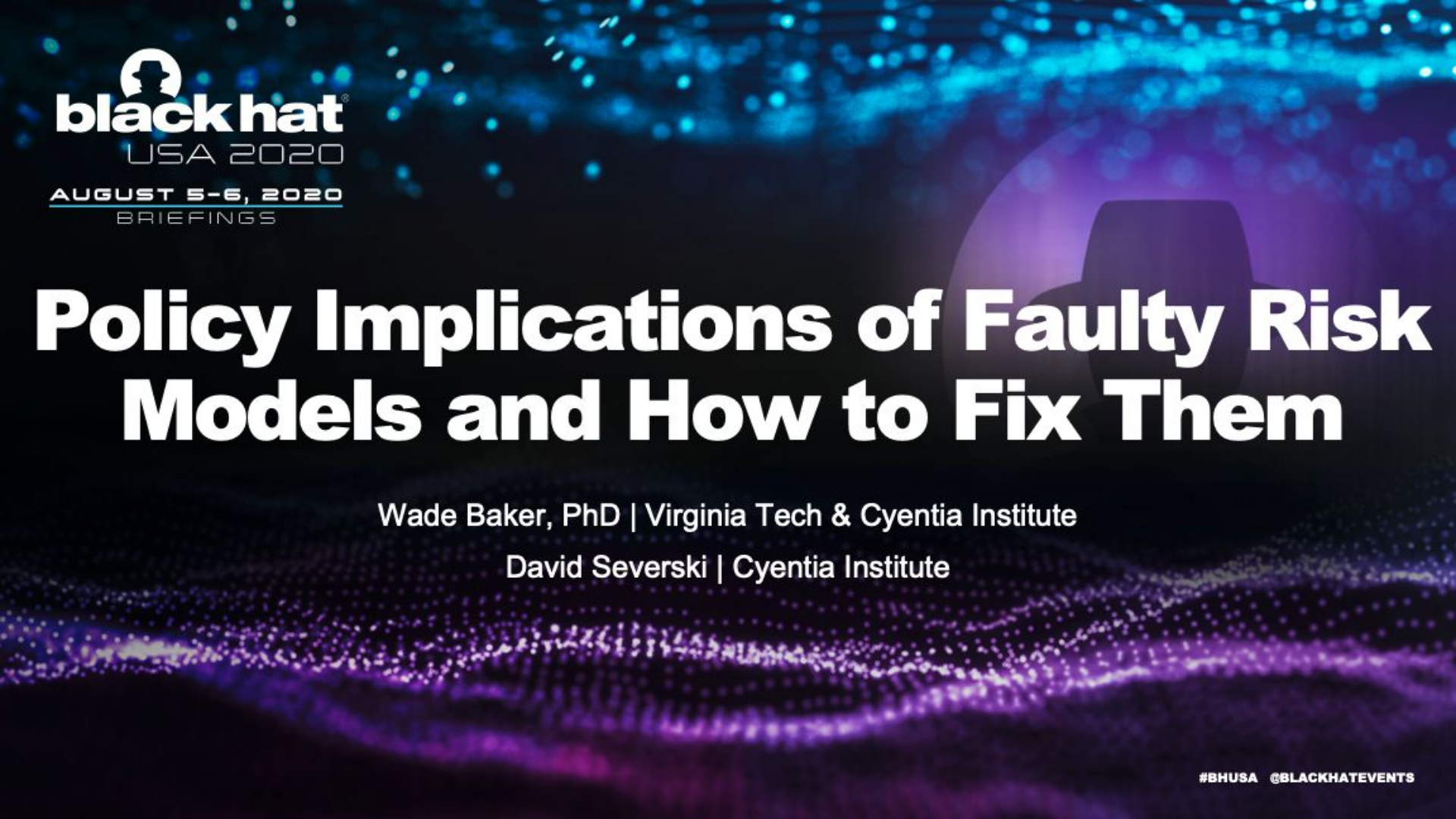


Policy Implications of Faulty Risk Models and How to Fix Them

Wade Baker, PhD | Virginia Tech & Cyentia Institute

David Severski | Cyentia Institute

Introduction

At Cyentia, we help the vendor community find a share the insights hidden in their data.

We're no stranger to incident data and models

- Verizon DBIR - The trail blazer of data-driven incident analysis
- Information Risk Insights Study (IRIS) 20/20 - A ten year review of cyber loss data events and the implications on cost modelling
- Ripples Across the Risk Surface- Study of multi-party security incidents and the propagation of downstream losses
- IRIS Extreme — Coming Soon! — A deep dive into the heavy tail of incident losses

Examples of Faulty Risk Models

cyentia

- Myth -

THE DENVER POST

BUSINESS › TECHNOLOGY

60% of small companies that suffer a cyber attack are out of business within six months.

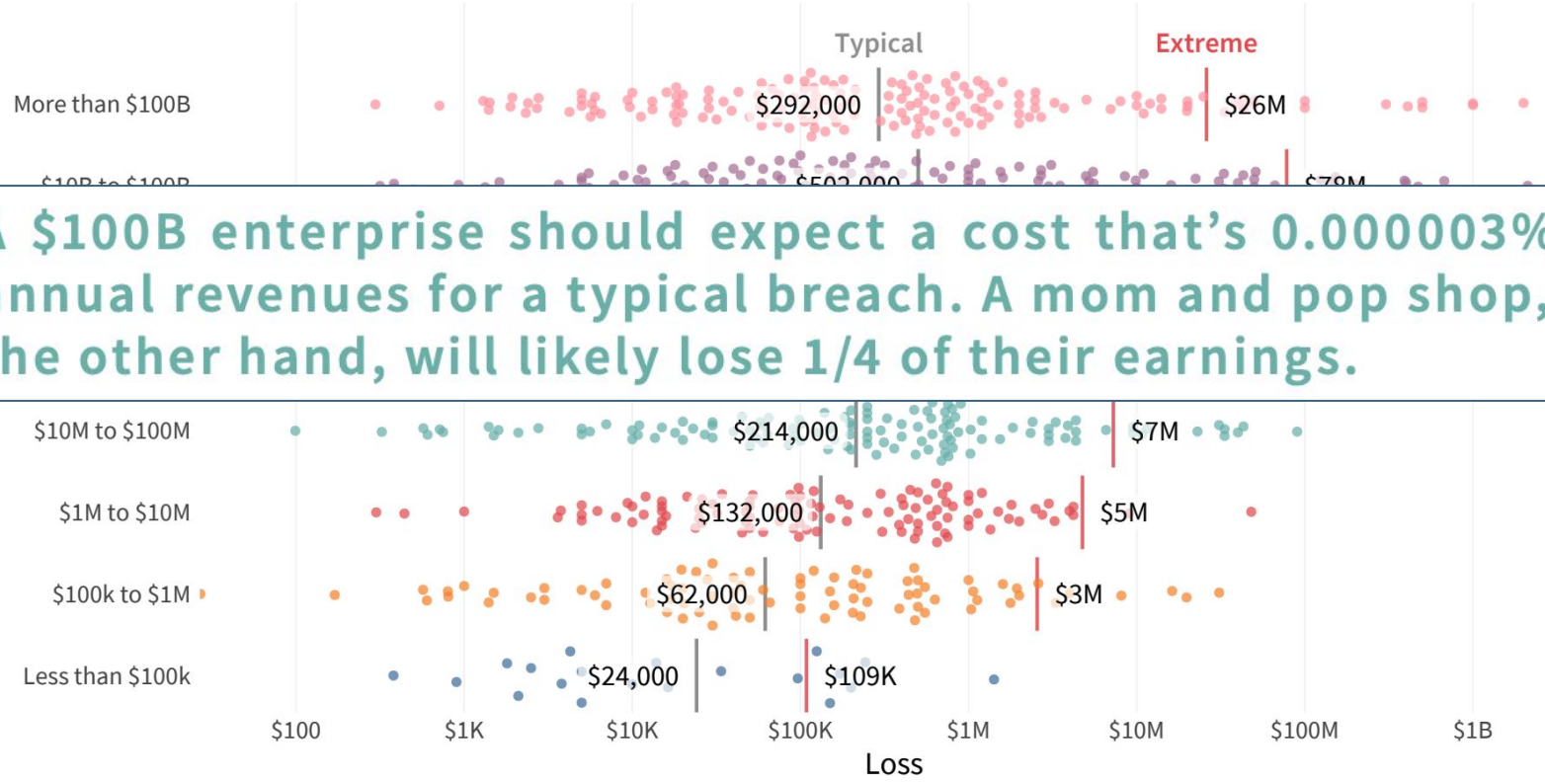
http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

> "The 2011 statistic that '60 percent of businesses close within 6 months of a cyberattack' is not from NCSA and its original source cannot be confirmed."

https://www.bankinfosecurity.com/blogs/60-hacked-small-businesses-fail-how-reliable-that-stat-p-2464

- Reality -

Figure 16: Distribution of breach losses by firm size (in revenue) with estimates for typical and extreme events



> **A $100B enterprise should expect a cost that's 0.000003% of annual revenues for a typical breach. A mom and pop shop, on the other hand, will likely lose 1/4 of their earnings.**

https://www.cyentia.com/iris/

- Myth -

TechRepublic. | SECURITY | CLOUD

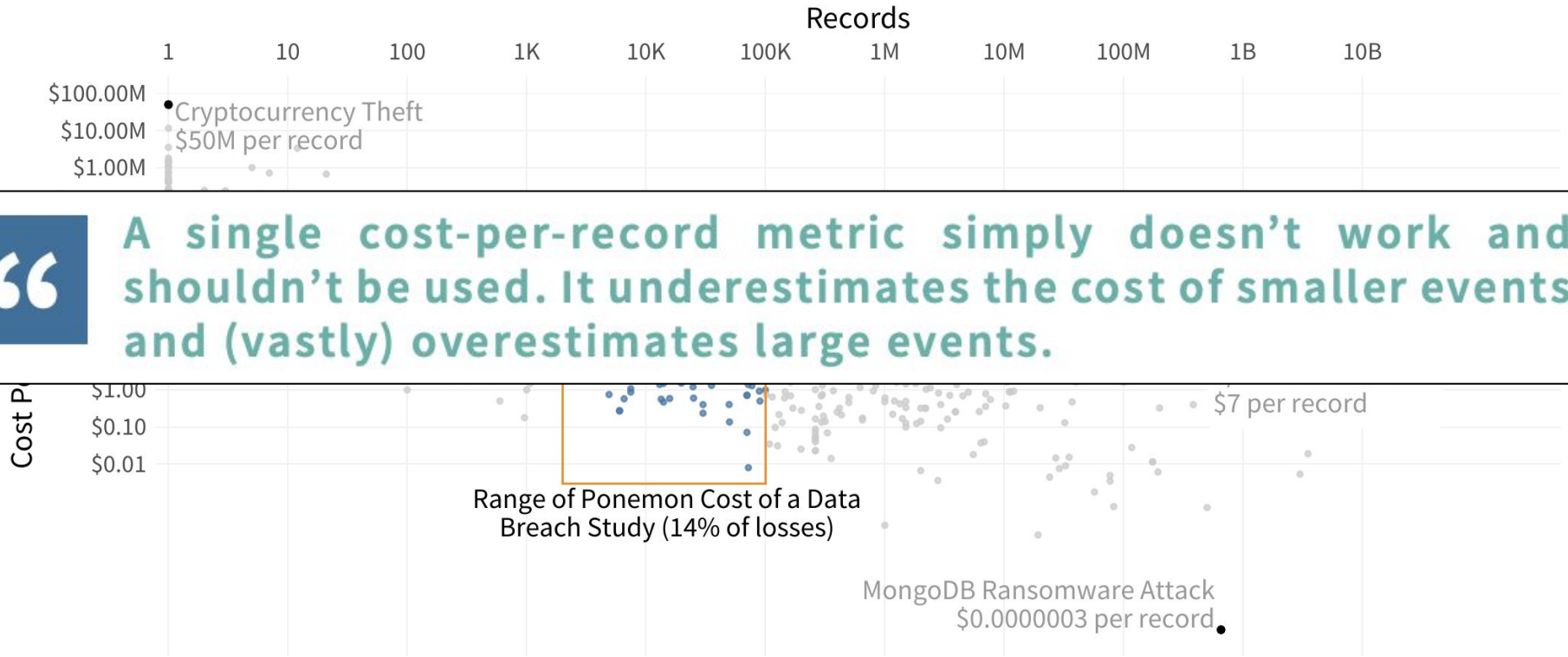
https://www.techrepublic.com/article/cloud-misconfigurations-cost-companies-nearly-5-trillion/

Cloud misconfigurations cost companies nearly $5 trillion

A DivvyCloud report finds 196 data breaches exposed more than 33 billion records due to environments without appropriate security.

Gartner estimated that the worldwide public cloud services market was $182.4 billion in 2018 and $214.3 billion in 2019. This means that the cost to companies due to breaches caused by cloud misconfigurations is more than 12 times the amount of worldwide investments in cloud services. Therefore, companies must adopt proper cloud security in order to protect this investment and prevent devastating costs associated with data breaches.

- Reality -

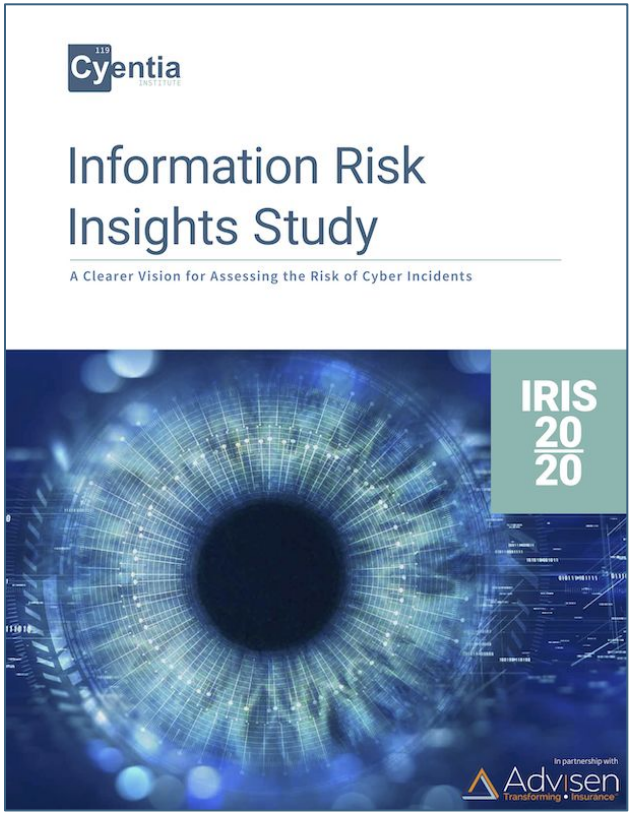


> **A single cost-per-record metric simply doesn't work and shouldn't be used. It underestimates the cost of smaller events and (vastly) overestimates large events.**

https://www.cyentia.com/iris/

First Party Losses

Information Risk Insights Study (IRIS) 20/20

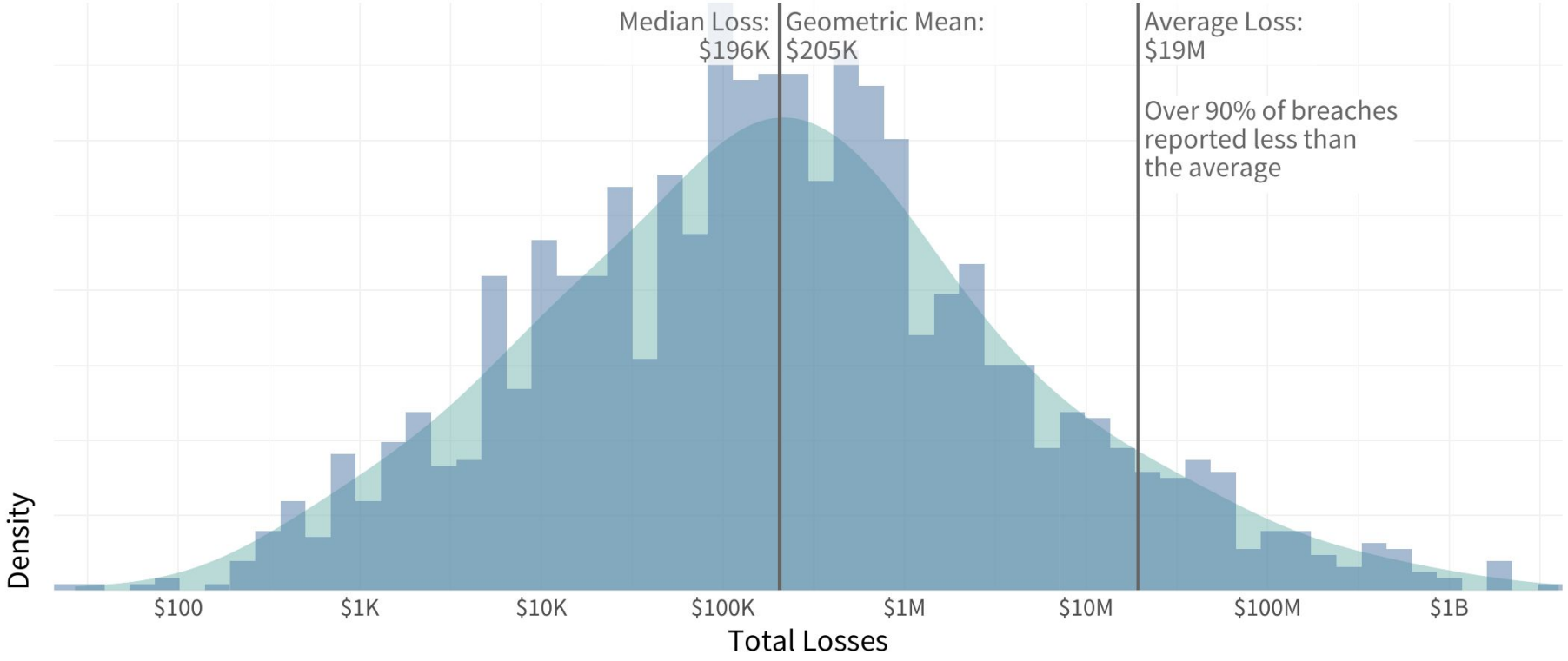


Objective: Provide data-driven models for better estimating the loss side of the risk equation.

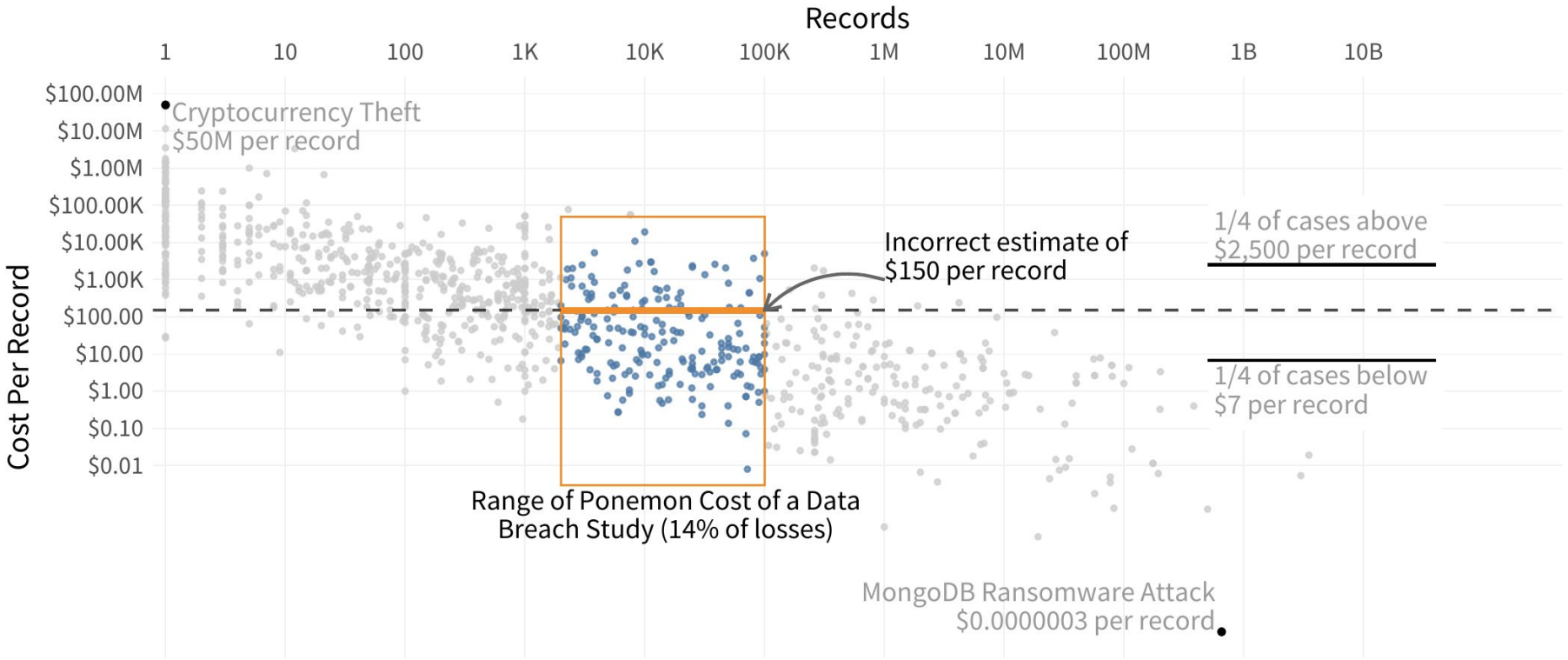
Data Source: Advisen's feed of over 100,000 publicly discoverable breach events.

Study sample: Ten year history (2010-2019) with over 56K events with breach data.

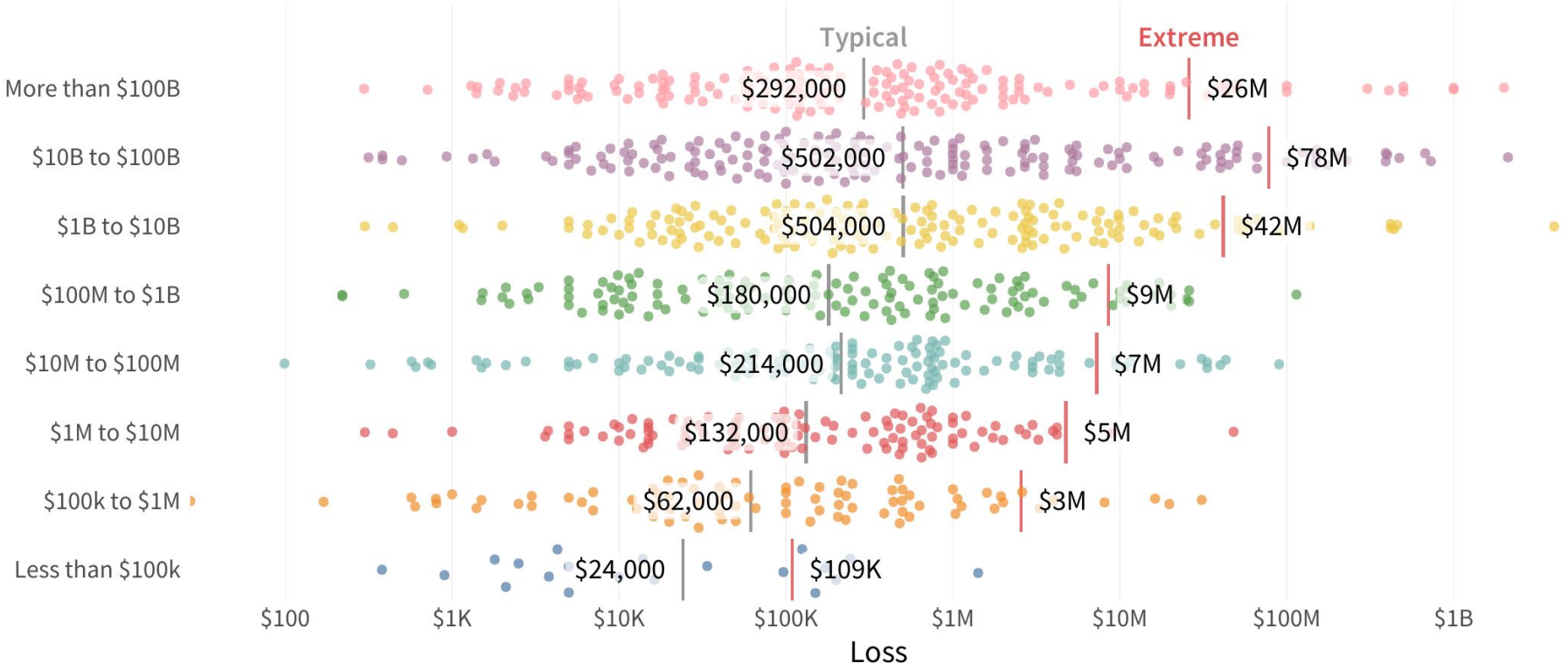
The Flaw of Averages



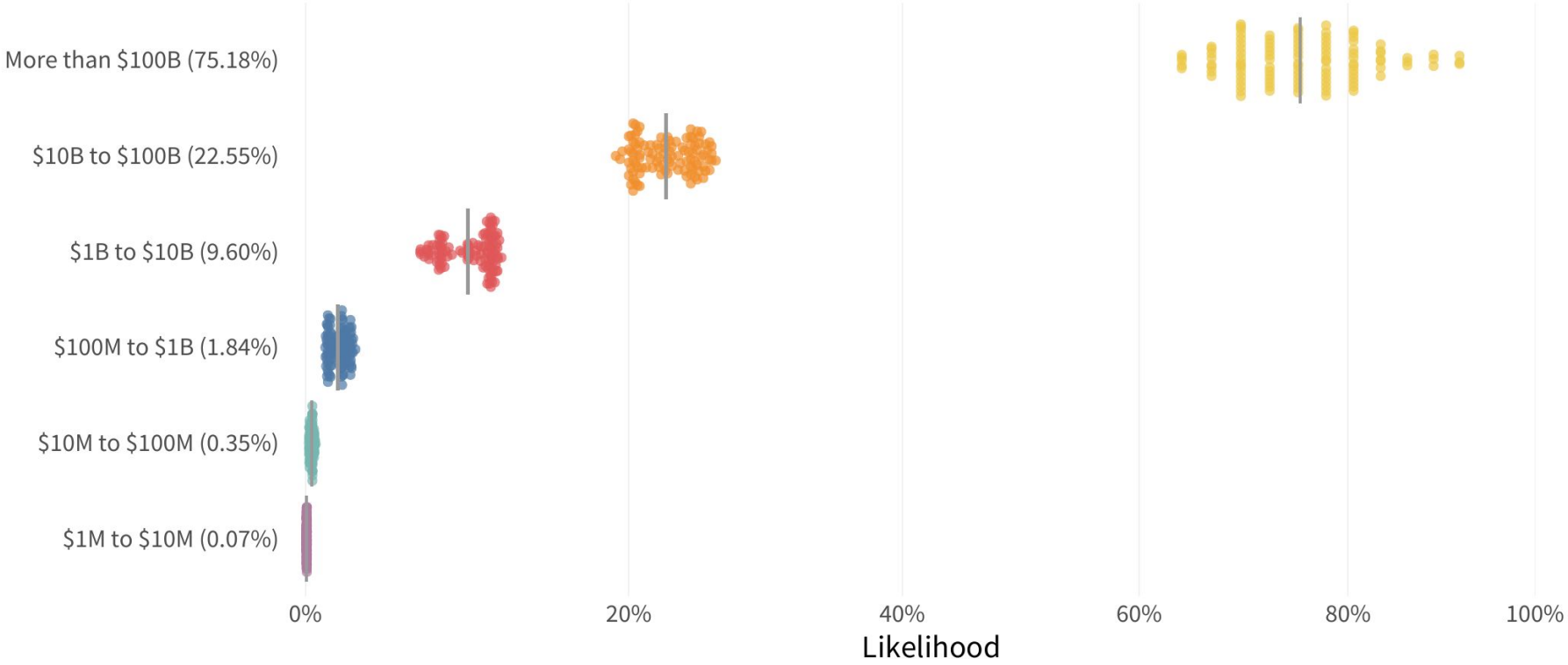
More Data is Essential for Good Results



For Loss, Size Matters

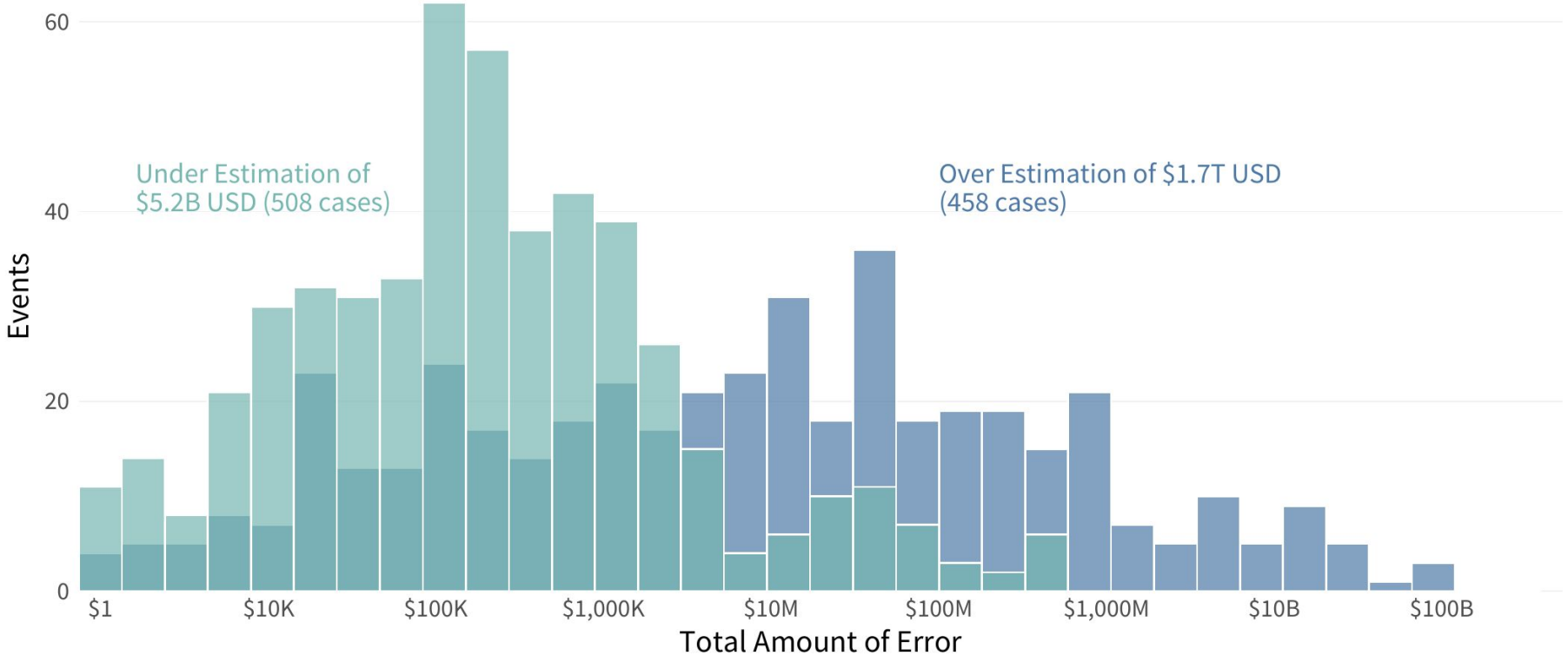


For Frequency, Size Still Matters



cyentia

But What Difference Does This Make?



~~Resuscitating~~ Replacing CPR

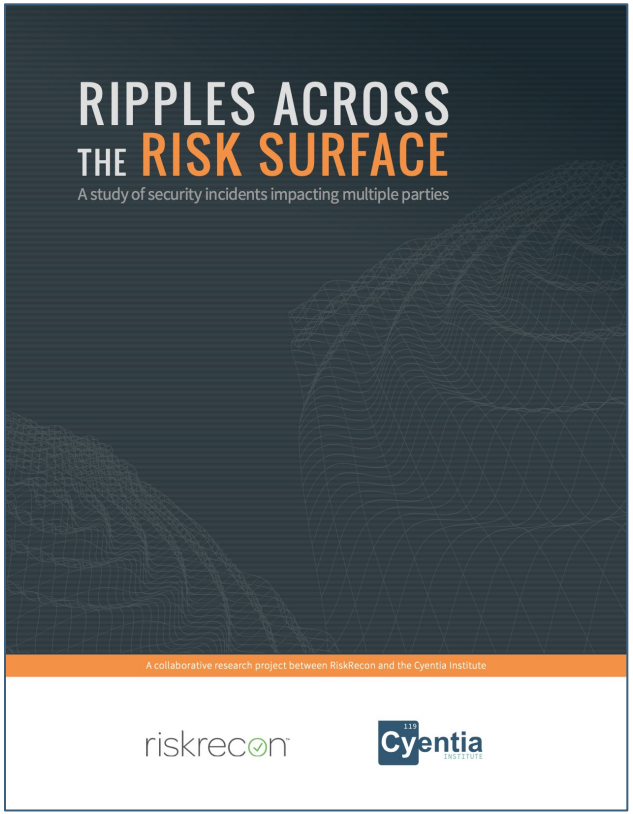
Records	Probability of At Least This Much Loss					
	$10K	$100K	$1M	$10M	$100M	$1B
100	82.0%	49.9%	17.8%	3.3%	0.3%	0.0%
1K	88.4%	60.9%	26.0%	5.9%	0.7%	0.0%
10K	93.0%	71.1%	35.8%	10.0%	1.4%	0.1%
100K	96.0%	79.8%	46.7%	15.8%	2.7%	0.2%
1M	97.9%	86.7%	57.7%	23.5%	5.0%	0.5%
10M	99.0%	91.8%	68.2%	32.8%	8.6%	1.1%
100M	99.5%	95.3%	77.4%	43.4%	13.9%	2.3%
1B	99.8%	97.4%	84.9%	54.5%	21.0%	4.2%
10B	99.9%	98.7%	90.5%	65.3%	30.0%	7.4%

Looking at Policy Through the IRIS

- SMB impacts
  - Small firms have rare, but disproportionate losses
- Losses are not evenly distributed
  - Most of the time, losses are not material
  - The heavy tail of losses is rare, but real
- Regulatory impacts
  - Disclosure laws
- Cyber insurance
  - Catastrophe modelling rises in importance

3rd Party Risk

Ripples Across the Risk Surface



Objective: Understand the frequency and impact of multi-party cybersecurity incidents, most common due to vendor security compromise

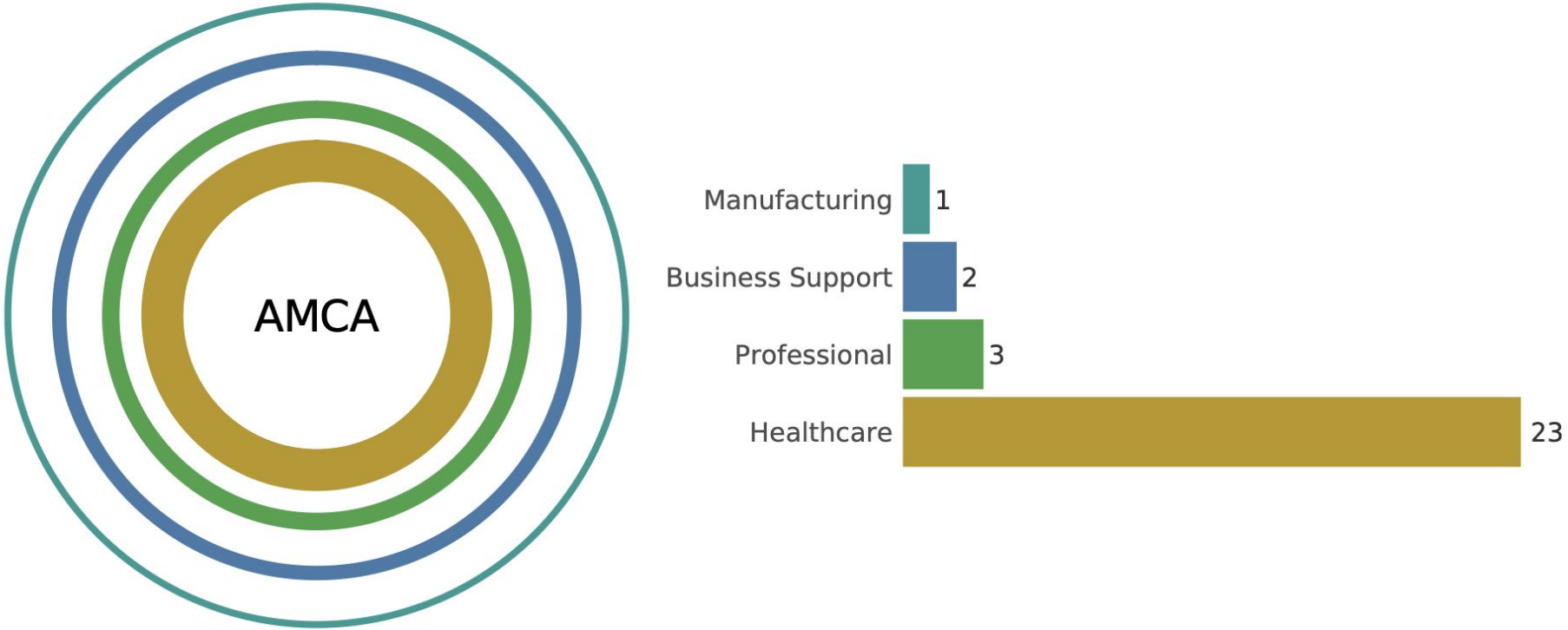
Data Source: Advisen's cyber loss database containing 92,000 cyber events collected from publicly verifiable sources

Study sample: Multi-party incidents (aka "ripple events")

- 813 unique ripple events identified in dataset.
- 5,437 organizations impacted by 813 ripple events.
- Range of 3 to 131 firms impacted in each ripple event

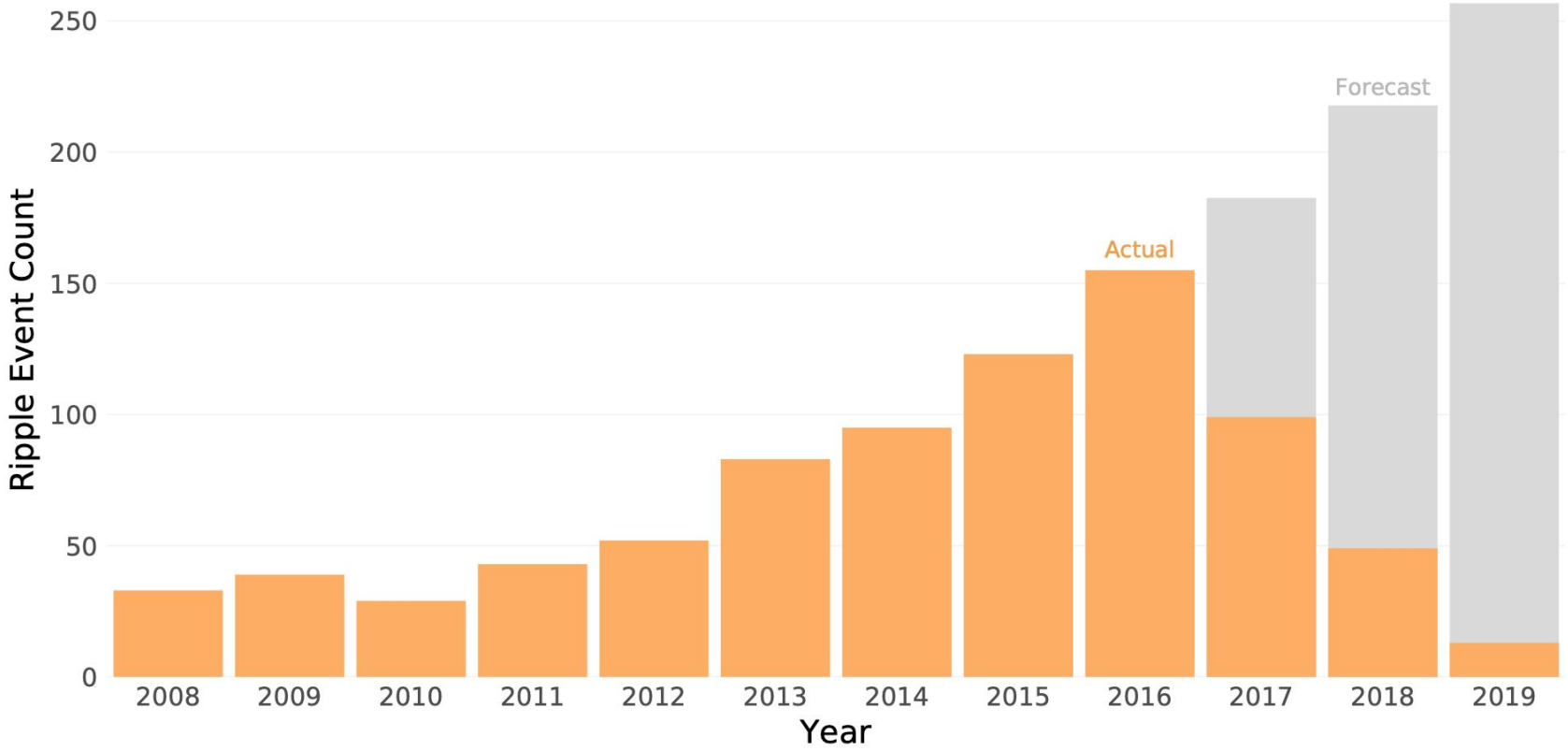
Losses Are Not Limited To Primary Victim

FIGURE 1: RIPPLE EFFECTS PROPAGATING ACROSS INDUSTRIES FROM THE AMCA BREACH



Multi-Party Events Becoming More Common

FIGURE 3: NUMBER OF ACTUAL MULTI-PARTY INCIDENTS (ORANGE) WITH FORECASTS ACCOUNTING FOR RECORDING DELAYS (GRAY)

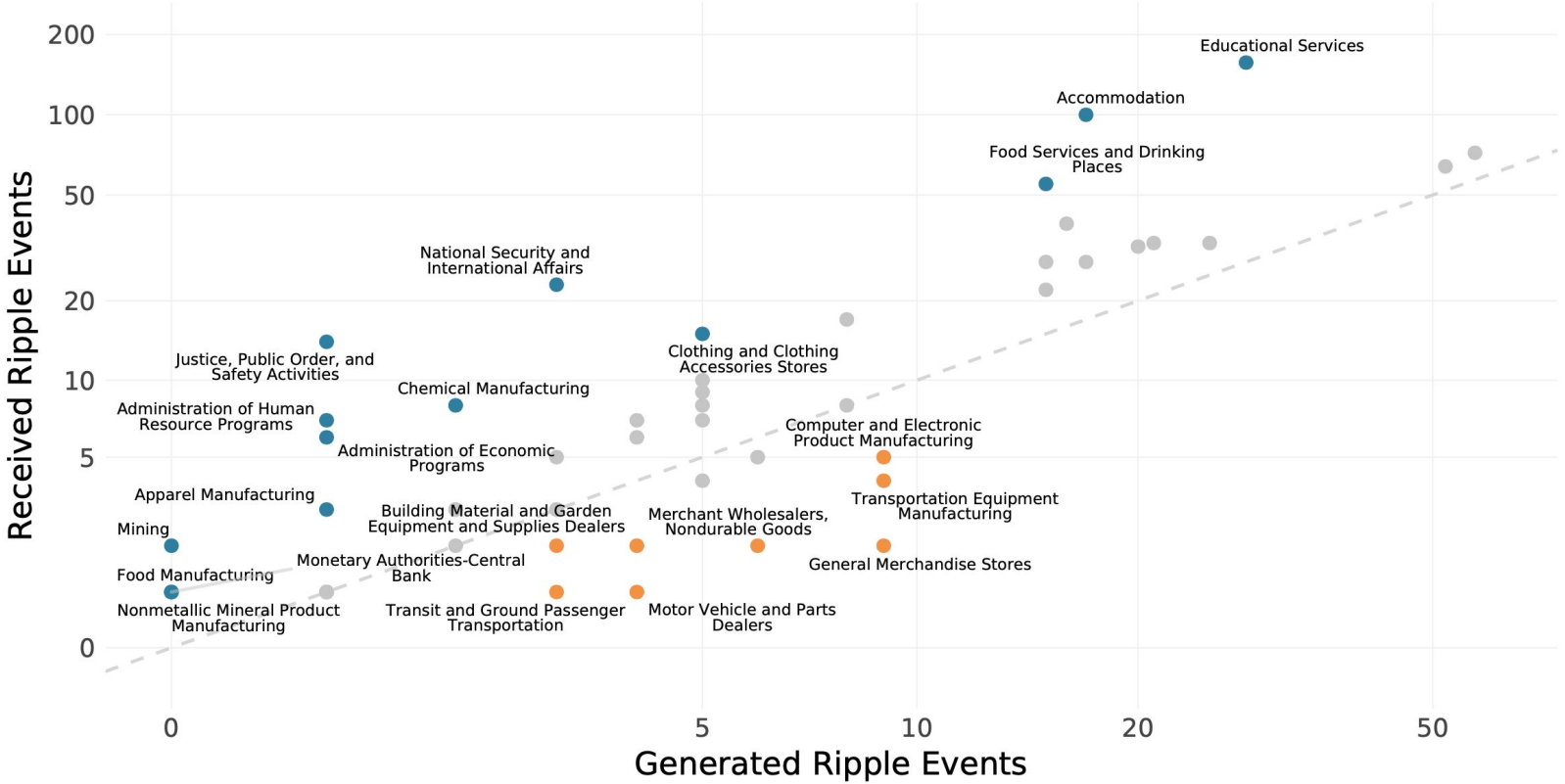


Ripple Events Amplify Downstream Victims

FIGURE 4: NUMBER OF CENTRAL VS. DOWNSTREAM ORGANIZATIONS AFFECTED IN MULTI-PARTY INCIDENTS

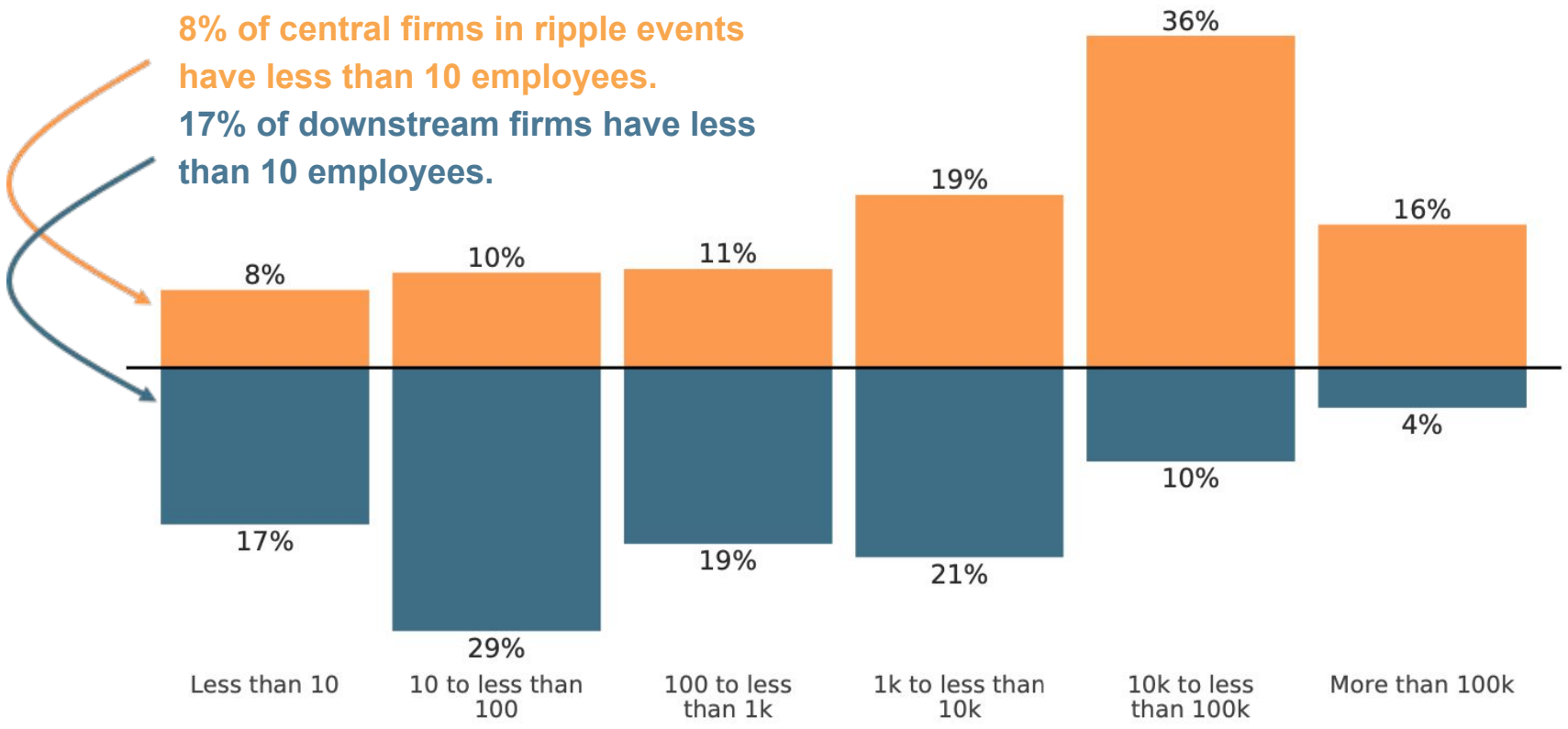
Sectors Don’t Generate/Receive Ripples Equally

FIGURE 9: RATIO OF CENTRAL VS. DOWNSTREAM RIPPLE EVENTS BY SUBSECTOR



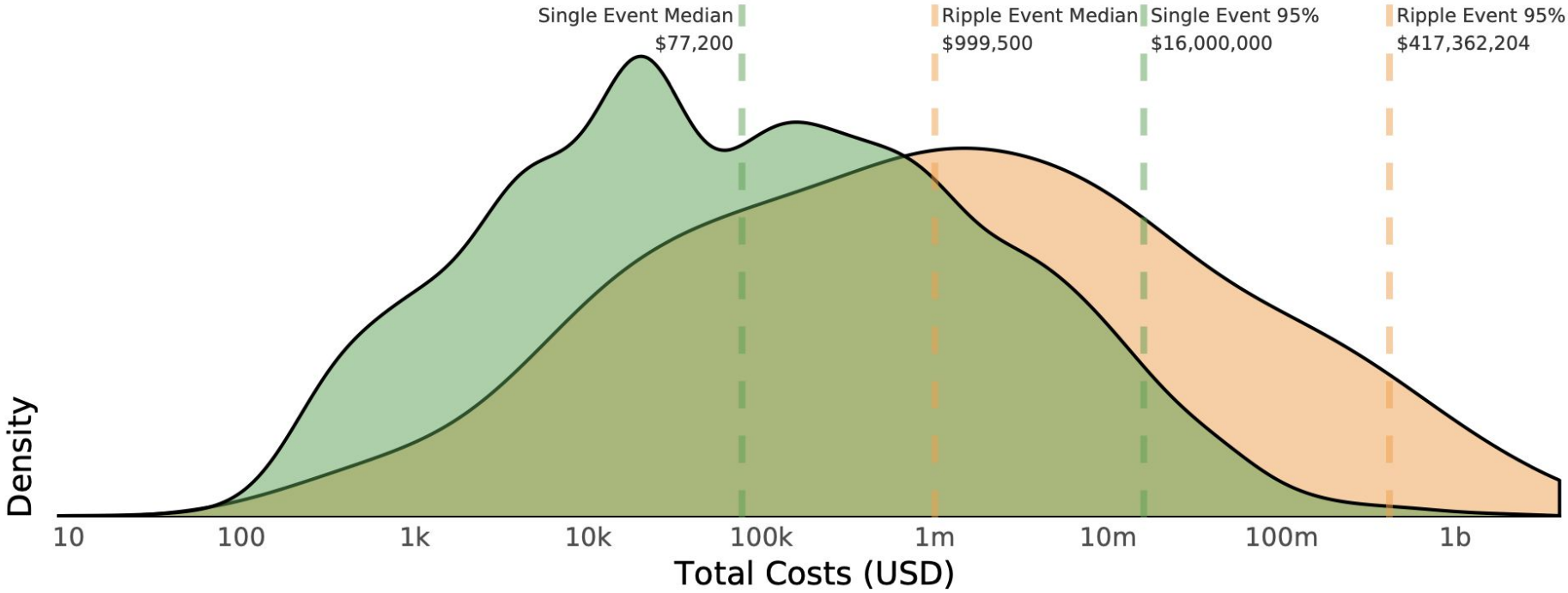
Downstream Victims Disproportionately SMBs

FIGURE 10: NUMBER OF CENTRAL VS. DOWNSTREAM RIPPLE EVENTS BY ORGANIZATION SIZE (EMPLOYEE COUNT)



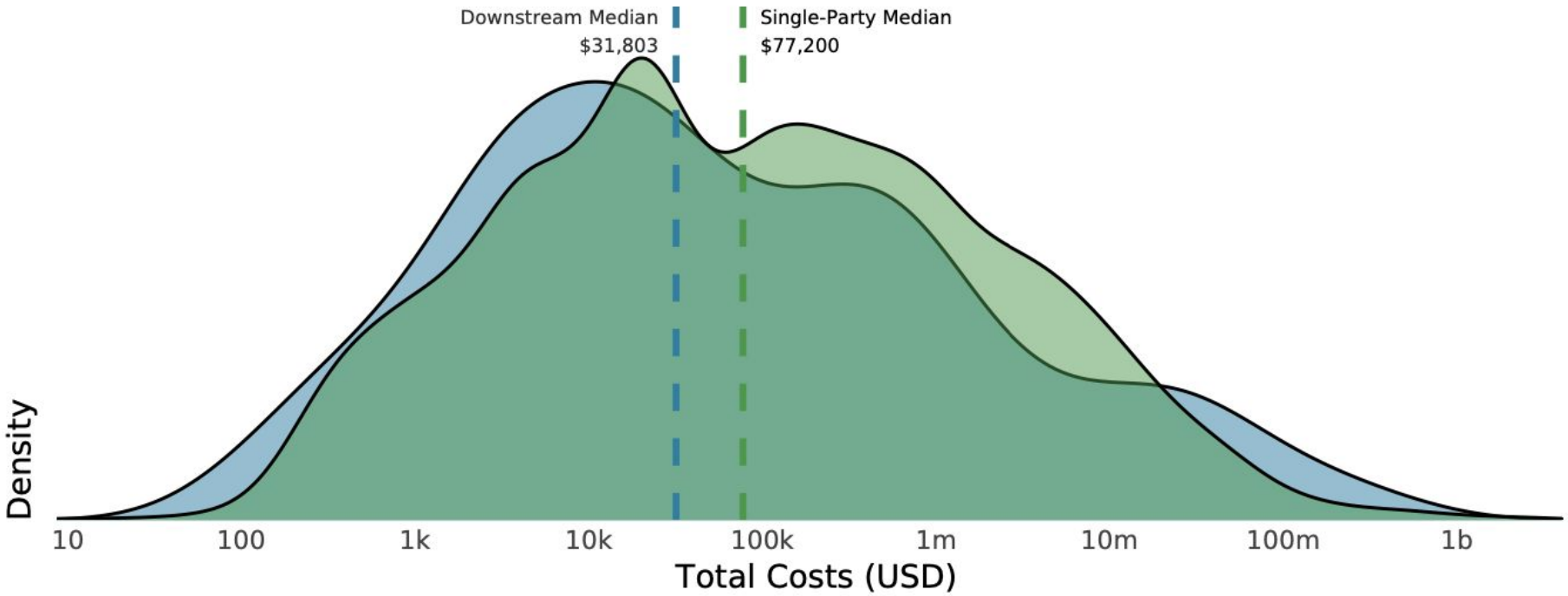
Total Losses Much Higher for Multi-Party Events

FIGURE 12: DISTRIBUTION OF TOTAL LOSSES FOR SINGLE-PARTY INCIDENTS VS. MULTI-PARTY INCIDENTS



Losses Similar For Central & Downstream Firms

FIGURE 13: DISTRIBUTION OF TOTAL LOSSES FOR SINGLE-PARTY INCIDENTS VS. DOWNSTREAM LOSSES IN MULTI-PARTY INCIDENTS



Implications of Poor 3rd Party Risk Models

- 3rd party risk "policy" mainly protects sourcing firms FROM suppliers
  - We've shown multi-party incidents disproportionately impact downstream, especially smaller, suppliers.
  - Is there a more equitable and effective approach to managing risk for the entire supply chain?
- Research suggests a type of "Bullwhip Effect" for 3rd party risk
  - Info sharing mitigates bullwhip effect in supply chain risk management.
  - Can more aggressive info/intel sharing help reduce 3rd party cyber risk?
- Recognition of data breaches as a form of negative externality has driven development of consumer data privacy policy and regulation
  - Negative externalities not only impact consumers but also downstream firms
  - How would this look/work applied to multi-party incidents?

Conclusions

The Failure of Policy

The burden of regulation affects smaller firms more than larger firms

- Larger firms seem to be successful in containing costs of breaches
- Smaller firms disproportionately affected

Disclosure laws

- Punitive environment for disclosing breaches

Policy and contractual remedies for breaches

- Nature of remedies are based on bad models

cyentia

...and How to Fix It

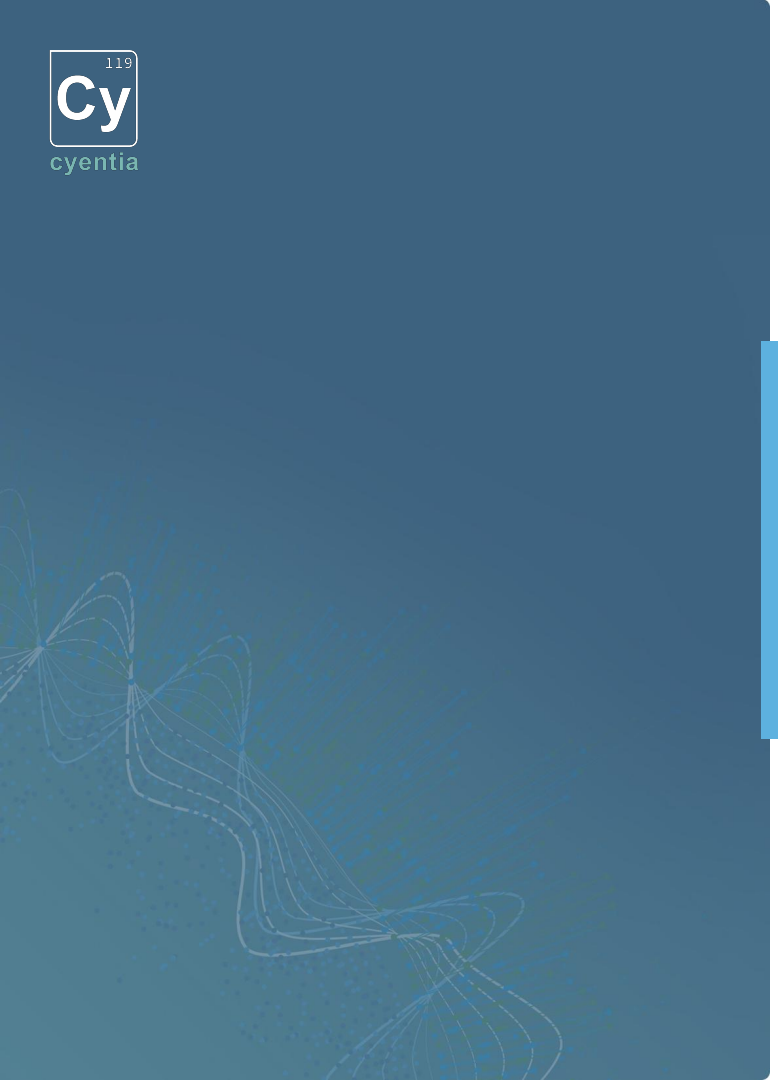
Specialization of security concerns

- Don’t roll your own crypto, or make your own POS system
- Firms will respond to regulatory regimes

We need better risk models to inform policy

Better Risk Models with Better Data Science

1. Collect better data
   a. Disclosure laws based on learning rather than shaming
   b. Fund and consolidate public sources of security data
2. Build better models
   a. Our field is beset with overly simplistic and unvalidated models in which we place far too much trust
   b. Many (like a flat cost per record for breaches) don't even pass cursory analysis, yet become tenets of our knowledge base
3. Conduct better research
   a. Reading industry reports often gives a sense that authors are more interested in promoting than learning
   b. Consume research with more skepticism
   c. Create research with more curiosity
   d. "Reward" organizations that produce solid research



Thank you!