FAIR Cyber Risk Scenario Taxonomy (FAIR-CRS™)

Introductions

Cody Scott
Senior Analyst, Security & Risk
Forrester

Pankaj Goyal
Director, Research & Standards
FAIR Institute

Todd Tucker
Managing Director
FAIR Institute

FAIR Is Evolving

FAIR Model

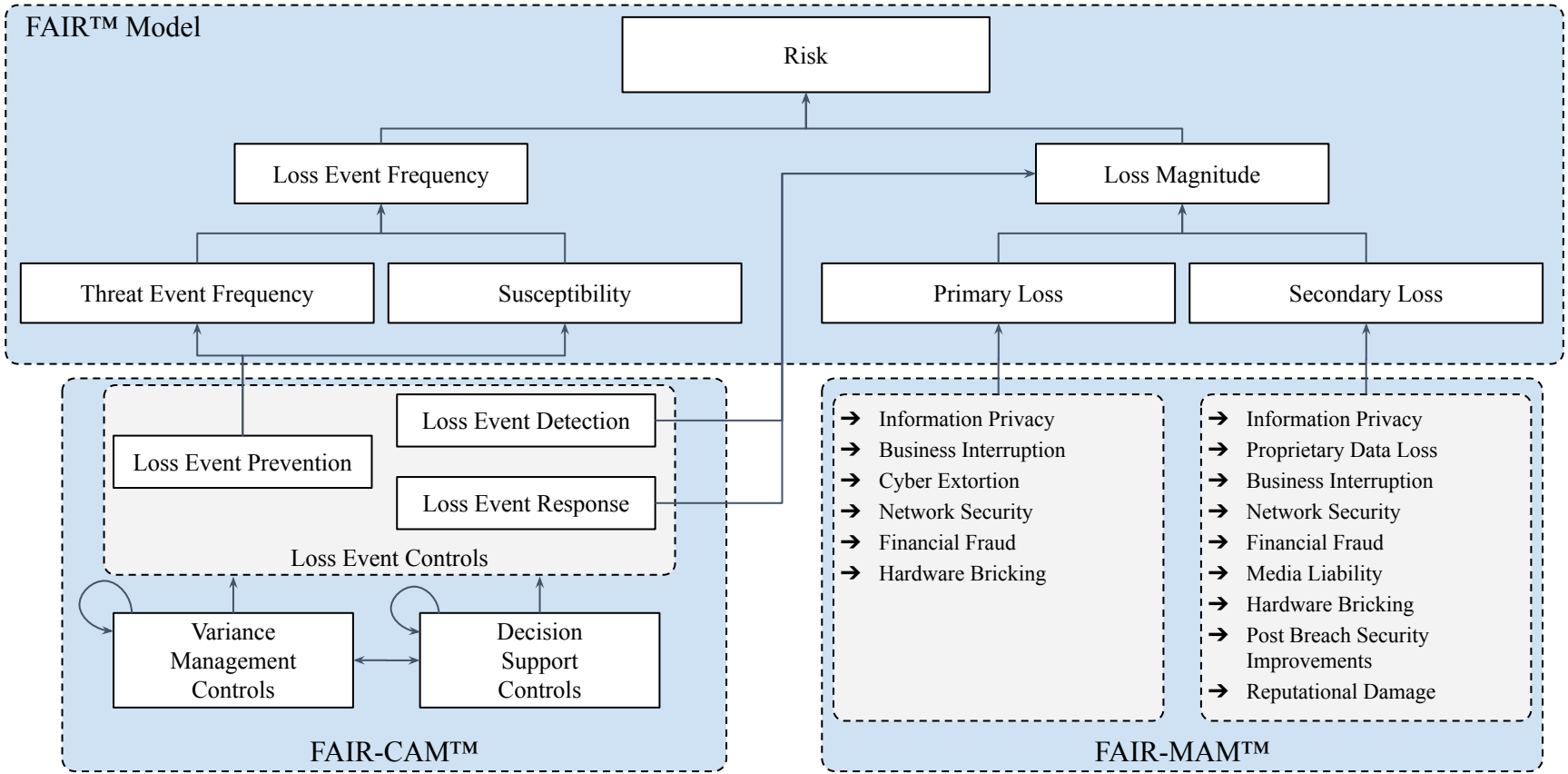
Cyber risk
quantification model

Enables standard definitions of risk and risk measurement

Limitations:

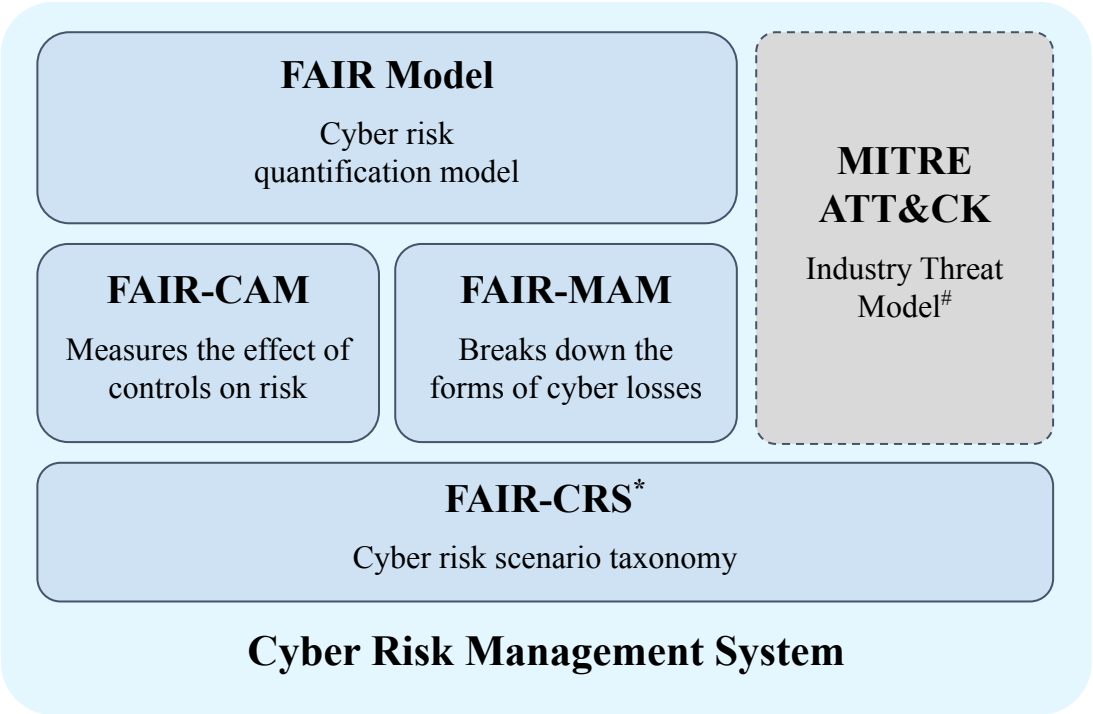
- No direct mapping to controls effectiveness
- Heavy reliance on calibrated SME inputs
- Perceived as not scalable
- Loss categories (6 forms of loss) too high-level

Expanding the FAIR Model



A Broader Standards Framework

Supports Quantification, Data Integration, Centralization



Expanded framework to:

- Support an objective, data-driven approach
- Enable continuous risk monitoring
- Implement a consistent, centralized model

* Proposed standard (draft)

Third-party model; framework allows for other threat intel models/sources

Cyber Risk Scenario Definitions

Problems with Many Risk Registers

- **Incorrectly Defined Risk Scenarios**: Scenarios lack specificity and fail to reflect real-world situations, hindering their applicability to actual risk assessments.
- **Irrelevant Risk Scenarios**: Scenarios focus on hypothetical or low-impact risks, diverting attention from more critical threats and potential losses.
- **Excessive Number of Risk Scenarios**: Overloading the risk register with too many scenarios creates unnecessary complexity and impedes actionable insights.
- **Poorly Measured Risk Scenarios**: Scenarios lack effective quantification of potential impact and likelihood, making it difficult to prioritize risks and allocate resources appropriately.

Cyber Risk Scenario - if Correctly Defined

- **Informed Decision-Making:** Clear risk scenarios enable organizations to make data-driven decisions regarding resource allocation, security investments, and risk mitigation strategies.
- **Strategic Resource Allocation:** By understanding the potential impact and likelihood of various risks, organizations can allocate resources effectively to address the most critical threats.
- **Enhanced Risk Posture:** Well-defined risk scenarios facilitate proactive risk management, enabling organizations to identify and address vulnerabilities before they are exploited.
- **Improved Communication:** A clear and structured risk register fosters better communication and collaboration among stakeholders, ensuring everyone understands the organization's risk landscape.

Cyber Risk Scenarios

Defining Elements

From whom/what are you protecting?	What are you protecting?	Which threat behavior concerns you?	What type of losses could materialize?
[Threat]	**[Asset]**	**[Method]**	**[Effect]**

“[Threat] impacts the [loss] of [asset] via [method].”

Example:

“**State-sponsored hacking group** impacts the **availability** of **our patient records** via a **ransomware attack**.”

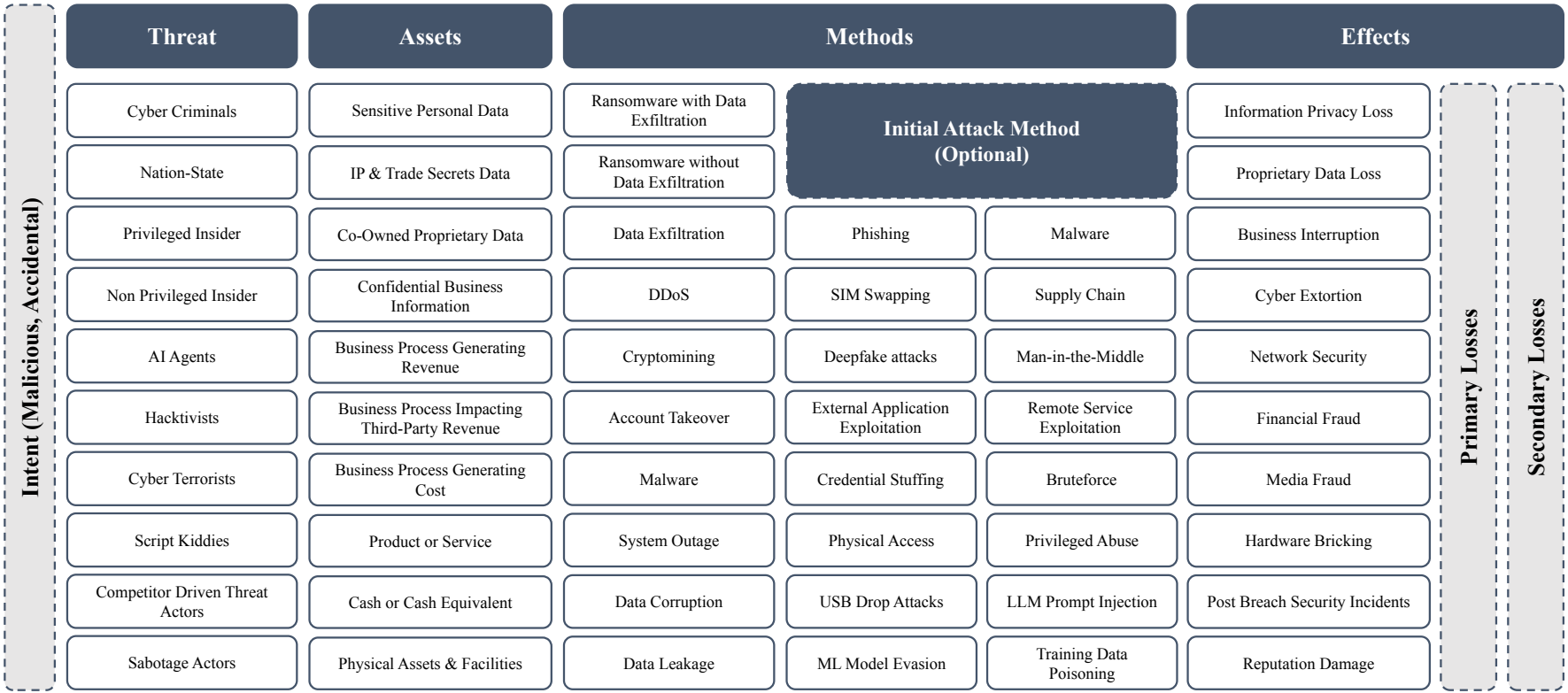
Ineffective vs. effective Risk Scenarios

Ineffective	Effective
“Phishing is a big risk to our organization.”	“Cybercriminals impact company funds (cash and cash equivalents) via a phishing-based business email compromise (account takeover), causing a direct financial loss (financial fraud).”
“Data breaches are a major concern.”	“A disgruntled employee (privileged insider) impacts proprietary research and trade secrets (intellectual property) via unauthorized file transfers (data exfiltration without ransomware), causing a competitive disadvantage and loss of future revenue (proprietary data loss).”
“We might get hit by ransomware.”	“A ransomware gang (cyber criminals) impacts customer billing and payment processing (business process generating revenue) via encryption malware and extortion (ransomware with data exfiltration), causing service downtime and ransom payment demands (business interruption and cyber extortion).”

Follow ups

- How many scenarios do I need?
- How do I identify the “right” scenarios?
- How specific does the scenario need to be?
- How do I find the right data for my analysis?
- How do I know if my data/estimates are accurate?

FAIR-CRS: Cyber Risk Scenario Taxonomy



FAIR-CRS: Cyber Risk Scenario Taxonomy

Includes proposed revisions for FAIR-CRS standard v1.0

Intent (Malicious, Accidental)

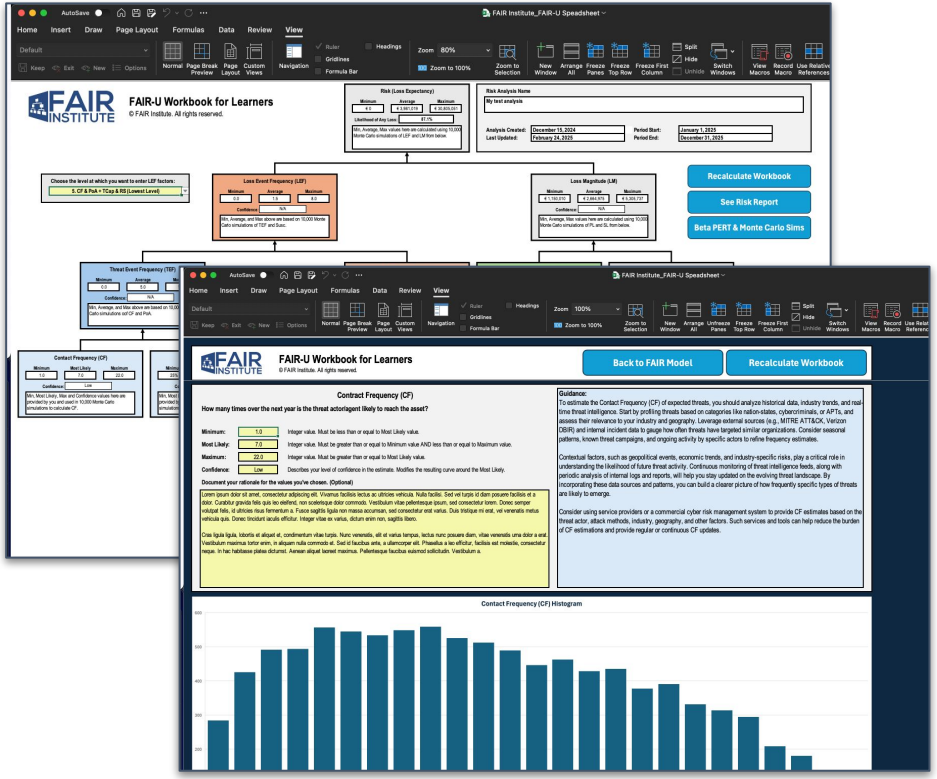
Threat	Assets	Methods			Effects	
			Initial Attack Method (Optional)			
Cybercriminals	Sensitive Personal Data	Ransomware with Data Exfiltration			Information Privacy Loss	Primary Losses
Nation-State Actors	IP & Trade Secrets Data	Ransomware without Data Exfiltration			Proprietary Data Loss	
Privileged Insiders	Co-Owned Proprietary Data	Data Exfiltration	Phishing	Malware	Business Interruption	
Non-Privileged Insiders	Confidential Business Information	DDoS	SIM Swapping	Supply Chain	Cyber Extortion	
AI Agents	Business Process Generating Revenue	Cryptomining	Deepfake Attack	Man-in-the-Middle	Network Security	
Hacktivists	Business Process Impacting Third-Party Revenue	Account Takeover	External Application Exploitation	Remote Service Exploitation	Financial Fraud	
Cyberterrorists	Business Process Generating Cost	Malware	Credential Stuffing	Bruteforce	Media Fraud	
Script Kiddies	Product or Service	System Outage	Physical Access	Privileged Abuse	Hardware Bricking	
Competitors (Corporate Espionage)	Cash or Cash Equivalent	Data Corruption	USB Drop Attacks	LLM Prompt Injection	Post Breach Security Incidents	
Disgruntled Employees (Saboteur)	Physical Assets & Facilities	Data Leakage	ML Model Evasion	Training Data Poisoning	Reputation Damage	Secondary Losses

Q&A / Wrap-Up

FAIR-U

Member Resources to Learn FAIR

- ➔ FAIR-U Workbook for Learners
  - ◆ Releasing in next few days
  - ◆ Similar functionality to original FAIR-U
- ➔ FAIR-U for Cyber
  - ◆ Shows enterprise-class CRMS
  - ◆ Based on SAFE One platform



2025 FAIR Conference

November 4-5 | The Glasshouse | New York, NY

Resetting Cyber Risk in the Age of AI

- ➔ The two-day global conference will bring together **CISOs, CIOs, and cyber risk experts** to meet on the rapid evolution in cyber risk management.
- ➔ **Key topics will include:**
  - Aligning cybersecurity investments to business risk
  - Managing AI risk and using AI to manage risk
  - Ensuring cyber resilience and managing third-party risk
  - Cyber risk management as a scalable system
- ➔ **November 2-3: Brand new *FAIR Foundations* and *FAIR Cyber Risk Analysis Training* courses**
- ➔ **Learn more / register: http://www.fairinstitute.org/faircon**

FAIRCON25 on November 4-5, 2025

Super Early Bird Registration

FAIRCON is coming to New York City!
Spectacular Venue @ The Glasshouse

GENERAL MEMBERS

$1,795

$1,995 AFTER JUNE 30, 2025
$2,495 AFTER AUGUST 31, 2025

SAVE $200 BY FIRST UPGRADING TO CONTRIBUTING MEMBERSHIP FOR JUST $150.

CONTRIBUTING MEMBERS

$1,595

$1,795 AFTER JUNE 30, 2025
$2,295 AFTER AUGUST 31, 2025

SAVE $200 BY FIRST UPGRADING TO CONTRIBUTING MEMBERSHIP FOR JUST $150.

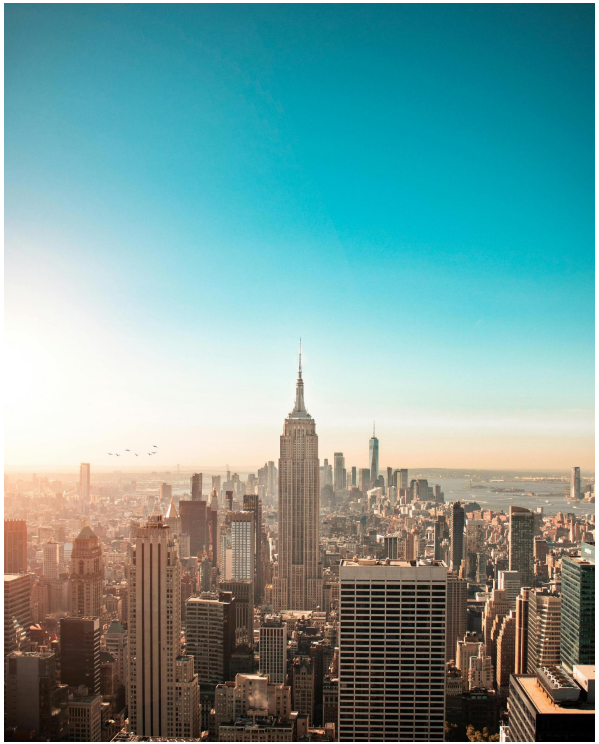
NON-MEMBERS

$3,995

FOR CONSULTANTS AND SOLUTION PROVIDERS WHO ARE NOT SPONSORS OF THE FAIR INSTITUTE.

ALL PACKAGES INCLUDE

- All Keynotes & Breakout Sessions
- Access to the Expo Hall
- Breakfast & Lunch — Tuesday / Wednesday
- Gala and Awards Dinner — Tuesday



www.fairconference.org