



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)

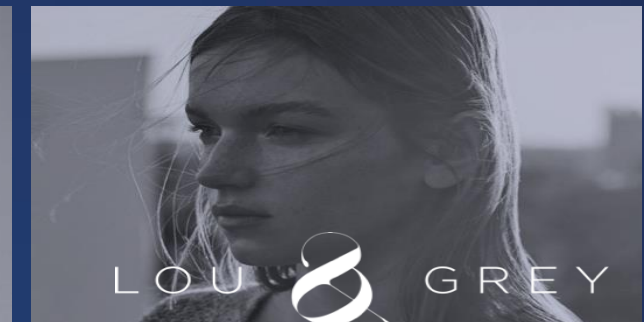
  @FAIRInstitute #NetworkWithFAIR



ascena
RETAIL GROUP INC.

FAIR at Ascena Retail

Mark Tomallo
Chief Information Security Officer



Uses within ascena Retail Group



• 3rd Party Risk

- Assess 150-200 vendors/month
- Limitation of Liability
 - Moved to Security Program and Value
- HIGHLIGHT: \$2M—\$40M in transferred liability per vendor
- Vendor selection

• Risk Acceptance

- Project prioritization and review
- Consistent calculation
- Consistent communication
- HIGHLIGHT: “I’ve never seen it laid out like this. No way I’m signing off on that.”

Audit Conversations

- Methodology
- Consistency mentioned earlier
- HIGHLIGHT: “Significant Deficiency” negotiated down to “Deficiency.”

In each of these examples, Risk is positioned “with” our lines of business. The perception is that we are on the front lines “fighting” for our business.

How Did We Roll it Out?

1. Talk the Talk

- Start using the FAIR nomenclature
- Start talking in terms of “Loss”
- Bring in SME’s/LOB and enable them to establish ‘loss tables’ (agreed upon calculations of loss)

2. Begin with IT

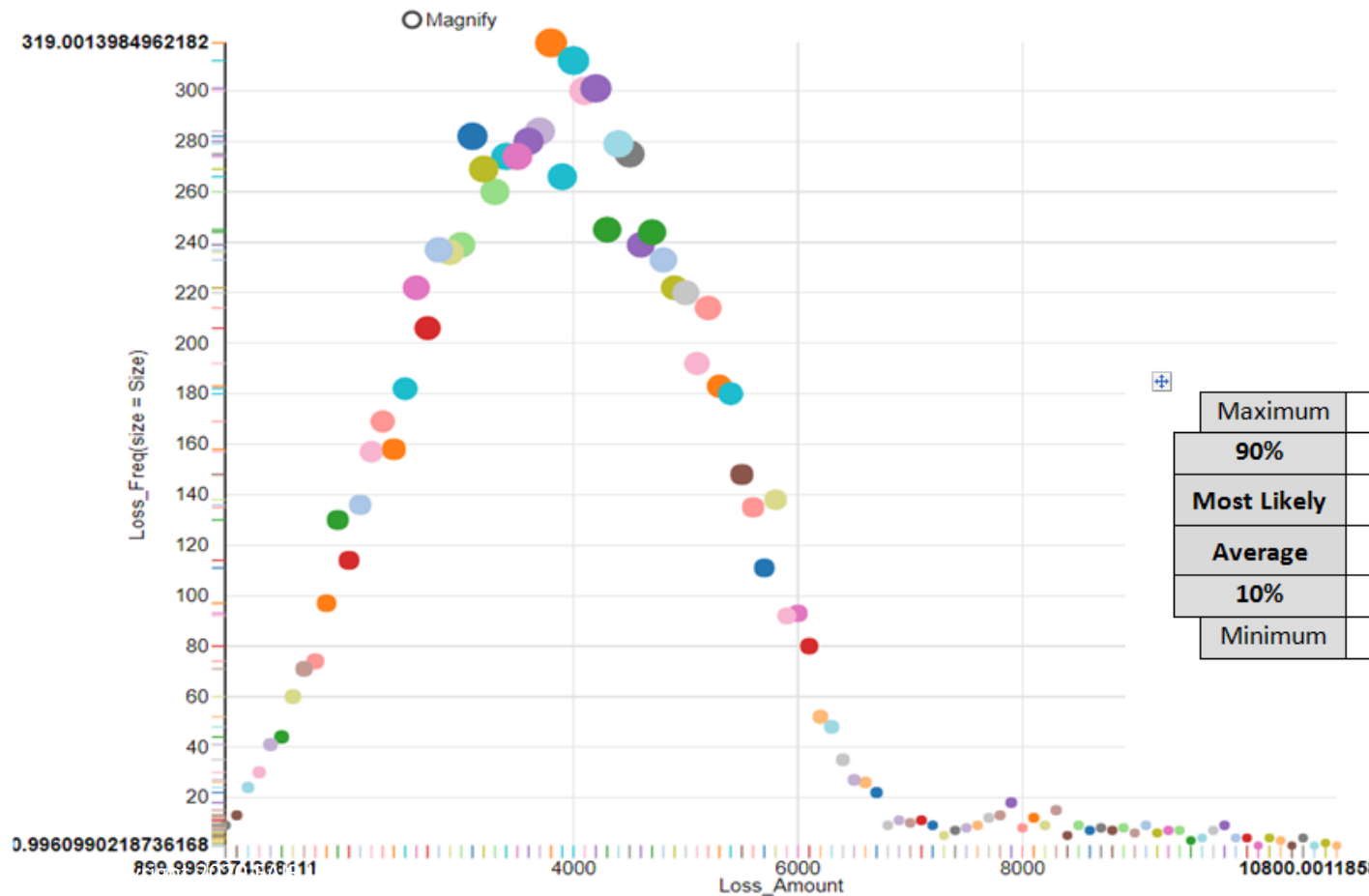
- In parallel, perform “Top 10 Risks” interviews with VP’s, then do similar exercise with Risk team
- Run FAIR Analysis on all. Big effort but many will be fast
- Discuss results with team:
 - Many will not even be risks
 - Actual risks will be less than expected

3. Run it

- In stealth mode, run FAIR against IT projects or IT Audit findings
- Repetition builds understanding
- Defend the Numbers!! Iron Sharpens Iron so rip it apart
- Use results to your advantage—Bring in the business when analysis supports their position
- Periodic update of ‘loss table’

Quantitative Conversations

The graph below represents 50,000 simulations of a loss event with the given parameters. Instances where there is no loss experienced have been eliminated. The loss amount of zero was reflected 79% of the time or 39,887/50,000 simulations. Only losses in excess of \$0 have been magnified.



Maximum	\$12K
90%	\$4K
Most Likely	\$0
Average	\$819
10%	\$0
Minimum	\$0

Simulations are meaningful

- Shows magnitude
- Shows Rigor

