



Pen Testing Your Board Pitch: An Interactive Exercise

Moderator: KIM JONES

Professor of Practice, Arizona State University

JAMES LAM

Head of Risk Committee, Director, E*TRADE

CHRIS INGLIS

Board of Directors Member FedEx, KeyW, Huntington Bank

CYBER RISK MANAGEMENT WORKGROUP

Steve Reznik, ADP Jeff Welgan, CyberVista

1 Copyright 2019 FAIR Institute, Inc.



A Breach Scenario: Tale of Two Banks

- Bank of the Isles fell victim to a massive cyber breach.
- Cybercriminals spearphish employee > malware downloaded > unpatched customer database compromised
 - Critical-level vulnerability announced 6-weeks prior
 - Over 2.3 million customers across 6 states affected
- Bank of the Isles is expected to lose approximately \$7.5M+



Breached!





n 🎔 🛛 #FAIRCON19



"The Bad Way"

An example of how not to brief the Board





Insights From the Board









"The Better Way"

A more meaningful Board briefing





VALE.

CYBER RISK DASHBOARD

	CYBER RISK			
	STRATEGIC RISK AREA		K METRICS	SUMMARY
Ð	A. Culture & Capability	Acceptable	100% 90% 70% 60% 40%	EEDANCE CURVE
Ð	B. Legal & Regulatory Compliance	Acceptable	100% 90% 70% 60% 40%	EDANCE CURVE
Ð	C. Data Integrity & Protection	Needs Review	100% 90% - LO 80% - 60% - 60% 50% - 60% - 60%	OSS EXCEEDANCE CURVE
Ð	D. Availability of Systems & Information	Needs Review	100% 90% 80% 60% 50%	EEDANCE CURVE
Ð	E. 3rd Party Risk & Due Diligence	Acceptable	100% 90% 70% 60% 40%	EEDANCE CURVE

in 🎔 #FAIRCON19

CYBER RISK DASHBOARD







in 🕑 #FAIRCON19





in 🎔 #FAIRCON19

CYBER RISK DASHBOARD





in y #FAIRCON19

WALE.

Material

Tolerance

Early Warning





in 🎽 #FAIRCON19





in y #FAIRCON19

Commercial A/P Systems - Options

in 🕑 #FAIRCON19

Insights From the Board

Cyber Risk Working Group

Update on Exec-Focused Cyber Risk Dashboard Research Project

CRWG Update

Project Milestones:

- 1. Establish core principals for cyber risk dashboards
- 2. Define/validate "strategic risk areas"
- 3. Establish/validate taxonomy, and 'tag' key inputs to each strategic risk area
- 4. Create methodology and mathematical model for 'cyber performance index' calculations
- 5. Test model and dashboard using genericized/anonymized data

Cyber risk scenarios

grouped to SRAs

Inputs from cyber risk

processed via the FAIR

Model

scenarios get analyzed and

FAIR Model

Cyber Risk (Aggregate Loss

expectancy for each SRA)c

Cyber Performance Index

FICO-like cyber performance score

in 🎐 #FAIRCON19

Thank You

