Operationalizing Risk Quantification into Enterprise Risk Management

Expedia Group + IBM

Krishna Sheshabhattar & Randy Spusta

FAIR22 CONFERENCE

Introductions

Randy Spusta
Global Competency Leader – Security Strategy
IBM

Krishna Sheshabhattar
Director, Security GRC
Expedia Group

FAIR22 CONFERENCE

Abstract

This session will look at how Expedia Group adopted FAIR methodology and framework to build the foundational risk quantification capability designed from the beginning to be applied across various functional areas.

We will also share how Expedia leverages FAIR to scale risk management from just being a security risk related construct to Enterprise Risk Management.

FAIR22 CONFERENCE

Expedia®

WE BELIEVE TRAVEL IS A FORCE FOR GOOD

Our mission is to power global travel for everyone, everywhere

FAIR22 CONFERENCE

Expedia Landscape

THE POWER OF OUR PLATFORM

REACHING THE WORLD THROUGH GLOBAL DISTRIBUTION

20+

Globally relevant brands

200+

Travel sites

70+

Countries

TECHNOLOGY

600b+

AI Predictions

29M+

Virtual Conversations

70PB+

Data

BROADEST OFFERING IN THE TRAVEL INDUSTRY

3M+

Properties

220K+

Unique Activities

500+

Airlines, dozens of cruise lines and thousands of car rentals

FAIR22 CONFERENCE

Expedia Risk Program Goals

Establish a quantitative approach that accelerates the ability to effectively manage risk by:

- Adopting standardization of a common risk management language
- Integrating Risk Management with Business Operations
- Aligning an integrated view of top risks among executive suite
- Implementing a strategic approach to risk management

Risk Management Objectives

1. Move from reactive to proactive risk management
Step from the tactical and operational view of risk management to a strategic view

2. Understand top threats, their probability of occurrence and their likely frequency
Measuring risk requires an understanding of likelihood of occurrence

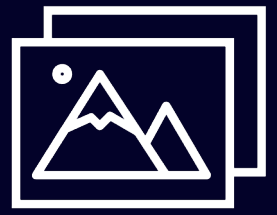
3. Identify and focus on the true value of your assets
Threats target assets, know your crown jewels

4. Understand the impact of risks based on expected loss and business operations
Quantify in dollars and cents, operational disruptions and impact to the business

5. Determine risk reduction remediation projects based on a cost/ benefit methodology
Analyze and compare various risk remediation options based on costs and expected risk reduction

FAIR22 CONFERENCE

Challenges



Framing with Scenarios

- Connectivity & COVID Implications
- Patching for Latest Vulnerabilities
- Technology Adoption Issues

Describing The Problem

- Distributed & Not Scalable
- Misaligned, Disaggregated
- Short Term & Tactical focus not driving Investment Decisions & Roadmap Prioritization

Why Does It Matter?

- Centralized Risk Universe
- Shift from Tactical to Strategic
- Roadmap to Certifications (SOC2 / ISO etc)
- Getting closer to Enterprise Risk Management

FAIR22 CONFERENCE

Solution

WHAT: A Risk-Based Approach for Security	WHY: This Matters	HOW: This Benefits Expedia Group
• We want to put the business lens in cyber events & reimage the way we look at risk • Risk Quantification helps bridge the communication gap between the business and security teams by speaking a common language	• Risk Quantification via the FAIR Methodology enables us to analyze and quantify cyber risk in financial terms • Data collected and reports generated will empower top-down decision making in all business units around Expedia Group	• We want to empower EG to make better risk-based decisions • We can create a clear understanding of the business impacts associated with incidents for bolstered planning and preparation • We can gain insight into how to best protect our brand and reputation

Benefits

Immediate Benefits

- Inspired **cultural change** by educating on FAIR & providing **POC use cases**
- Established Expedia **target operating model** & process documentation
- Demonstrated how FAIR terminology can **clarify risk** & **scope** countable loss events
- Proved that **FAIR risk analysis can help better-inform decisions**
- Conducted **risk register normalization** exercise to catalyze change

Downstream Benefits

- Scalability and capability to **bring RQ to other Expedia verticals**(Compliance, Threat Intel, BCPDR, Etc.)
- Implementing what we have built that leads toward risk acceptance structure
- Continue to **unlock the value of security**

Expedia Use Cases - 1

Creating Leadership & End-User Awareness Around Benefits of a Compliance Program (Cost/Benefit Analysis)

Annualized Scenario Results

Minimum	10th Percentile	Average	Most Likely	90th Percentile	Maximum
$455.7K	$1.6M	$6.8M	$2.4M	$11.2M	$453.6M

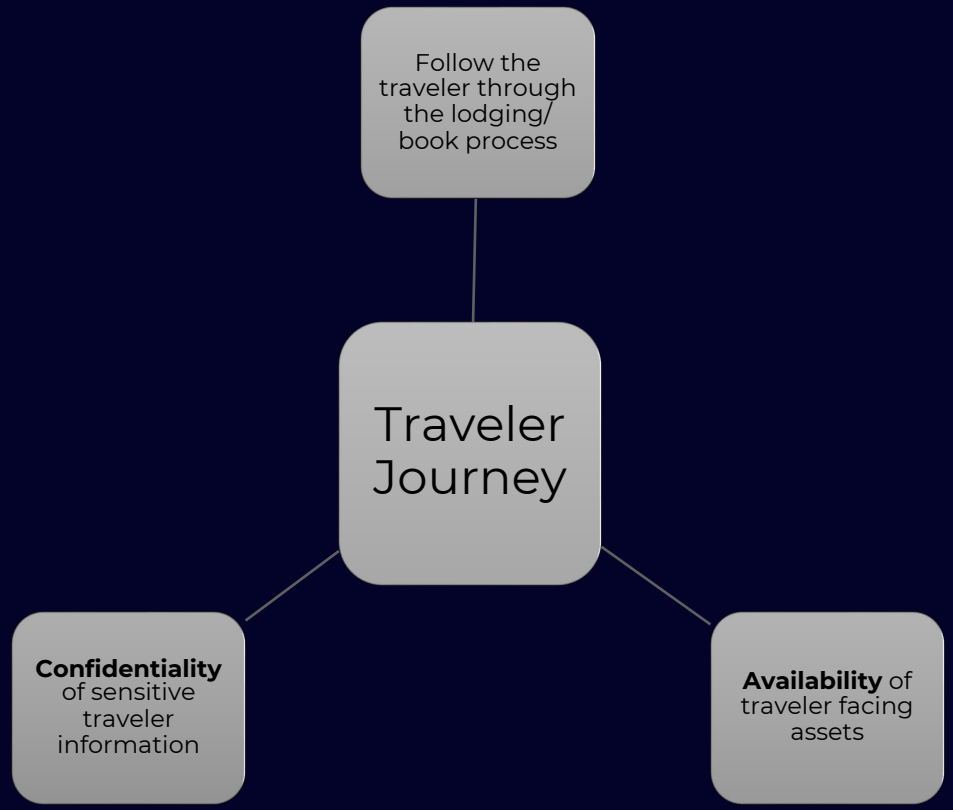
Remediation Effort	Change in Cost	Most Likely ROI Per $1 Spent	90th Percentile ROI Per $1 Spent	Maximum ROI Per $1 Spent
MAX Hours	$1M Increase	$2.31	$11	$439
ML Hours	$326.6K Increase	$7.32	$34	$1.4K
MIN Hours	$12.6K Increase	$189.11	$884	$25.9K
Change in Risk Exposure		-$2.4M	-$11.2M	-$453.6M

FAIR22 CONFERENCE

Expedia Use Cases - 2

Traveler Booking Journey – Cyber Risks as Business Risks

Scoping Scenario



Expedia Use Cases - 2 (Continued...)

Traveler Booking Journey – Cyber Risks as Business Risks

Key Results – Key Web Site abc.com Misconfiguration Outage

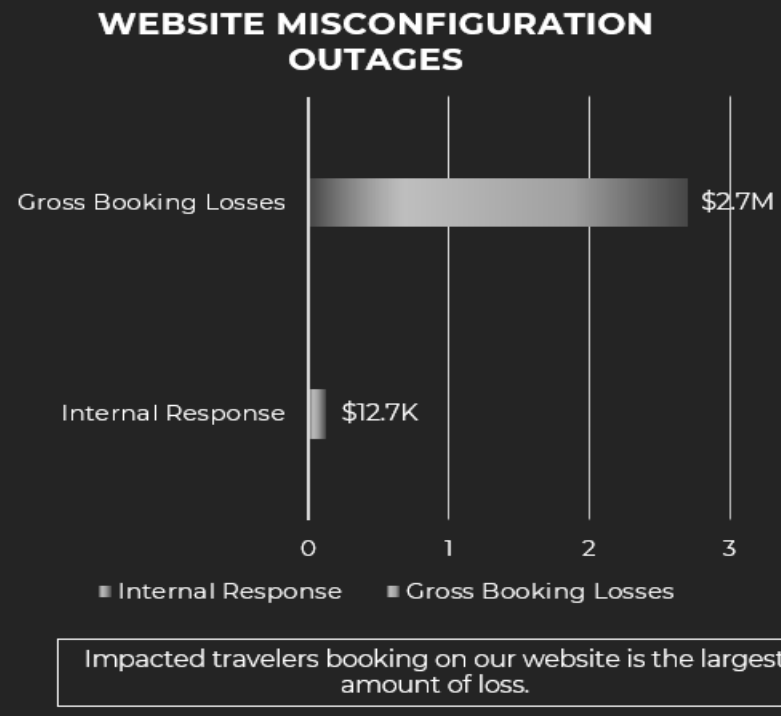
2
Loss events forecasted per year
100% forecasted within a year

$2.7M
Average Per Event Loss
Non-annualized, assumes secondary losses

$4.7M
Average Annualized Loss Exposure

84%
Probability of exceeding $1M threshold every 1.2 years

Forms Of Loss Breakdown



Impacted travelers booking on our website is the largest amount of loss.

FAIR22 CONFERENCE

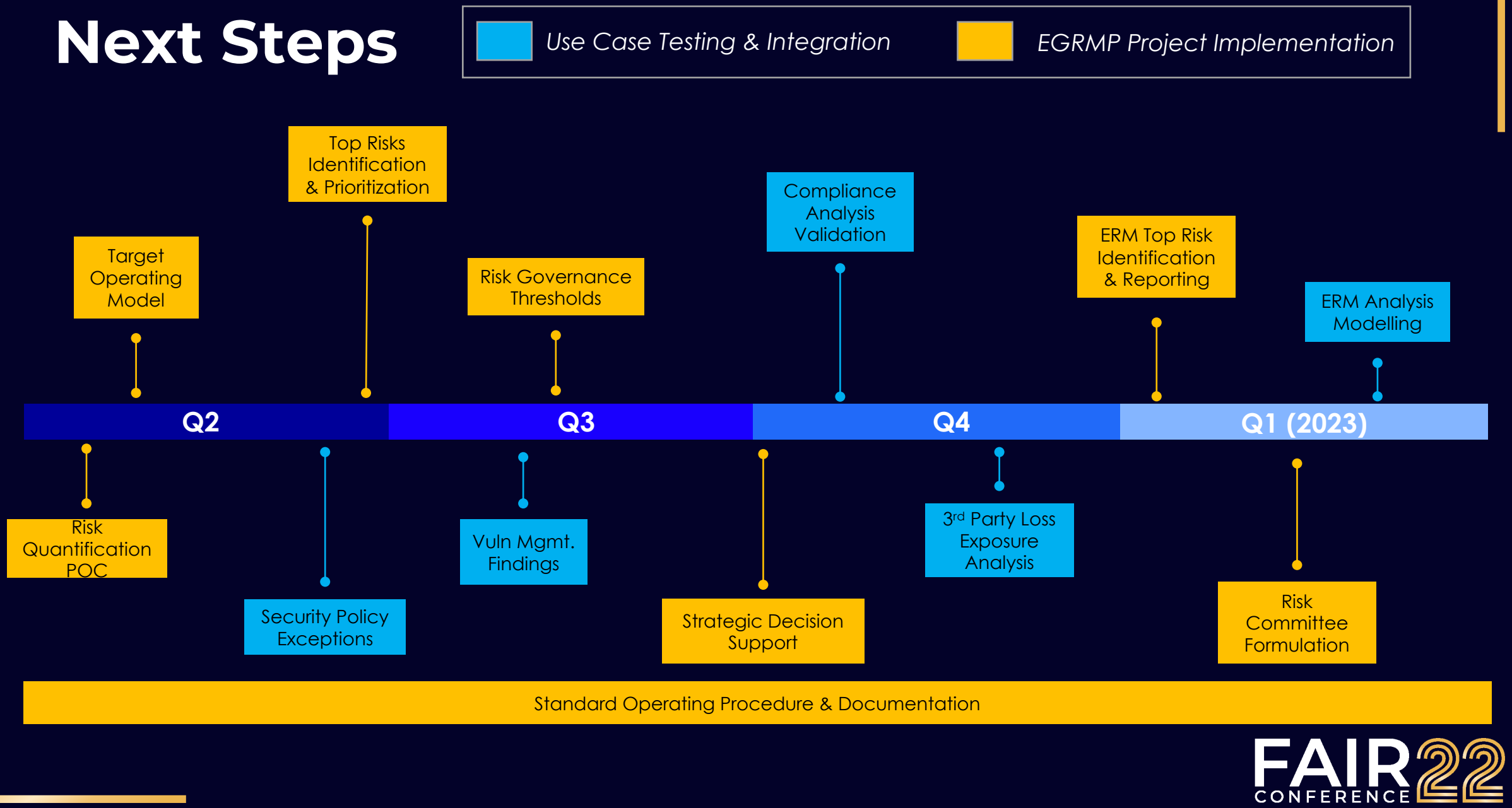
Learnings from Use Cases & POC Work

- Leadership understanding of compliance threat landscape
- Grasp on compliance importance and creating awareness
- Decision making capabilities

Overall, We Learned the following – Using FAIR We CAN

RAISE AWARENESS about technology, digital & security risks, INFLUENCE THE BEHAVIORS of our people, and FOSTER A CULTURE OF SECURITY, COMPLIANCE AND PRIVACY throughout Expedia Group.

Next Steps



FAIR22 CONFERENCE

Questions

FAIR22 CONFERENCE


IBM
Expedia
Thank You
IBM