

# FAIR: Okay, Now What?

Setting Up a Quantitative Risk Program Anywhere

Michael Meis

## Introduction

# Michael Meis



**A**

Over 13 years  
experience in  
Cybersecurity

**B**

M.S. Cybersecurity,  
MBA

**C**

Led programs  
for DoD, USDA,  
& H&R Block

**D**

Associate CISO for  
University of  
Kansas Health  
System

# My Journey to Cyber Risk Quantification



### **Confusing Terminology**

Nobody understands what we are talking about... including us



### **Broken Math**

(Red + Yellow)Critical –  
(3.5/Effective) = “Do This”  
MATH!

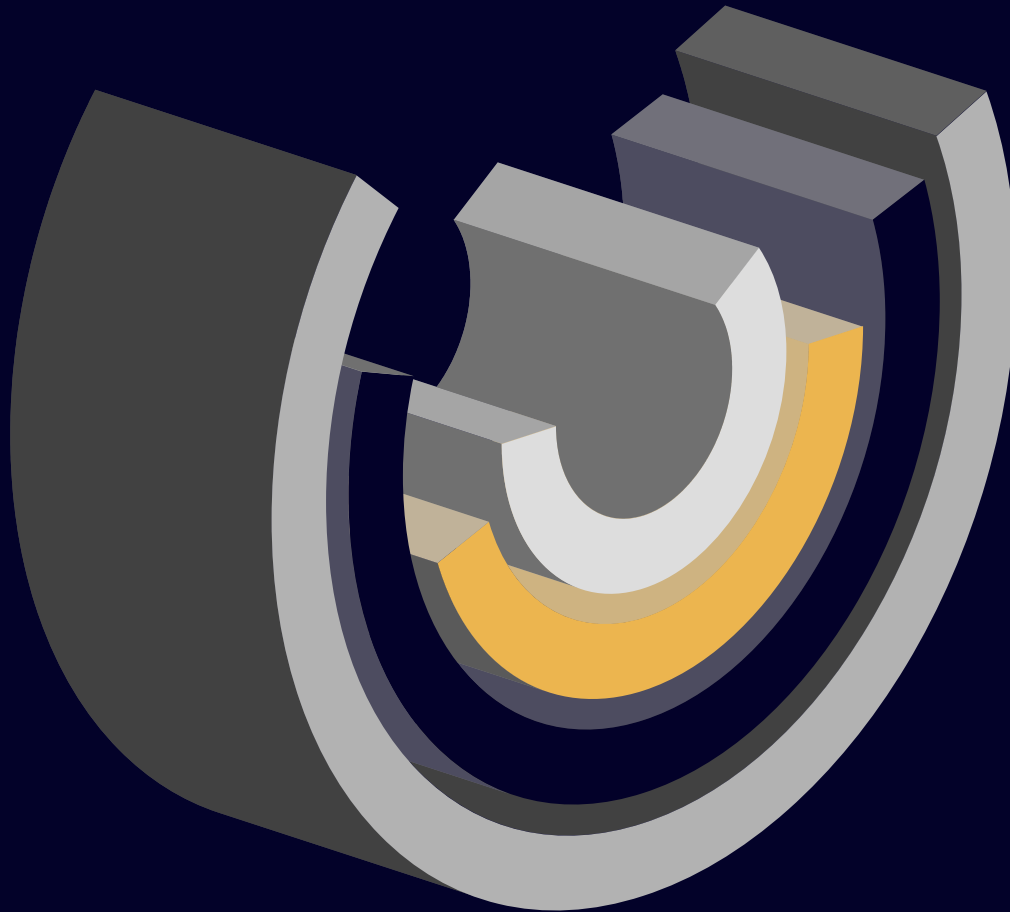


### **Insufficient Training**

Not enough formal training.  
Too much learning on the job. Overly focused on frameworks.

# FAIR Adoption Drivers

# How Does FAIR Help?



- ▶ **A Transparent & Consistent Method For Measuring Risk**
- ▶ **A Foundation For Effective Prioritization**
- ▶ **A Framework For Communication**
- ▶ **Robust Community & Training**

# Okay, Now What?

FAIR Adoption Approaches

**1**

**Top Down**

**2**

**Bottom Up**






**3**

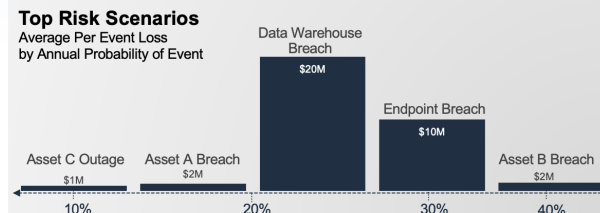
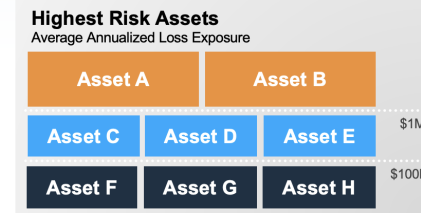
**Big Game  
Hunting**

# Top Down

## Cyber Top Risk Dashboard

Includes 20 risk scenarios identified for 15 assets broken into 4 risk categories

Risk Categories					Annualized Loss	Roadmap Initiative
Aggregated risk scenarios, 10 <sup>th</sup> - 90 <sup>th</sup> %						
	\$10M	\$20M	\$30M	\$40M	\$50M	
<b>Insider Access</b> Loss caused by priv. insiders (malicious or error)						\$100K - \$6M • Multifactor Authentication • Priv. Access Management
<b>Endpoint Security</b> Loss from end user software or devices						\$0 - \$8M • Endpoint Detection
<b>Customer Data Compromise</b> Loss due to customer data being compromised						\$0 - \$42M • Network Access Controls
<b>Corporate Data Theft</b> Loss affecting collections of corporate data						\$100K - \$5M • App Security Upgrade • Data Loss Prevention
						

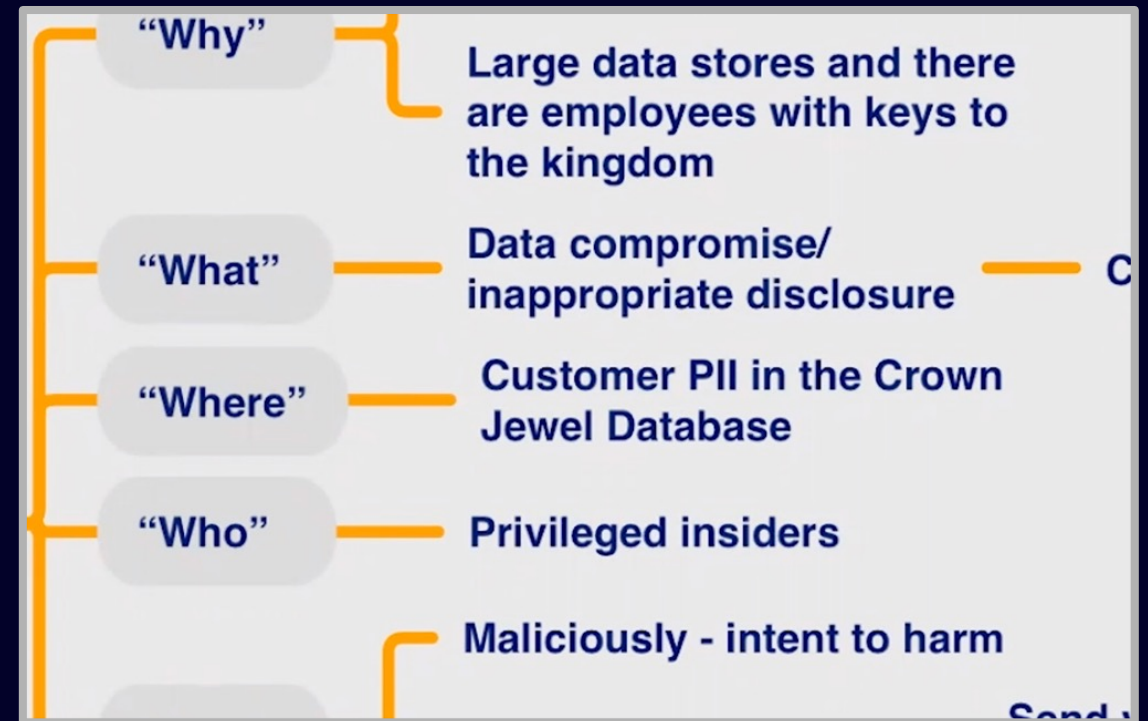


- Begins with key organizational risks
- Designed to build momentum at the Board/SLT level
- Most resource intensive approach
- Longer Time To Value



# Bottom Up

- Takes existing risks/issues and converts to risk scenarios
- Builds momentum with less visibility
- Less resource intensive
- Shorter time to value
- Sometimes difficult to connect with ERM or strategic planning



# Big Game Hunting



- Find a big decision/problem and use quantification to provide additional context
  - Audit finding, big investment, etc.
- Can build immediate buy-in
- Size of upfront investment can vary widely



# Helpful Advice

AKA: Avoiding The Mistakes We All Made





**Know Your "Why"**

# Don't Be A Hero





# Train, Train, & Train Some More

- Dedicate resources to formal training, beyond FAIR training
- Read..... A lot
- Engage in the FAIR and CRQ communities



# Build & Sustain Momentum

- Get some quick wins
- Communicate when wins will come along the way
- Shift focus to sustainment and scale
- Ensure you understand how, where, and when to use qualitative methods
- Integrate with existing process wherever possible









# Thank You!

Michael Meis  
[Michaelmeis.com](https://michaelmeis.com)