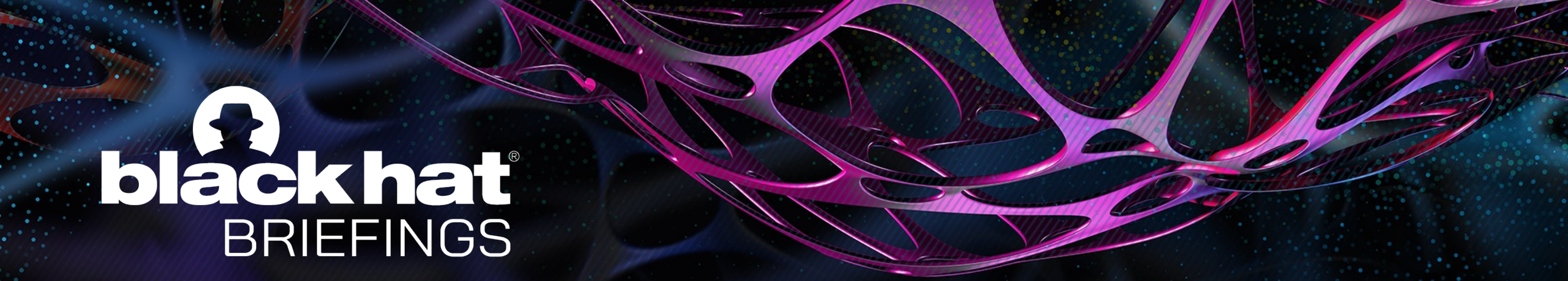


AUGUST 6-7, 2025

MANDALAY BAY / LAS VEGAS

Digital Dominoes: Scanning the Internet to Expose Systemic Cyber Risk

Morgan Hervé-Mignucci

Morgan Hervé-Mignucci PhD, CFA, CISSP

- Lead **Cyber Catastrophe Modeling** at Coalition, Inc.
- Pioneered cyber risk models adopted by global insurers & reinsurers
- Previously featured in Financial Times / New York Times for research on systemic infrastructure & climate risk

3 Large-scale Cyber Events in 2024

CHANGE HEALTHCARE

CDK GLOBAL

CROWDSTRIKE

Cyber Catastrophe Risk (CAT)

- Insurance-specific
- Portfolio losses quantification
- Commercial CAT models
- **Risk Management**: underwriting, coverage, capitalization, reinsurance

≠

Systemic Cyber Risk (SCR)

- Broader than insurance
- Economy- / industry-wide impact
- Ad hoc impact assessment
- **Interventions**: public policy, regulation, public-private sector collaboration

Same Root Cause

Accelerated Interconnectedness in our Increasingly Digital Economies

Dissecting Past Cyber Events

Categorizing Landmark Cyber Events

Supply Chain Compromise

3rd party access vector
Software update vector

Direct Targeted Attacks

Nation-State Operations
Destructive Attacks
Ransomware Operations

Shared Technology Vulnerabilities

Protocol Vulnerabilities
OSS Dependencies
Platform Vulnerabilities

Trusted Security Tool Failures

Security Tool

(More or Less) Common Cyber Insurance Levers

From “Silent Cyber” to Affirmative Cyber

Coverage Expansion & Exclusion

Sub-Limits Introduction

Premium Adjustment

Underwriting Scrutiny + Formal Controls

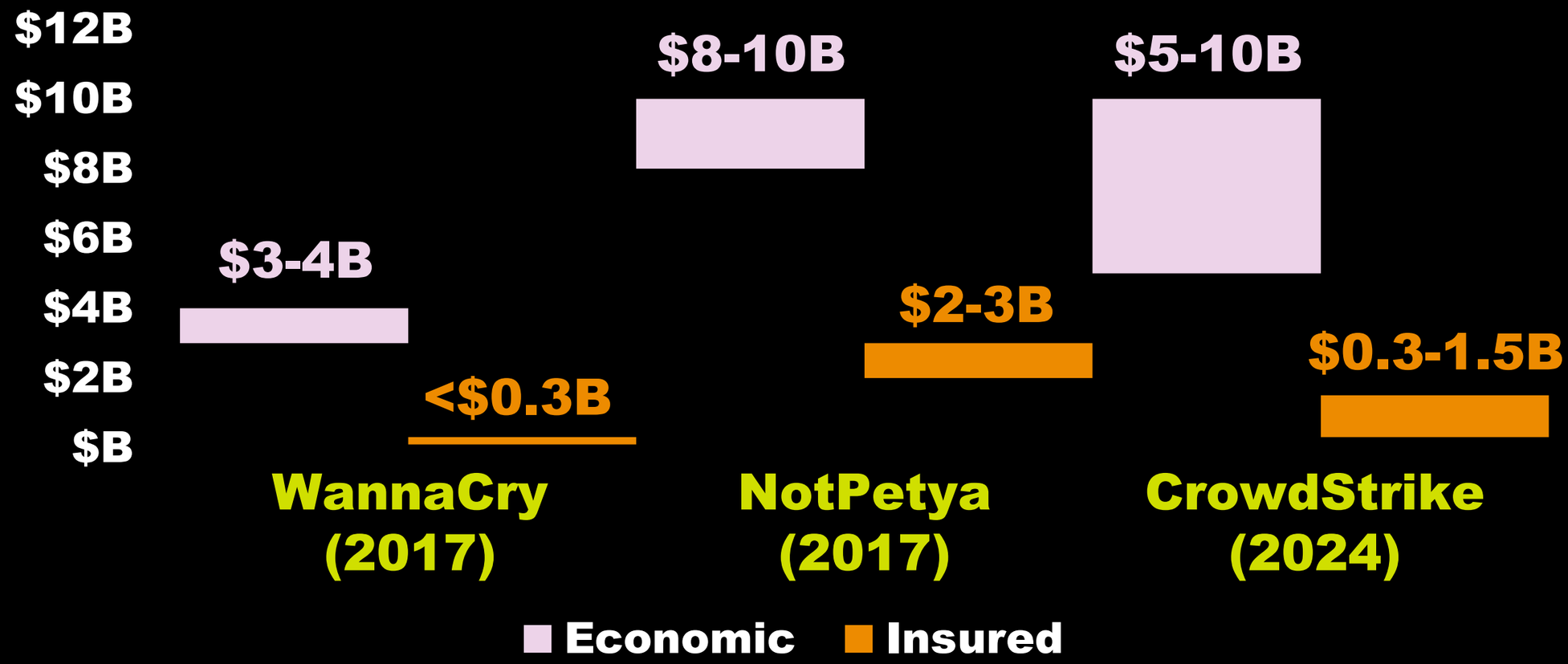
More Robust Data Collection

Reinsurance / Risk Capital

Major Public Policy / Regulator Response

Public Reporting	Best Practice / Guidance / Advisory	Attribution / Coordinate / “Fix”	Charges / Fines / Sanctions
Supply Chain Visibility	Critical Infrastructure	Finance & Insurance	

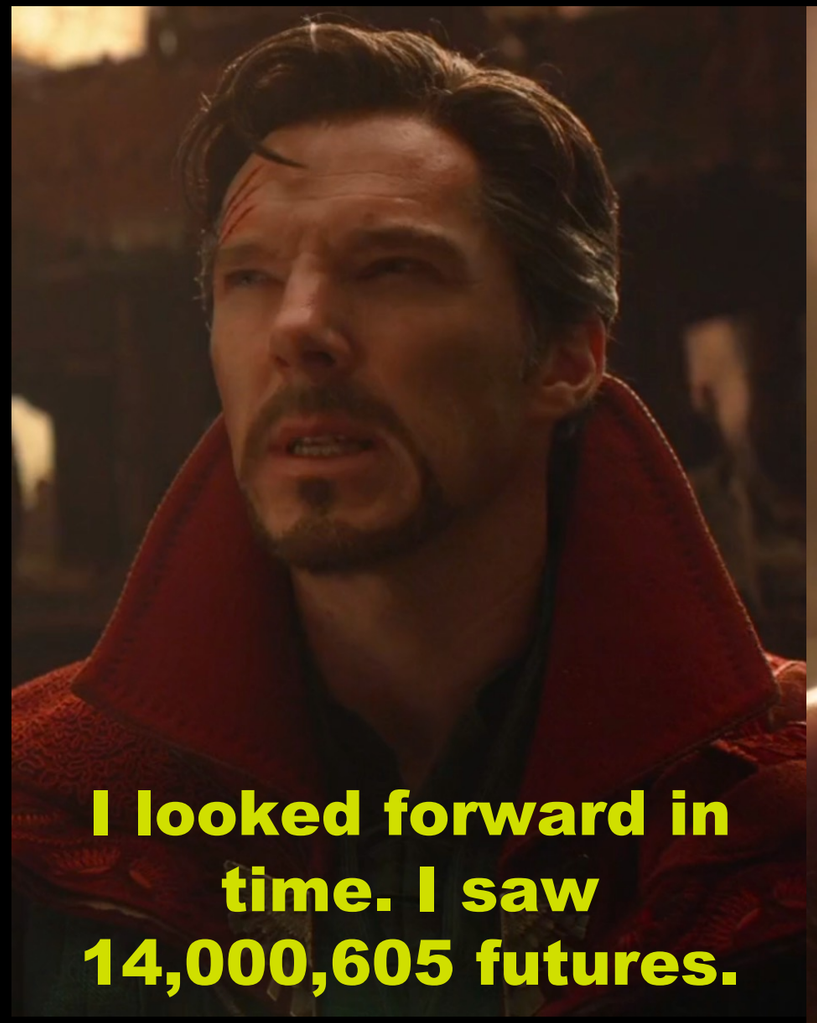
Loss Estimates from Past Cyber Events



black hat BRIEFINGS

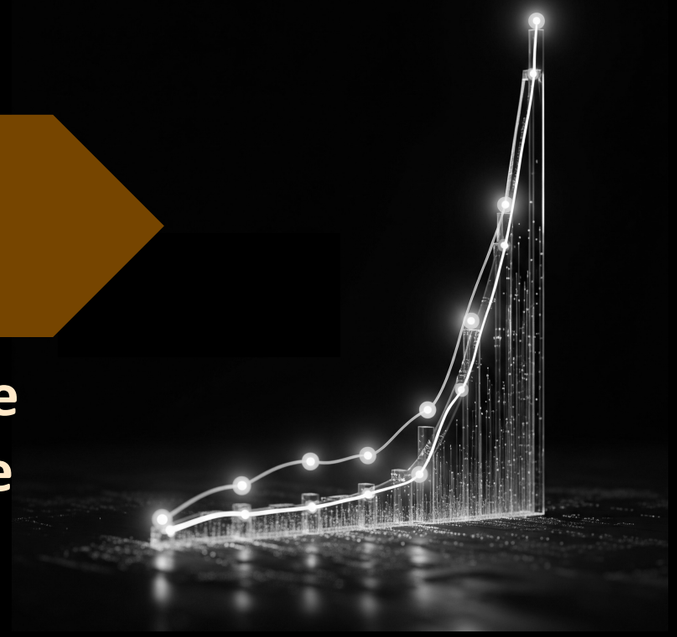
Modeling What Matters in Systemic Cyber Risk

What is Cyber Catastrophe Risk Modeling?



Insurance Catastrophe Modeling 101

1. Event Set
2. Hazard Footprint
3. Exposure (assets, orgs)
4. Vulnerability / Severity
5. Insurance Coverage



Great fit for insurance / reinsurance risk quantification & management use cases

… But CAT Models suboptimal for SCR

Misaligned Modeling Paradigm

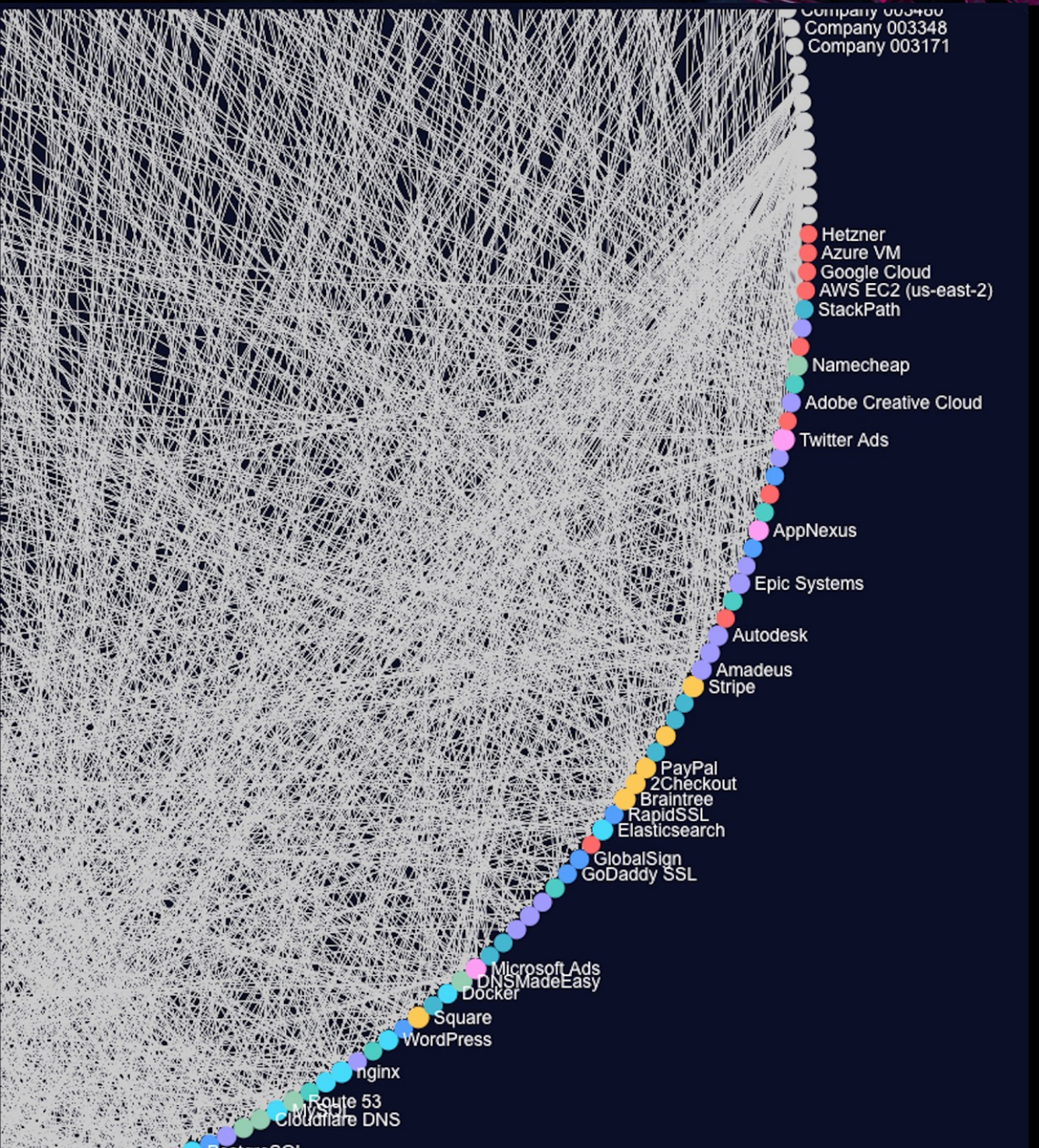
- Static “Nat Cat” approach is a poor fit for dynamic **SCR**

Data Issues

- Models unvalidated by a true catastrophe precedent
- Non-insured organizations are out of scope

Vendor Inertia & Flawed Anchoring

- Vendor models initially overstated risk
- Business inertia prevents necessary model updates



Data-Driven SCR Modeling

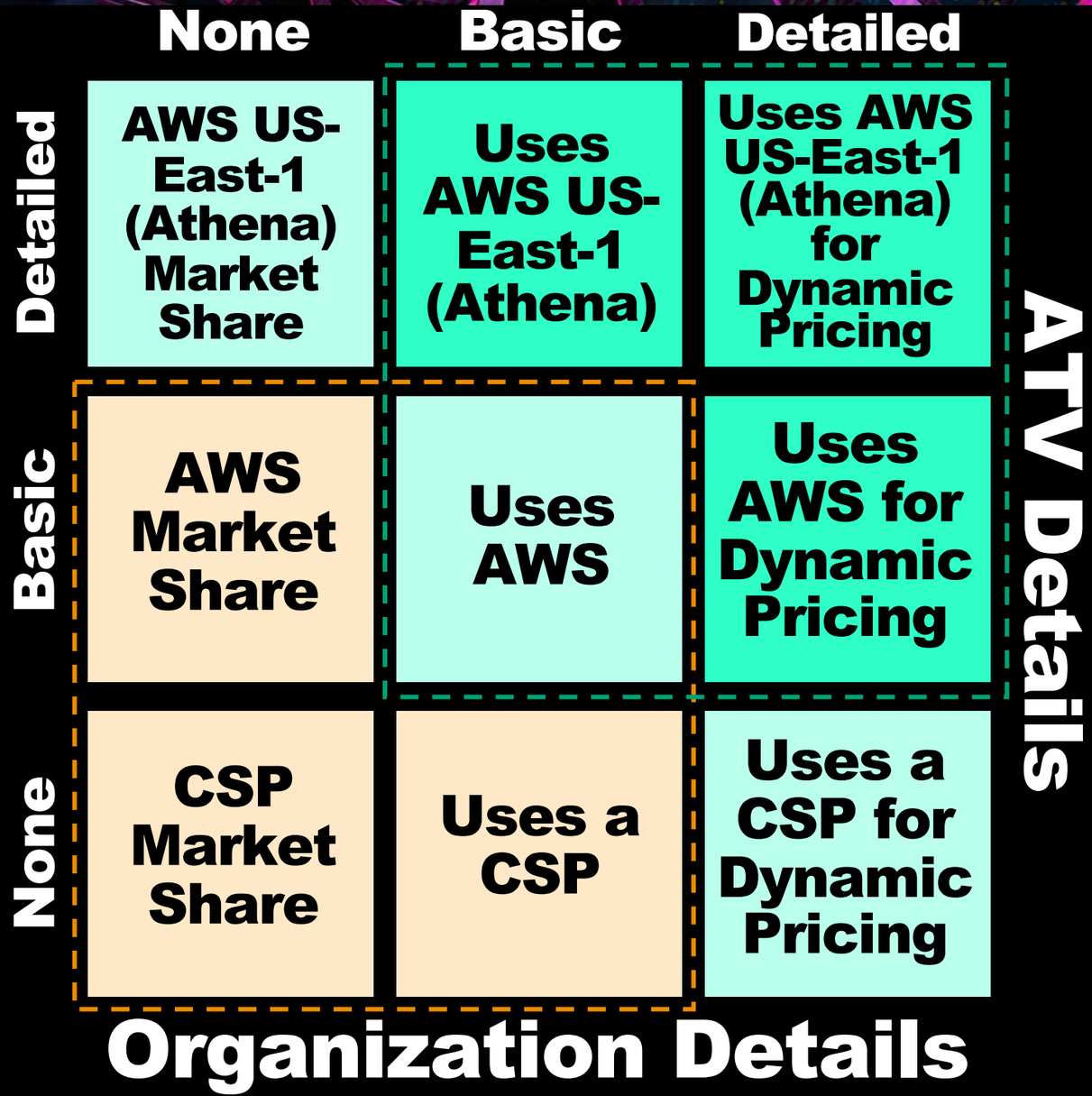
SCR is best represented as a Massive Graph

- Leverage Coalition's data to curate **Aggregation Technologies & Vendors (ATV)** datasets

Focus on what is Known (i.e., public-facing internet)

CAT Typical Level of Detail

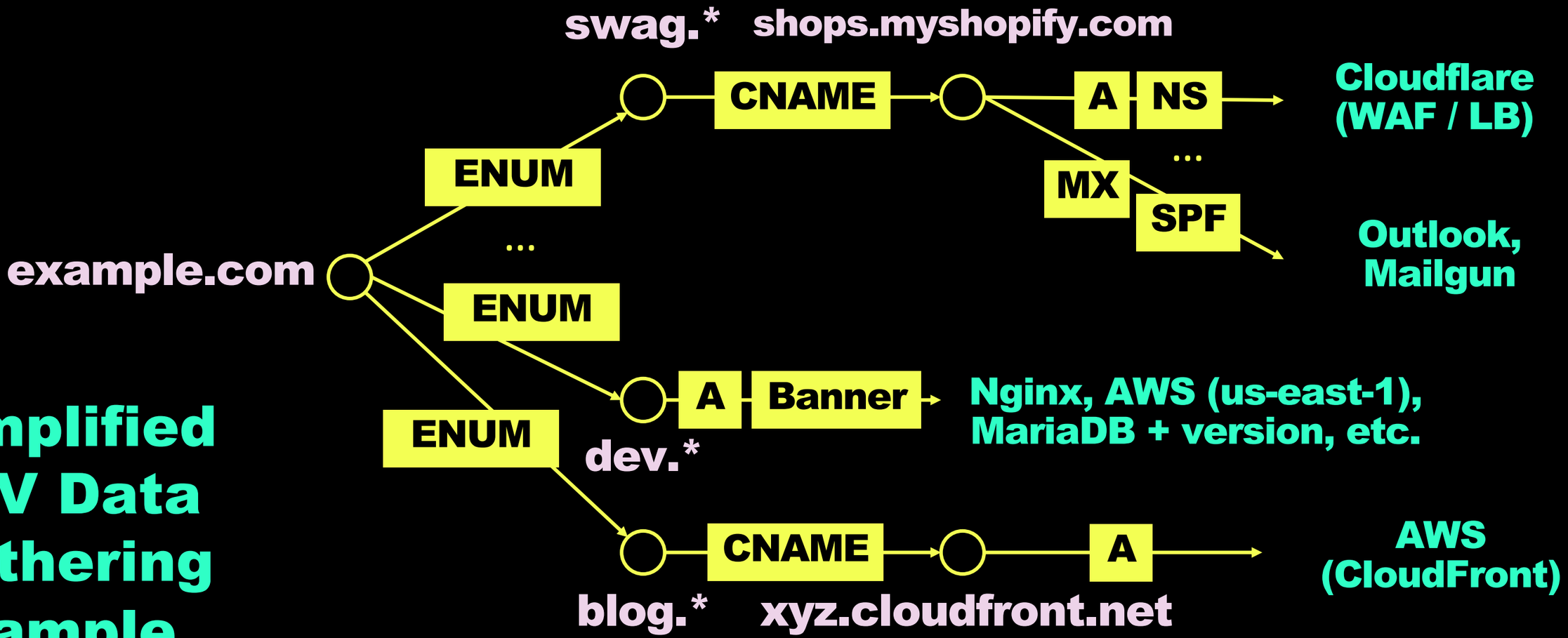
- Overestimate Concentration & Losses
- Limited / Flawed Insights



SCR Target Level of Detail

- More Credible Losses
- Nuanced understanding of **SCR**

Identifying Aggregation Technologies & Vendors



Simplified ATV Data Gathering Example

Industry / Segment Deep Dives

Inc. 5000 Firms

5K
US Orgs.

200%+
Growth

1.4M
Headcount

~5K
Unique Domains

$317B
Revenue

Systemic Cyber Risk is Cross-Sectoral

DEMO #1 – Most leading ATVs can be found in multiple, sometimes unrelated, industries

Registered Investment Advisory Firms

22K
Firms

$145T
AUM

1M+
Headcount

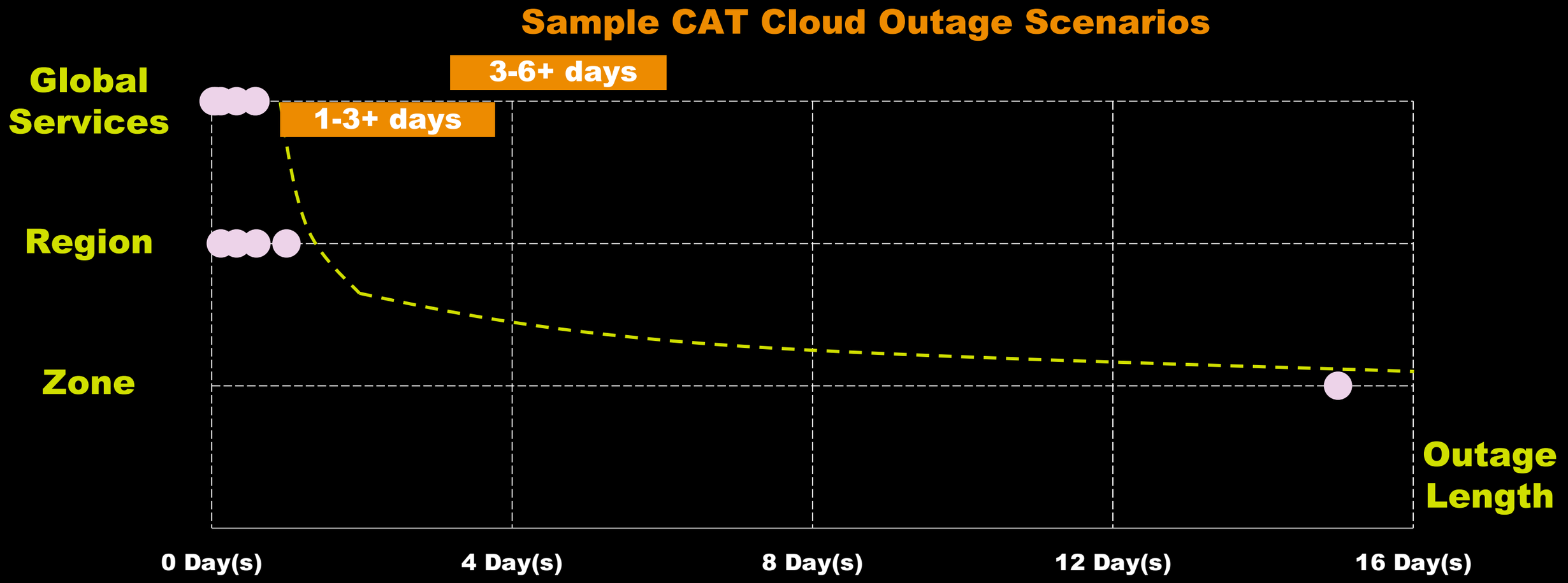
18K+
Unique Domains

60M+
Clients

Cloud Outage Risk More Nuanced Than Claimed

DEMO #2 - A more nuanced data-driven understanding of cloud architecture generates more credible cloud outage loss estimates

Multiple Levels of Cloud Outage Risk



Scope: longest AWS, GCP, and Azure outages over 2020-2025

US Real Estate Agencies (CT)

20+K
Agents

2.5+K
Agencies

~2K
Unique
Domains

Aggregation via SaaS & Franchisor IT

DEMO #3 – Most industries have industry-specific ATVs around which organizations tend to be clustered

Identifying High-SCR Technologies & Vendors

All ATVs from 2024 SCR events were named in an antitrust proceeding

NSS Labs, Inc. v. ***CrowdStrike, Inc.*** *et al, (N.D. Cal. 2020)*

U.S.A. v. UnitedHealth Group & ***Change Healthcare*** *(D.D.C. 2022)*

In re Dealer Management Systems Antitrust Litigation (N.D. Ill. 2024) – including ***CDK Global, LLC***

A Glimpse of More to Find in FTC Data

Mortgage / Real Estate
- Origination
- Marketplaces
- Bulk data

Finance
- Software / API

Healthcare
- Bulk Data
- EHR / CRM

Implications & Recommendations

For Policymakers

Shift to a Proactive, Data-driven Approach to SCR Policymaking

Expand Definition of "Critical Infrastructure"

- Focus on Systematically Important Technologies (i.e., **ATVs**), not just sectors

Mandate & Incentivize Measurable Resilience

- Mandate Supply Chain Visibility for organizations utilizing designated critical **ATVs**
- Incentivize resilience through market mechanisms like cyber insurance

Leverage Dependency Data to Guide Antitrust and Regulation

For Risk Owners / CISOs

Cannot Prevent SCR -> Build Resilient Organization

Resilience & Supply Chain Security

- Nth-party **ATVs**
- Architecture
- TPRM / SBOM

Vulnerability & Exposure Management

- Real-Time Inventory
- Continuous ASM
- Emergency Patching

Containment & Operational Recovery

- Zero-Trust
- Immutable Backups
- IR Playbooks

Governance & Crisis Management

- (Real) Tabletop
- CRQ
- Cyber Insurance
- Out-of-Band

For Risk Modelers

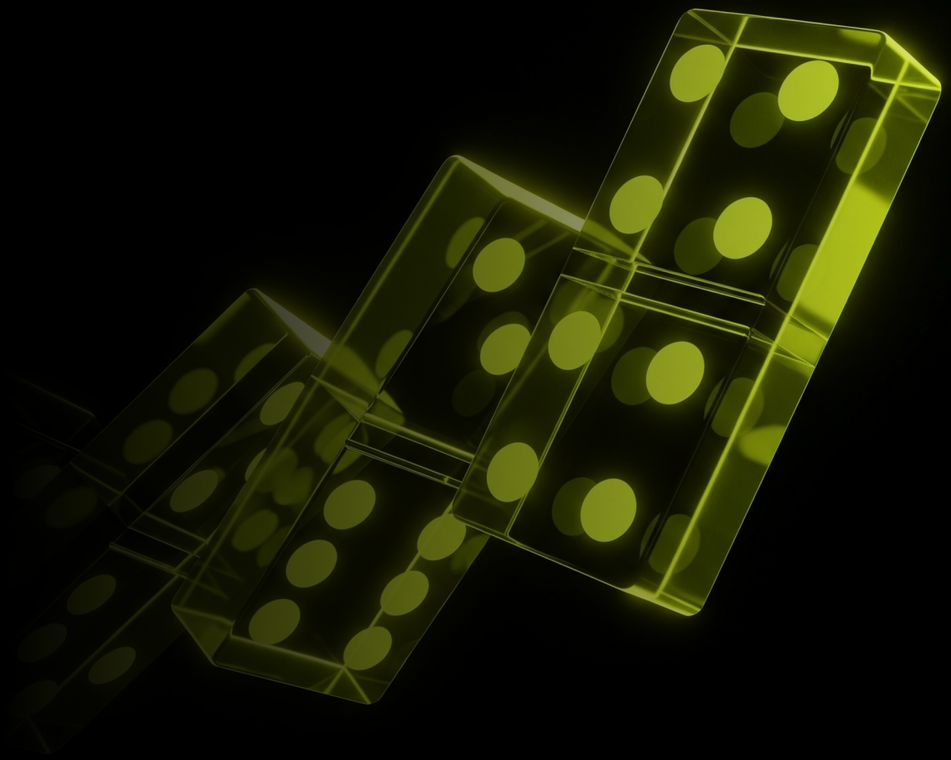
Prioritize Data-Driven Modeling of Economic Losses

- Embrace Granular **ATV** Usage & Detection Data
- Gold Standard -> Modeled Loss Traceability
- Else GIGO for Insured Losses

About Catastrophic Scenarios

- Stress Testing ≠ Systematic FUD
- Anchor Event Catalogs & Assumptions in Updated Data

Next Steps



Addressing Limitations

Known Unknowns:

- WAFs / VPCs / Internal Networks / Clients
- Non-Digital Vendor Relationships

Unknown Unknowns:

- Unnoticed OSS / Components

Even Better Data Quality:

- Discovery / Enumeration / Attribution
- Richer Context & Asset Classification

Black Hat Sound Bytes

- Systemic Cyber Risk is a "**Too Connected to Fail**" reality, driven by the deep interconnectedness of our digital economies
- We must shift from static, theoretical catastrophe models to a **dynamic, data-driven approach** that maps the Internet's true dependencies
- For Risk Owners, the goal is **not prevention but resilience**; you must understand your risk through the lens of shared technology and your n^{th}-party supply chain