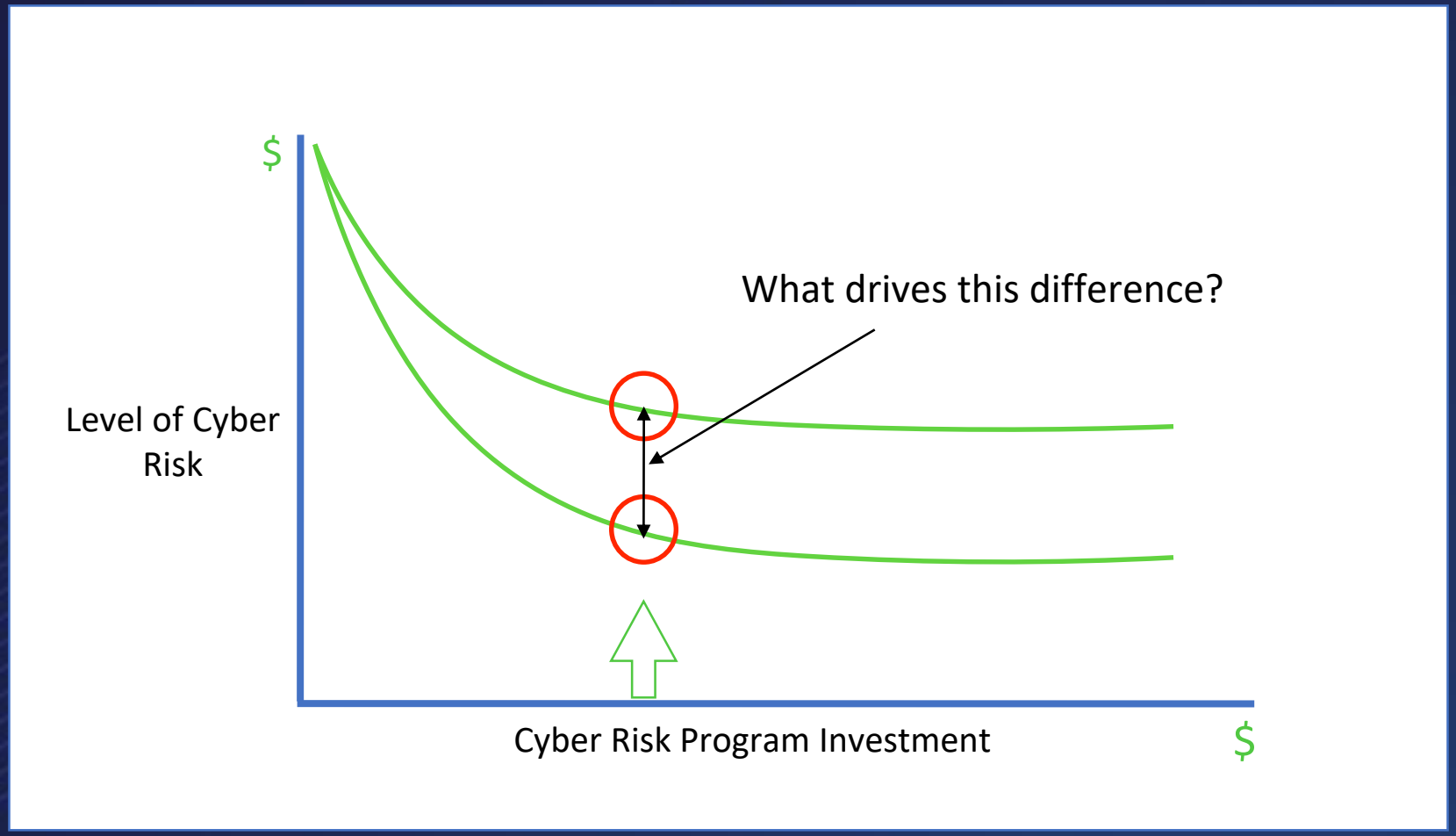
Jack Jones
Chairman, FAIR Institute
Co-Founder and Chief Risk Scientist, RiskLens



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

*Salaries, benefits, services, technologies, etc.

Why it matters…



Decisions

How cost-effectively we apply our risk management resources.

Weak password

Missing patch

Cyber criminals

Which of the “Highs” is highest?

Outdated policy

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?

Prioritization example #1

SQL Injection weakness!

- Not Internet-facing
- Requires authentication
- No sensitive data

Prioritization example #2

Unreliable access privilege management

Weak intrusion detection

Which to fix first!

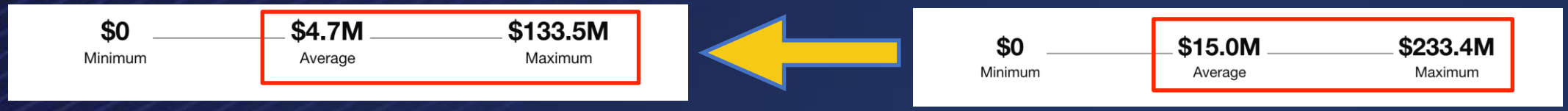
What's the ROI for "fixing" it?

Improvement cost:

Year 1: $750k

Year 2: $300k

Weak intrusion detection



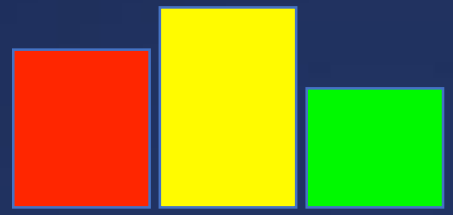
Risk Reduction Per $ Spent

Avg: $14

Max: $133

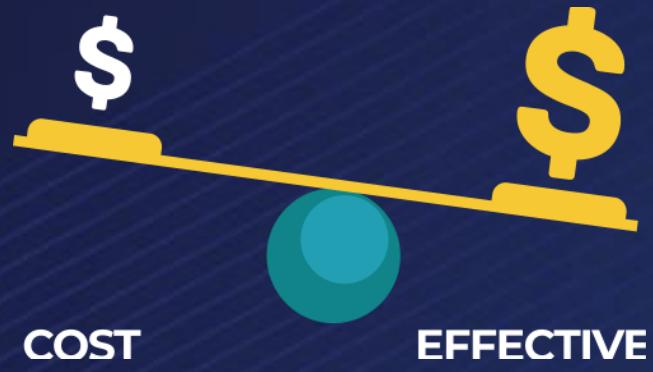
Beliefs — The Biggest Hurdle?

“Too difficult”



"Good enough"

But Logic Often Isn't Enough…



Elements of a Roadmap

Start with “Why”?

Quantitative Risk Management Program Continuum

RISK LANDSCAPE CLARITY

Top Risks Identification
Audit Findings Prioritization
Policy Exception Request Reviews
Emerging Threat Analysis

OPERATIONAL DECISION SUPPORT

Top Risk Assessments
Comparative Analysis
Cost-Benefit Analysis
High-Value 3rd Party Analysis

STRATEGIC DECISION SUPPORT

Risk Aggregation and Trending
Risk Appetite Definition
Risk Portfolio Analysis
Board Reporting

AUTOMATED DECISION SUPPORT

Real-Time Risk Dashboard
Controls Management
3rd Party Landscape Monitoring

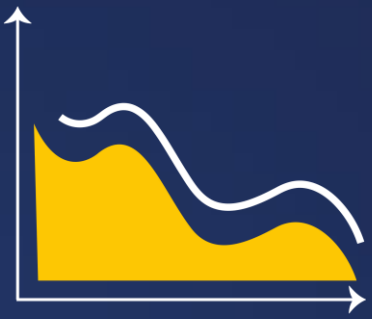
Source: RiskLens FAIR Enterprise Model™

What Capabilities Are Required?

Models

Skills

Data



Tools?

Models

TESTED

vs.

NOT TESTED

An Example Starting Point

		Risk Landscape Clarity	Operational Decision Support	Strategic Decision Support	Automated decision support
Skills	Dedicated				
	Not dedicated	✓			
Data	Telemetry				
	Reusable libraries				
	Calibrated SME estimates	✓			
Tools	Commercial CRQ apps				
	Home-grown CRQ apps				
	Spreadsheets				

Evolving to…

		Risk Landscape Clarity	Operational Decision Support	Strategic Decision Support	Automated decision support
Skills	Dedicated		✓		
	Not dedicated				
Data	Telemetry				
	Reusable libraries				
	Calibrated SME estimates		✓		
Tools	Commercial CRQ apps		✓		
	Home-grown CRQ apps				
	Spreadsheets				

All Roadmaps Begin with…

A clearly defined initial objective

Risk analysis training

Roadmap Considerations

Executive Support

Budget

Potential Obstacles

Critical Thinking Skills

“All things are difficult before they are easy.”

Thomas Fuller

The First Steps are the Hardest

Just start doing analyses

Wrapping up…

Why it matters…