FAIR CONFERENCE 2019

Use Case Panorama: How Quantification Enables Risk-Aligned Decision Making

LUKE DOMET
Technology Risk and Information Security Professional,
Fidelity Investments

INDIA SUTTON
Cyber Risk Analyst
Daimler Mobility

Moderator: CHRIS PATTESON
Executive Director
Risk Transformation Office,
RSA

ALEX ROGOZHIN
VP of Information Security
Data Intelligence,
BB&T

LAURA VOICU
Senior Security Architect,
Swisscom

#FAIRCON19

FAIR CONFERENCE 2019

How quantification enables risk-aligned decision making

The Swisscom Journey

Laura Voicu, Swisscom

A Brief History

Now we have the chance to benefit from new opportunities

FAIR CONFERENCE 2019

Gut feeling decision making

Green-yellow-red risk assessments, incoherent or insufficient information, is cloud computing really a risk?

Fact based decision making

Risk management framework, FAIR methodology, lean risk management processes, and a better understanding of the actual risk exposure

AI-driven and automated decision making

Everything is coming together. Data and insights are automatically integrated in risk management to better support decision making

...?

We don't yet know what the future will bring. What we do know is that the next wave is coming.

2018

TODAY

2020

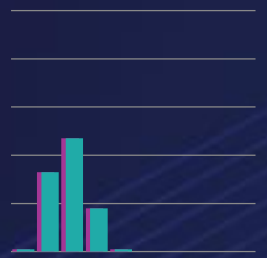
? ? ?

...

#FAIRCON19

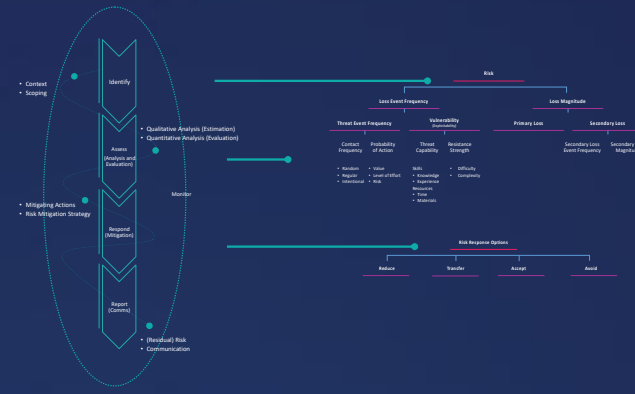
Current State of Information Risk Management
The journey has just begun

FAIR CONFERENCE 2019

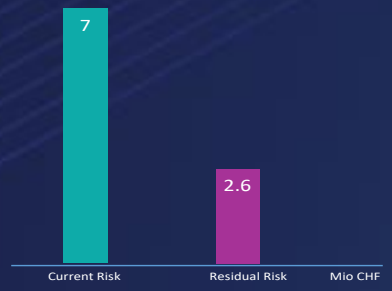


FAIR for Risk Assessment

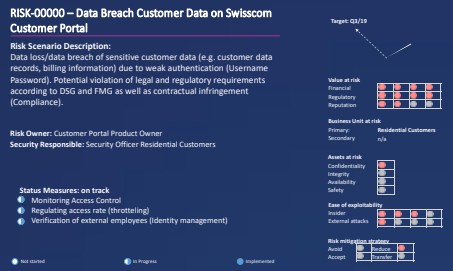
Framework



Process



Reporting

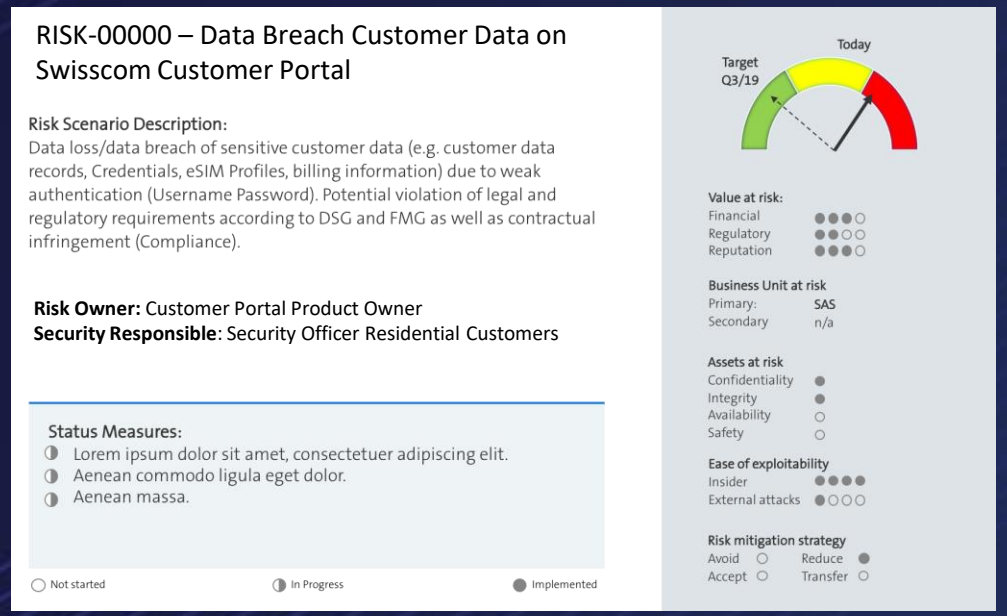


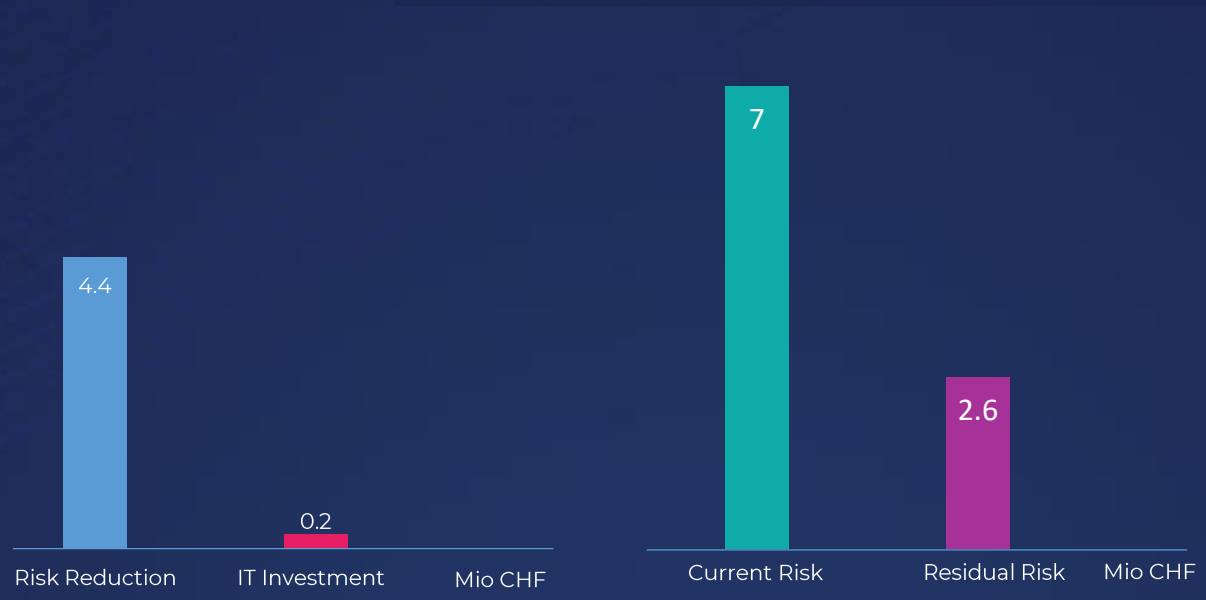
Management Summary

Make the Change

4.4 Mio CHF Average Risk Reduction

- Reduction of secondary loss magnitude of data breach
- Reduction of primary response efforts





Analysis	Min	Average	Max	Vulnerability
Data Breach of sensitive customer data – without two-factor authentication	0 CHF	7 Mio CHF	15 Mio CHF	80%-90%
Data Breach of sensitive customer data – with two-factor authentication	0 CHF	2.6 Mio CHF	5 Mio CHF	20%-40%

Take Aways

FAIR CONFERENCE 2019

TAKE AWAYS

Bring the discussion to the people who can affect change

Approach business as risk takers and risk owners (If you approve the budget, you own the risk)

Think big, start small

From Proof of Concept with small number of stakeholders to alignment with operational and enterprise risk management

Manage risks for today and tomorrow

Keep the topic on the radar and launch a feedback loop between business and risk management functions

Think critically, communicate clearly

View a complex problem from multiple perspectives, and accept the fact that uncertainty is always present.

FAIR CONFERENCE 2019

Demonstrating the Value of FAIR in a Grassroots Manner

Alex Rogozhin, BB&T

FAIR CONFERENCE 2019

Disclaimer

The views that I express are my own and do not necessarily represent those of the BB&T Corporation, SunTrust Banks, Inc. or Truist Financial Corp.

Grassroots (bottom-up) Approach

FAIR CONFERENCE 2019

Our journey was slightly different from most large organizations… Our FAIR implementation started as a grassroots effort in the Information Security Data Analytics team and expanded in scope over time.

1. **Pilot: Data Encryption at Rest.** Demonstrate that the model works in BB&T's environment using our data.
2. **Professional Services: Prioritization of remediation efforts for Payments Ecosystem.** Demonstrate pragmatic business value for Information Security operations.
3. **Model validation with Model Risk Management**. Operationalizing the FAIR model for the Information Security department.

Pilot → Professional Services → Operationalization

FAIR CONFERENCE 2019

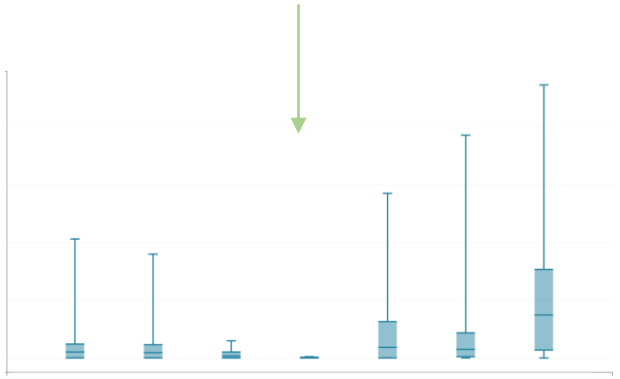
Pilot

Data Encryption at Rest

# of Records	Annualized Loss Exposure		
	Before	After	Reduction
50K	$300K	$50K	$250K
250K	$1M	$50K	$950K
1M	$3M	$55K	$2.9M
10M	$20M	$200K	$19.8M
50M	$30M	$300K	$29.7M

Professional Services

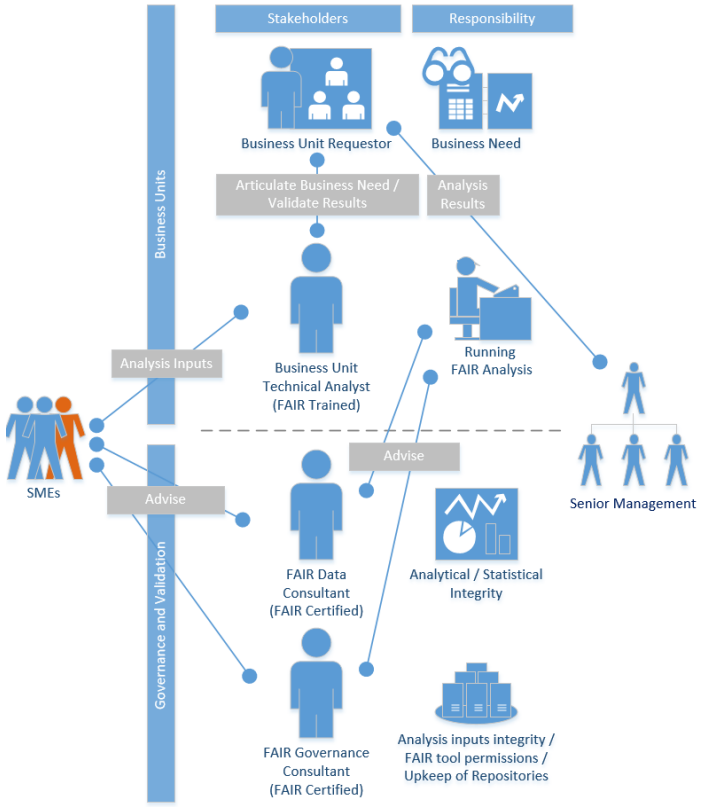
Prioritization of remediation efforts for Payments Ecosystem



Additional insights gleaned from FAIR analysis:

Limiting the maximum amount lost via fraudulent wire to $X, whether via additional internal controls, insurance coverage, etc., would reduce the maximum ALE by 30%.

Operationalization



Key Takeaways

Based on our experience implementing FAIR in a grassroots manner, the following were the key takeaways.

FAIR CONFERENCE 2019

1. **Gradually demonstrate business value.** By following "Pilot -> Professional Services -> Operationalization" approach we removed management's anxiety about failure: were we to fail at the early stages, political impact and material losses to the executive sponsor would be minimal. This enabled us to grow FAIR organically and implement lessons-learned along the way.

2. **Be aware of and manage political forces "FOR" and "AGAINST".**

FOR	AGAINST
○ Regulatory requirements ○ Pragmatic managers ○ Executive sponsor ○ Building alliances	○ Always done it another way ○ Resistance to change ○ Fear of being left behind

3. **Be willing to educate, partner, and pass-on the responsibility**. Throughout the process, we have given numerous presentations across the IT organization. We identified key stakeholders who could either enable or derail the implementation of FAIR, and either gained their support or mitigated their impact. Finally, we partnered with the IT Risk function, preparing them to be the future owners of FAIR capability.

FAIR CONFERENCE 2019

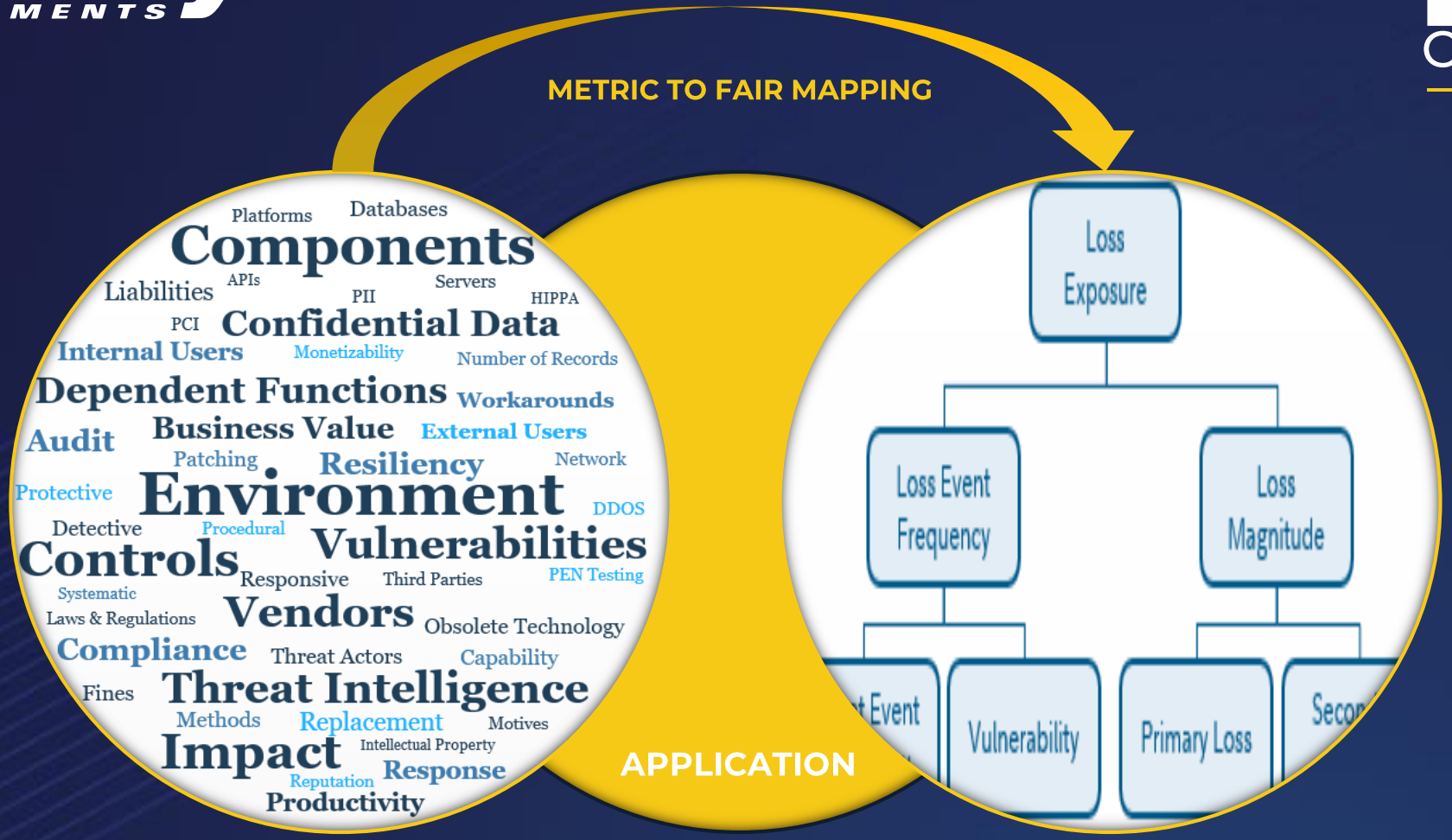
Fidelity® INVESTMENTS

Where do we focus?

Luke Domet,
Center of Excellence Lead -
Technology Risk Assessments

Fidelity INVESTMENTS

FAIR CONFERENCE 2019



Application

FAIR

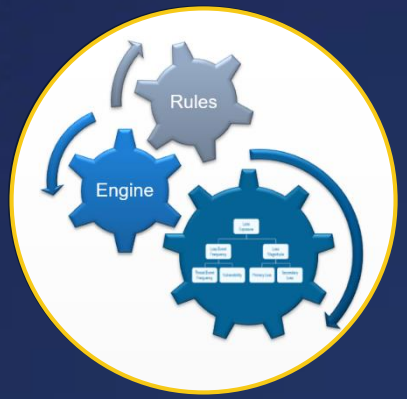
Fidelity INVESTMENTS

FAIR CONFERENCE 2019

How do we scale?

Application Portfolio

Automated Metrics Gathering



Automated Estimating Engine

Portfolio Heat Map

Fidelity®
INVESTMENTS

Where do we focus?

FAIR CONFERENCE 2019

Daimler Mobility CyberSecurity

CYBER RISK IS BUSINESS RISK

ENABLING BUSINSS-DRIVEN SECURITY THROUGH CYBER-RISK QUANTIFICATION

INDIA SUTTON
Global Cyber-Risk Management Specialist

#FAIRCON19

Daimler Mobility CyberSecurity

FAIR CONFERENCE 2019

PART 1: THE STORY

CYBERSECURITY TRANSFORMATION

- CREATE MEANINGFUL MEASUREMENTS TO UNDERSTAND RISKS IN OUR ENVIRONMENT
- PRIORITIZE AND INVEST IN CAPABILITIES THAT ADDRESS RISKS
- EFFECTIVELY COMMUNICATE RISKS ACROSS THE BUSINESS

INDIA SUTTON
Global Cyber-Risk Management Specialist

Daimler Mobility CyberSecurity

FAIR CONFERENCE 2019

PART 2: THE GOAL

ENABLING BUSINESS-DRIVEN SECURITY

COMMUNICATING CYBER RISK IN FINANCIAL TERMS

How does our actual risk compare to our risk appetite?

Did risk decline or increase in the last quarter?

What assets represent the greatest risk exposure?

What percentage of aggregate loss exposure is driven by what control deficiency?

INDIA SUTTON
Global Cyber-Risk Management Specialist

Daimler Mobility CyberSecurity

PART 3: THE PROCESS

BUILDING BLOCKS

FAIR CONFERENCE 2019

CYBER RISK QUANTIFICATION PROGRAM

SCOPED RISK SCENARIOS

500 ATTACK VULNERABILITIES

Function of prior incidents and security problem management input

Control gaps and issues from internal risk register

SELECTED A CRQ TOOL

RiskLens®

Purpose-built on FAIR performs Monte Carlo simulations

Randomizing data inputs over 5,000+ iterations to ensure best statistical probability of model output

COLLECTED DATA

50% OF CROWN JEWELS

High-criticality, enhanced-protection applications containing millions of NPPI records

Threat actors their motivations and attack vectors to build attack scenarios developed using Daimler Mobility AG's Security Operations Center inputs

INDIA SUTTON
Global Cyber-Risk Management Specialist

Daimler Mobility CyberSecurity

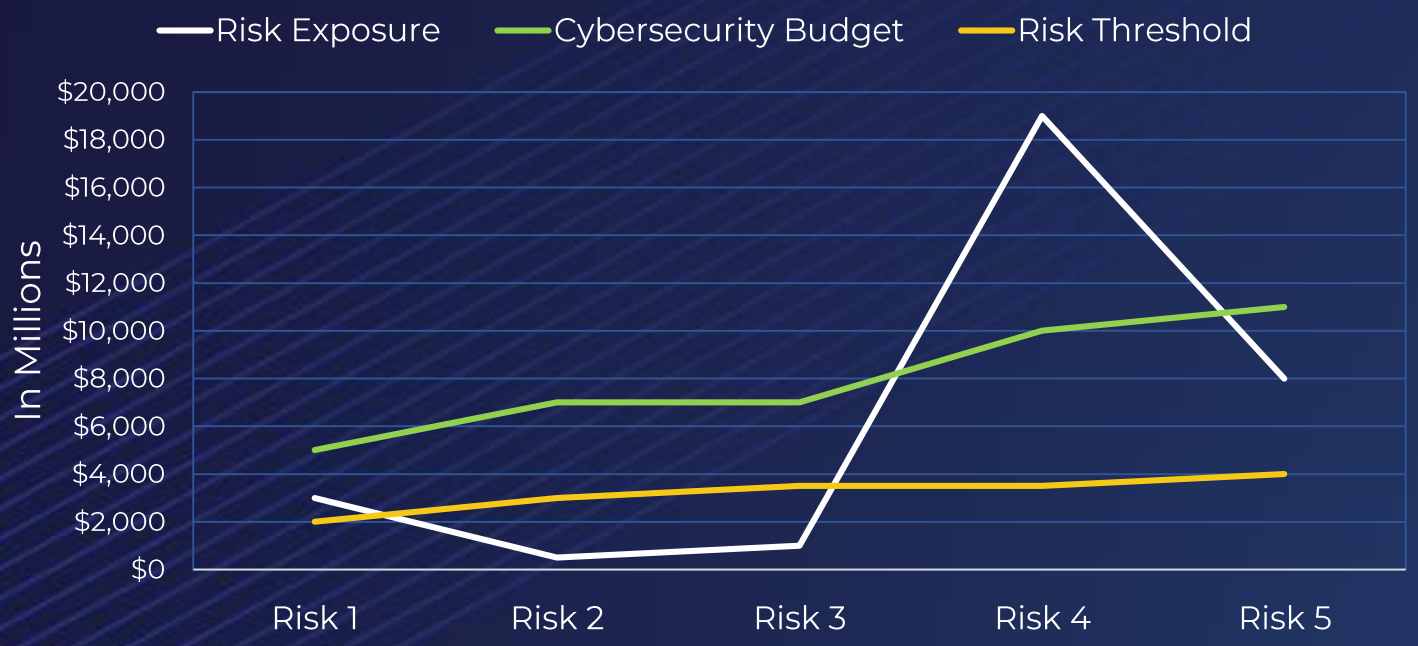
PART 3: THE PROCESS

BUILDING BLOCKS

FAIR CONFERENCE 2019

CYBER RISK QUANTIFICATION PROGRAM

THE TOP 5 CYBER RISKS IN FINANCIAL TERMS



	Risk Scenario	Likelihood	Risk Exposure
1	**Actor:** Cybercriminal **Motivation**: Data theft **Vector:** Vendor compromise **Outcome:** Disclosure (exploitation)	Threat Event Frequency: ~Annual **Likelihood: 20%**	**$3M**
2	**Actor:** Employee **Motivation**: Accident **Vector**: System upgrade **Outcome**: Application outage	Threat Event Frequency: ~Semi-annual **Likelihood: 8%**	**$0.5M**
3	**Actor**: Hacktivist **Motivation:** Data theft **Vector:** Phishing email, vulnerability exploit (remote code execution) **Outcome:** Disclosure (exploitation)	Threat Event Frequency: ~5 years **Likelihood:0.5%**	**$1M**
4	**Actor**: Cybercriminal **Motivation:** Financial gain **Vector:** Ransomware **Outcome:** Destruction	Threat Event Frequency: ~2 years **Likelihood: 2%**	**$19M**
5	**Actor**: Angry user **Motivation:** Revenge **Vector:** Credential misuse **Outcome**: Disclosure	Threat Event Frequency: ~5 years **Likelihood: 11%**	**$8M**

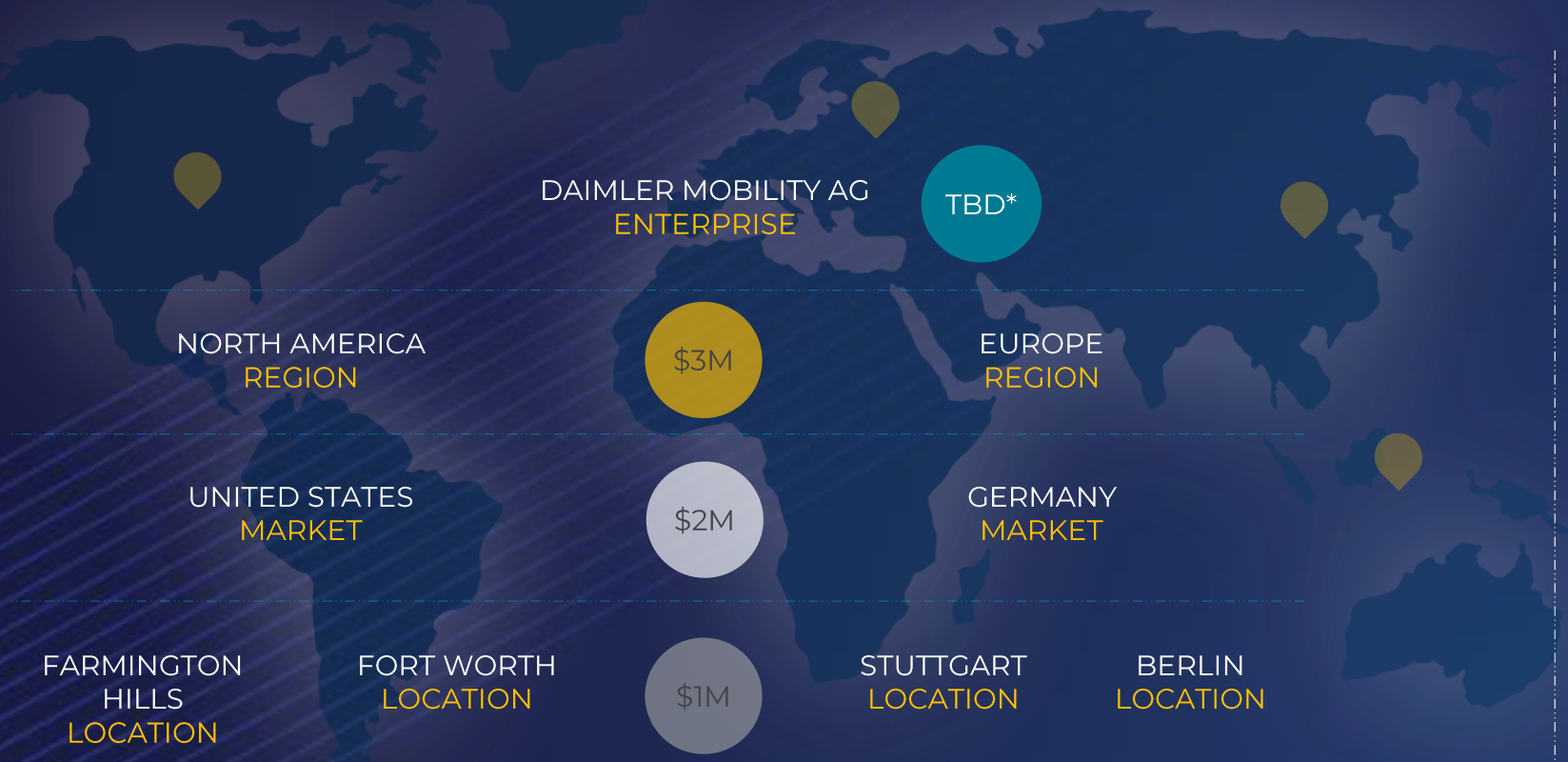
INDIA SUTTON
Global Cyber-Risk Management Specialist

Daimler Mobility CyberSecurity

FAIR CONFERENCE 2019

PART 4: THE OUTCOME

A GLOBAL VIEW OF CYBER RISK



ACCOMPLISHMENTS

100%
Reallocated budgeted investment in third-party risk

25%
Reorganized risk reducing projects

15%
Consolidated remediation plans

DAYS TO HOURS
Reduced risk analysis time to completion for faster path to transparency

CRQ RESULTED IN A RIGHT-SIZED BUDGET, PROJECT PLAN AND RISK REGISTER

#FAIRCON19