We’re polishing our lenses…

The webinar shall begin shortly.

119 Cyentia INSTITUTE

IRIS 2022

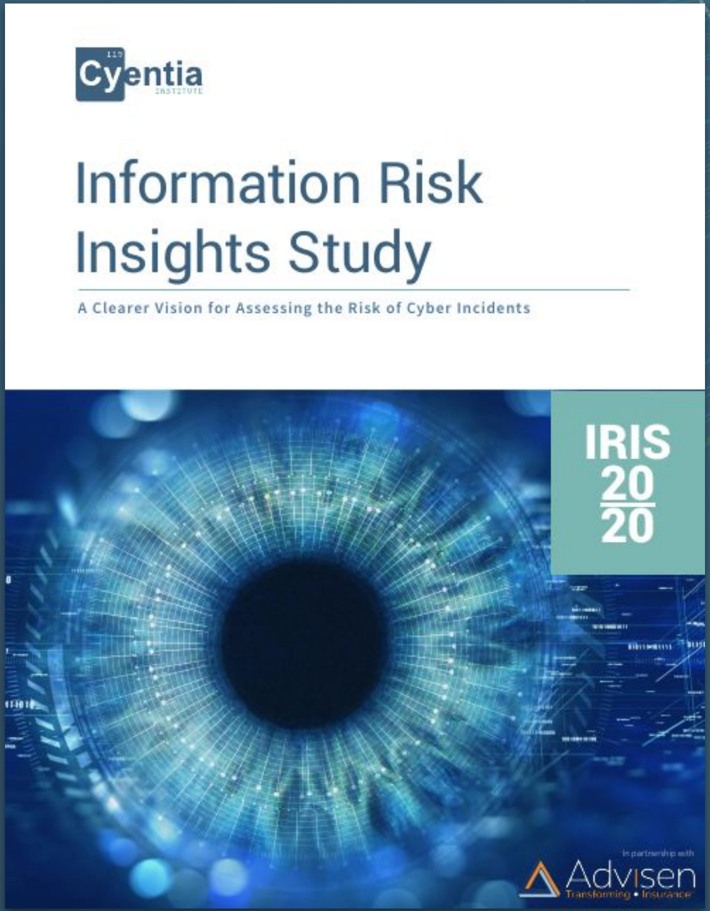
A Clearer Vision for Assessing the Risk of Cyber Incidents

David Severski and Olga Livingston

cyentia.com/iris

October 18, 2022

Cyentia and the IRIS



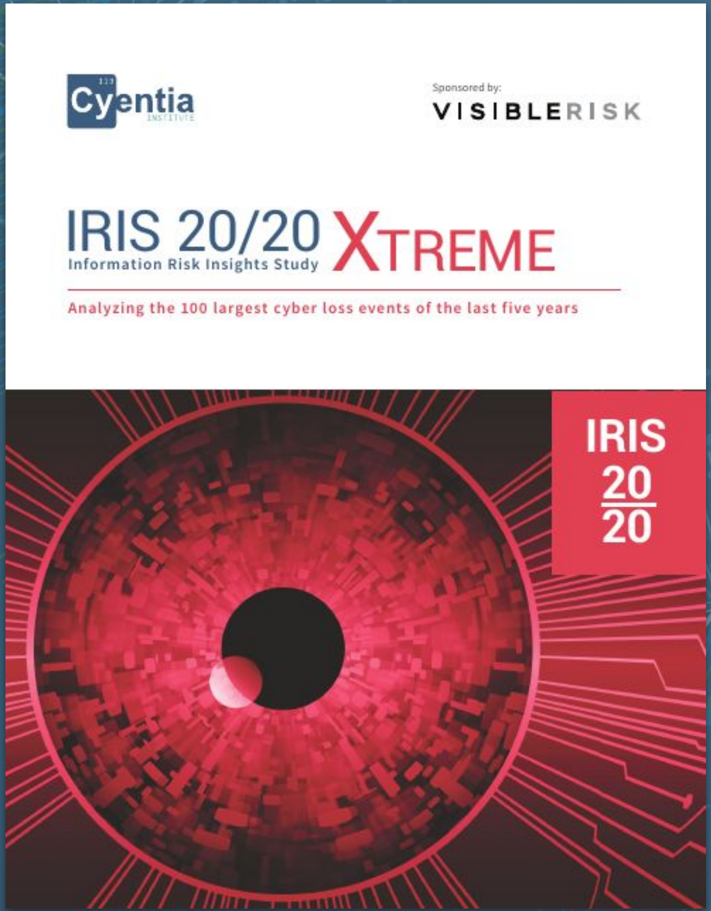
Cyentia INSTITUTE

Information Risk Insights Study

A Clearer Vision for Assessing the Risk of Cyber Incidents

IRIS 20 20

In partnership with Advisen Transforming • Insurance



Cyentia INSTITUTE

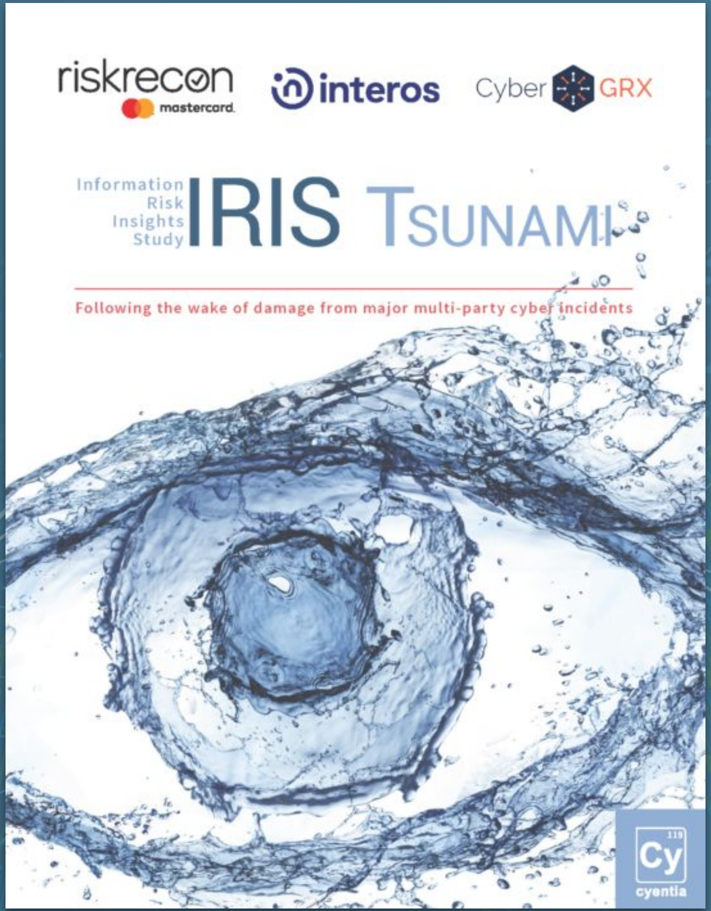
Sponsored by: VISIBLERISK

IRIS 20/20 XTREME

Information Risk Insights Study

Analyzing the 100 largest cyber loss events of the last five years

IRIS 20 20



riskrecon mastercard

interos

CyberGRX

Information Risk Insights Study IRIS TSUNAMI

Following the wake of damage from major multi-party cyber incidents

Cy cyentia

Who is the IRIS for?

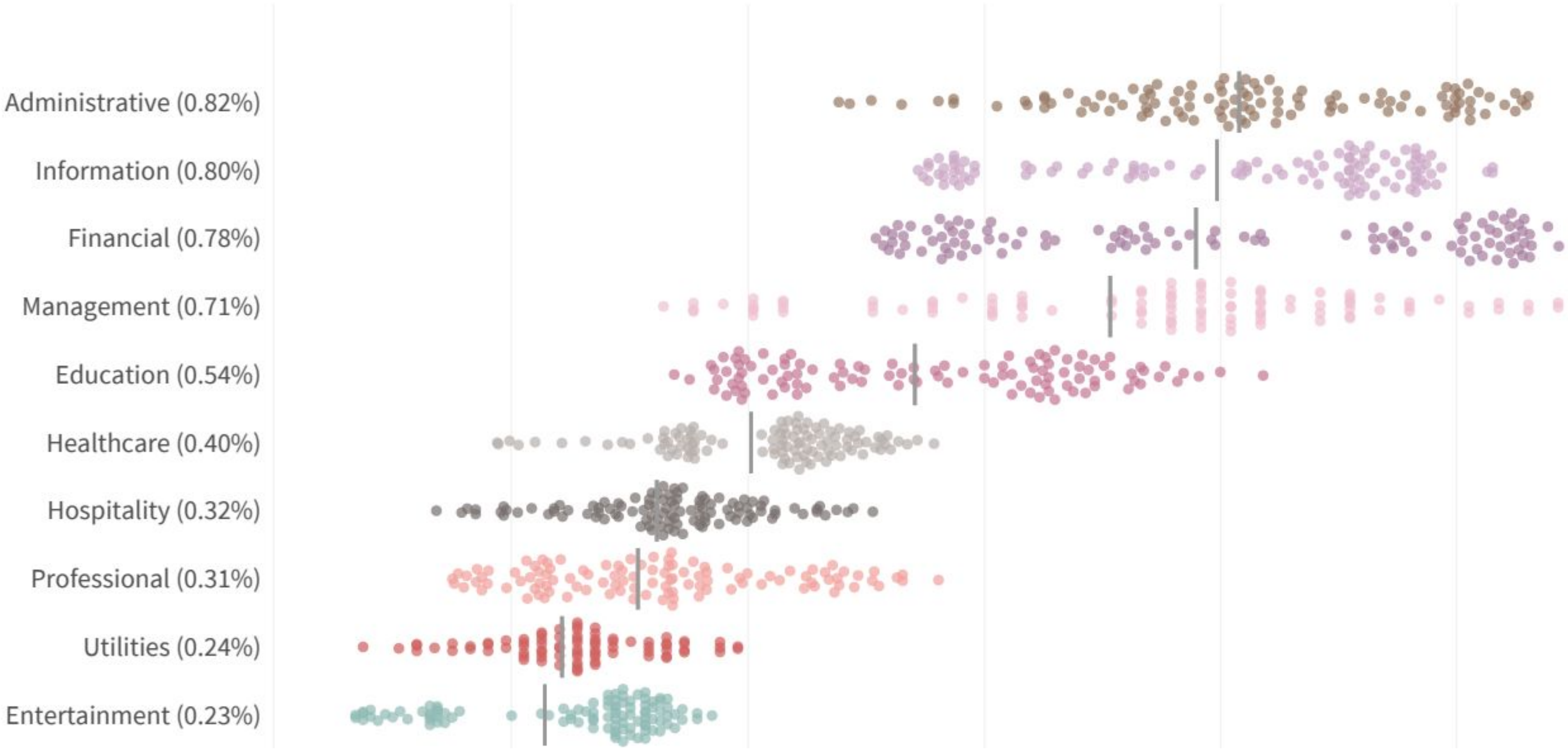
- Cyber Risk Quantification
- Insurance buyers
- Infosec strategists
- SOC analysts
- Vulnerability managers
- GRC professionals
- …and you!

Loss Event Frequency (LEF)

IRIS 2022

Hindsight is 20/20: Flashback to IRIS 20/20

Figure 6: Comparison of annual breach likelihood among firms by sector



Hindsight from 20/20: LEF lessons learned

1. LEFs based on sector alone will be heavily skewed toward smaller firms.
    a. Org size has a **major** effect on LEF (orders of magnitude).

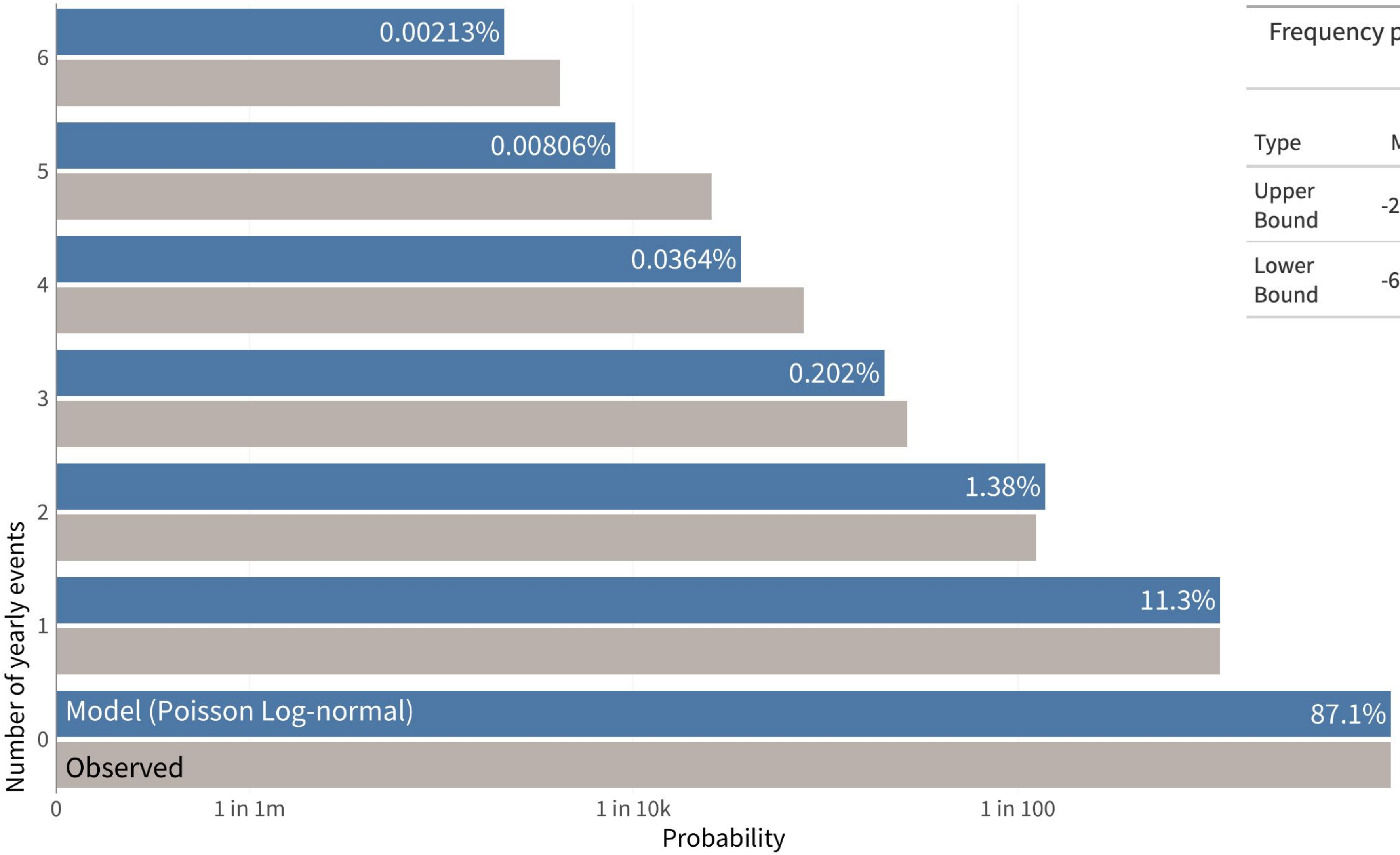
2. Estimating population size is **HARD** but has a **HUGE** effect on LEF.
    b. Using a known population (e.g., F1000) avoids this.
    c. Our denominator last time was almost certainly too large.
    d. Due to the uncertainty, we chose to create upper and lower bound LEFs.

New to IRIS 2022

Upper bound: A risk averse estimate using the number of organizations observed over the entire measurement period.

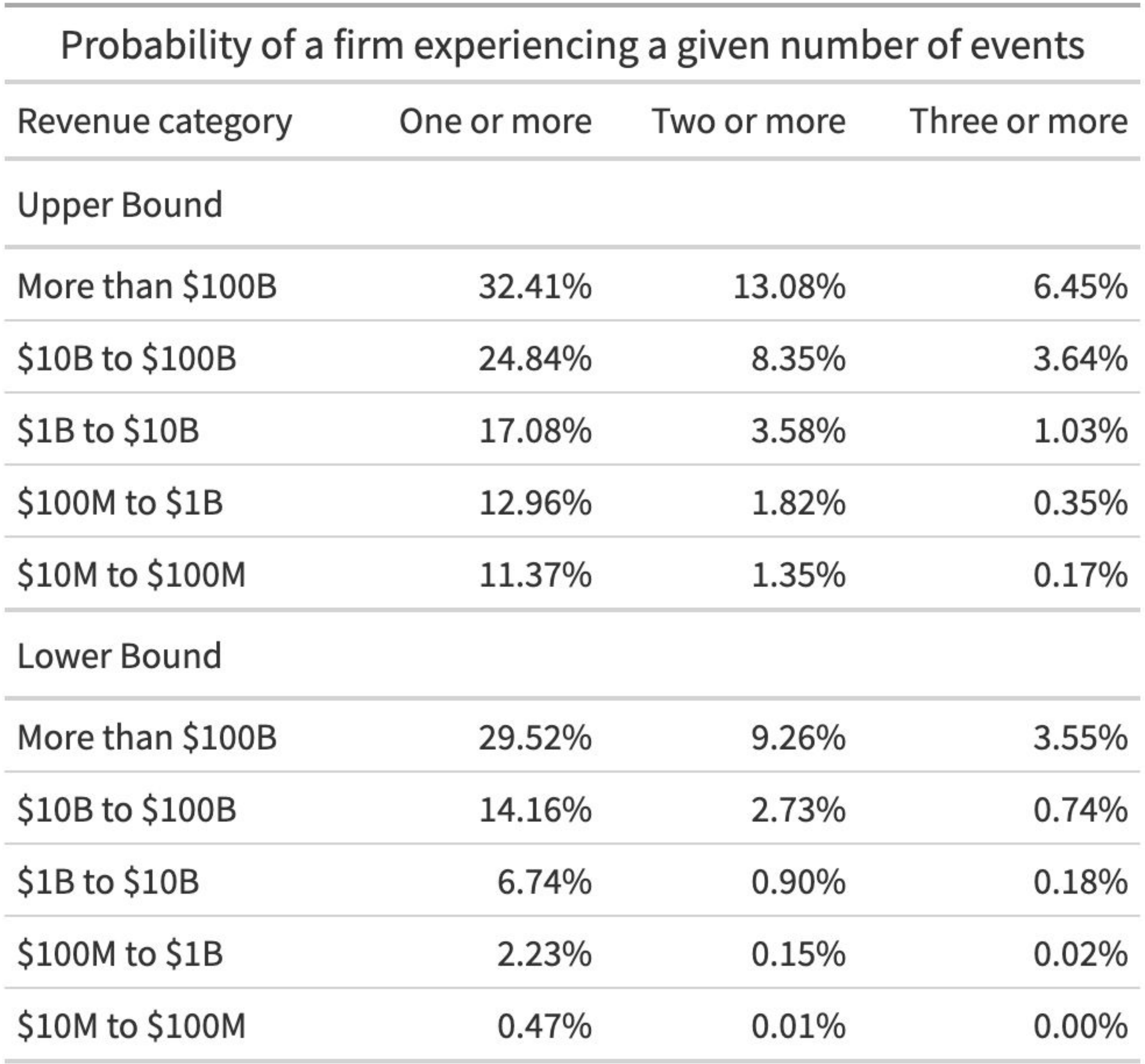
Lower bound: A risk tolerant estimate using the number of firms suspected to be present in a population.

Overall loss event frequency (upper bound)



Frequency parameters: Poisson log-normal		
Type	Mean (μ)	Standard deviation (σ)
Upper Bound	-2.284585	0.8690759
Lower Bound	-6.394251	1.7831914

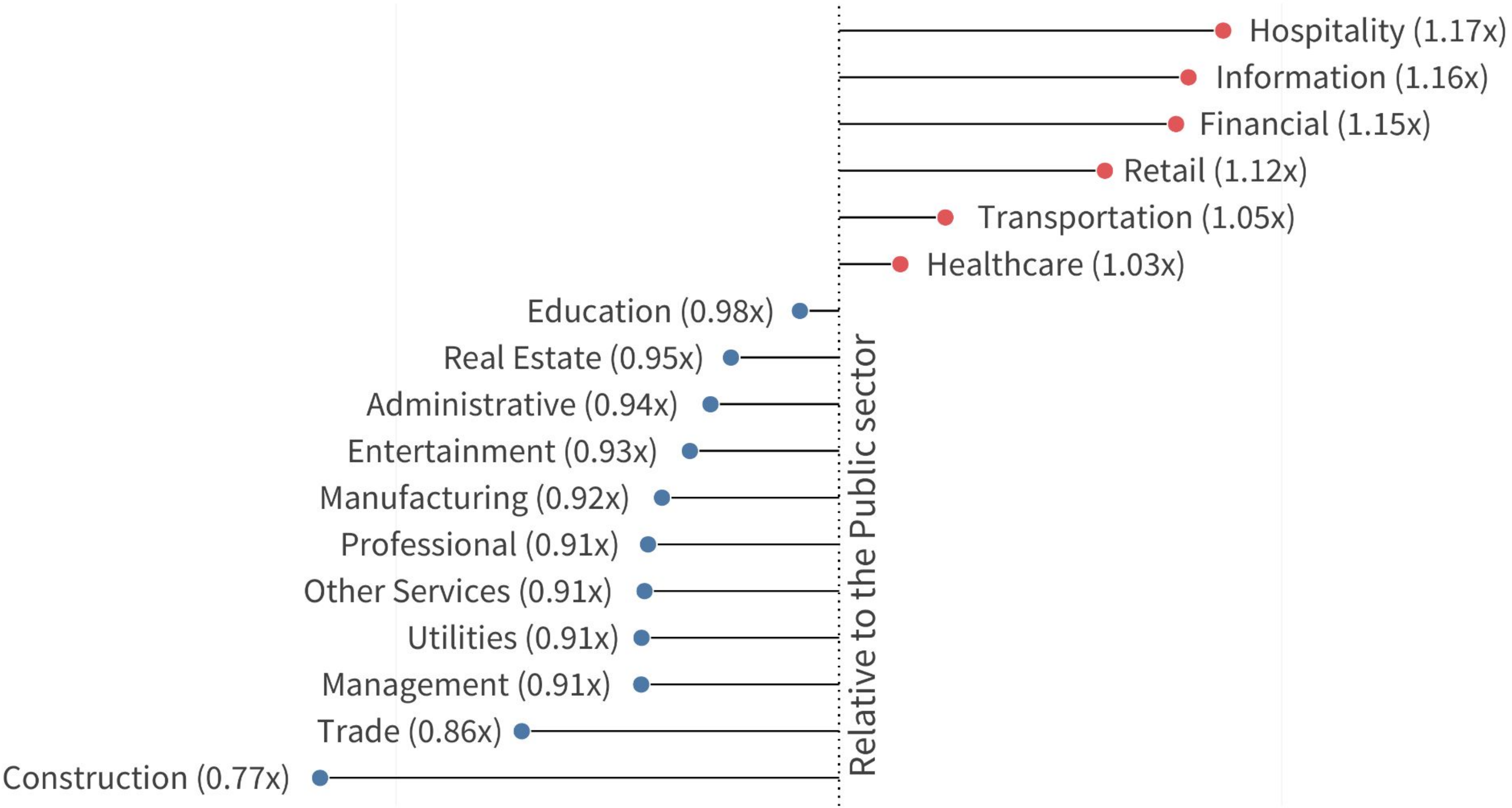
Probability of experiencing at least one event



Probability of a firm experiencing a given number of events

Revenue category	One or more	Two or more	Three or more
Upper Bound			
More than $100B	32.41%	13.08%	6.45%
$10B to $100B	24.84%	8.35%	3.64%
$1B to $10B	17.08%	3.58%	1.03%
$100M to $1B	12.96%	1.82%	0.35%
$10M to $100M	11.37%	1.35%	0.17%
Lower Bound			
More than $100B	29.52%	9.26%	3.55%
$10B to $100B	14.16%	2.73%	0.74%
$1B to $10B	6.74%	0.90%	0.18%
$100M to $1B	2.23%	0.15%	0.02%
$10M to $100M	0.47%	0.01%	0.00%

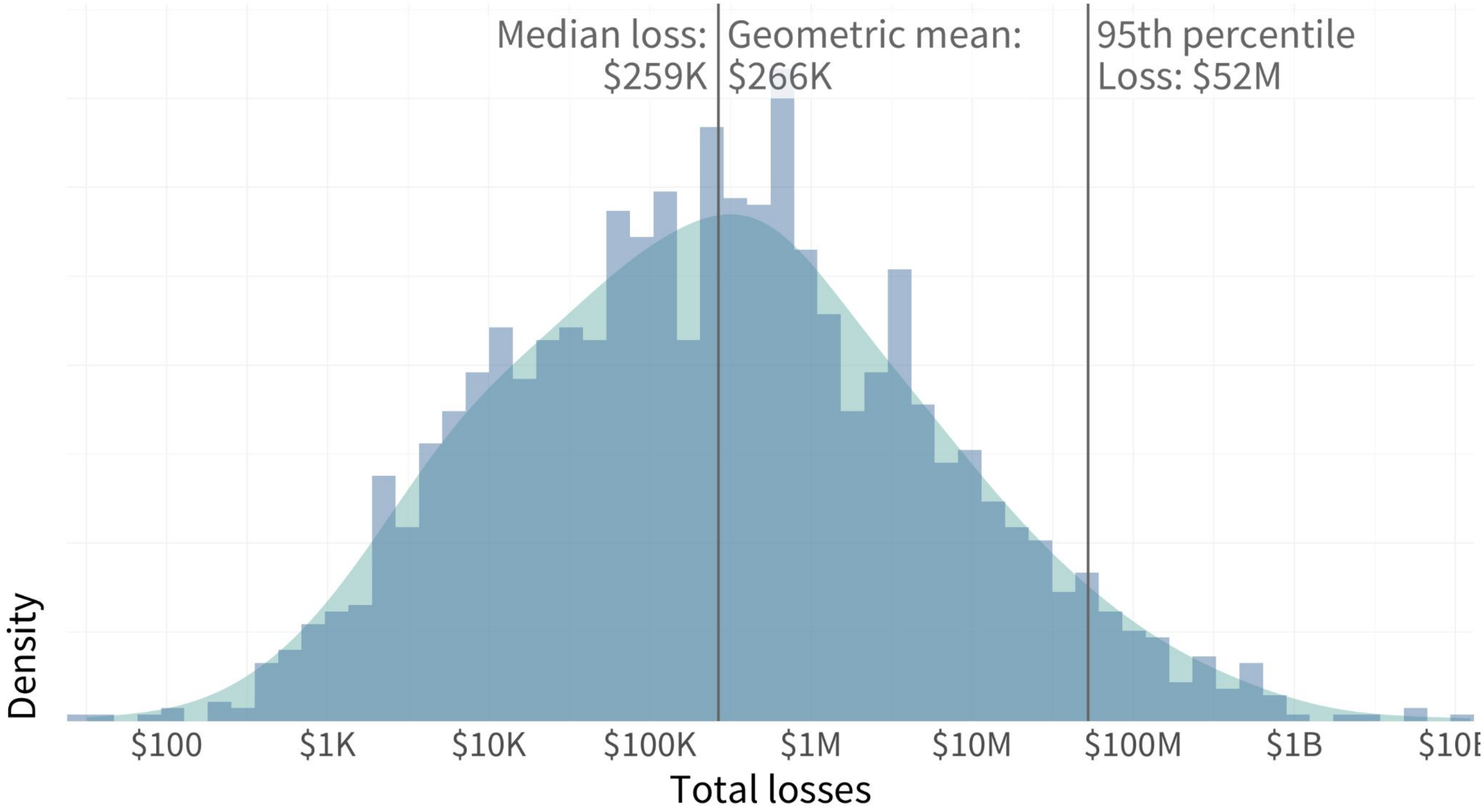
Relative LEF among sectors



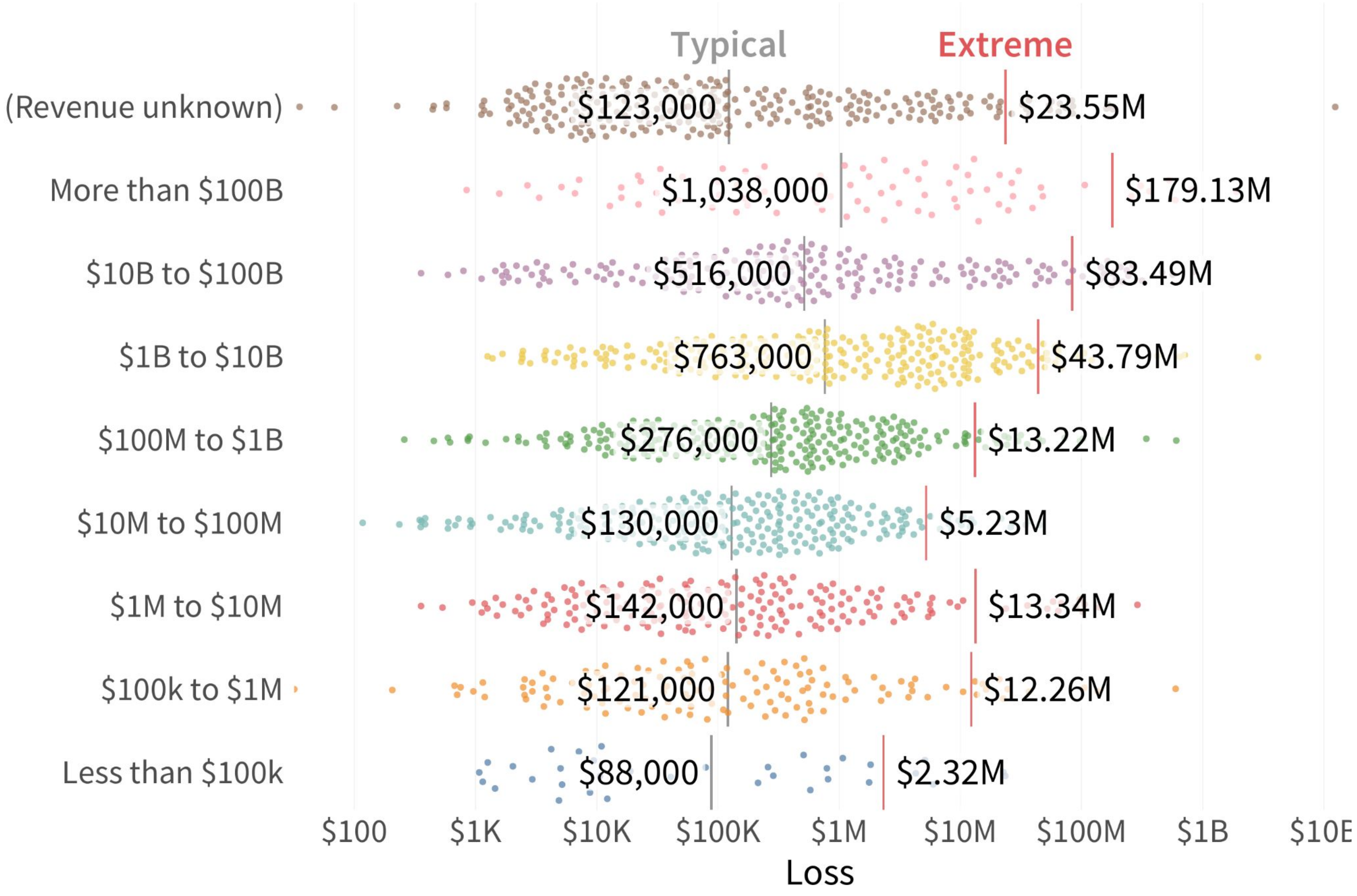
Loss Magnitude (LM)

IRIS 2022

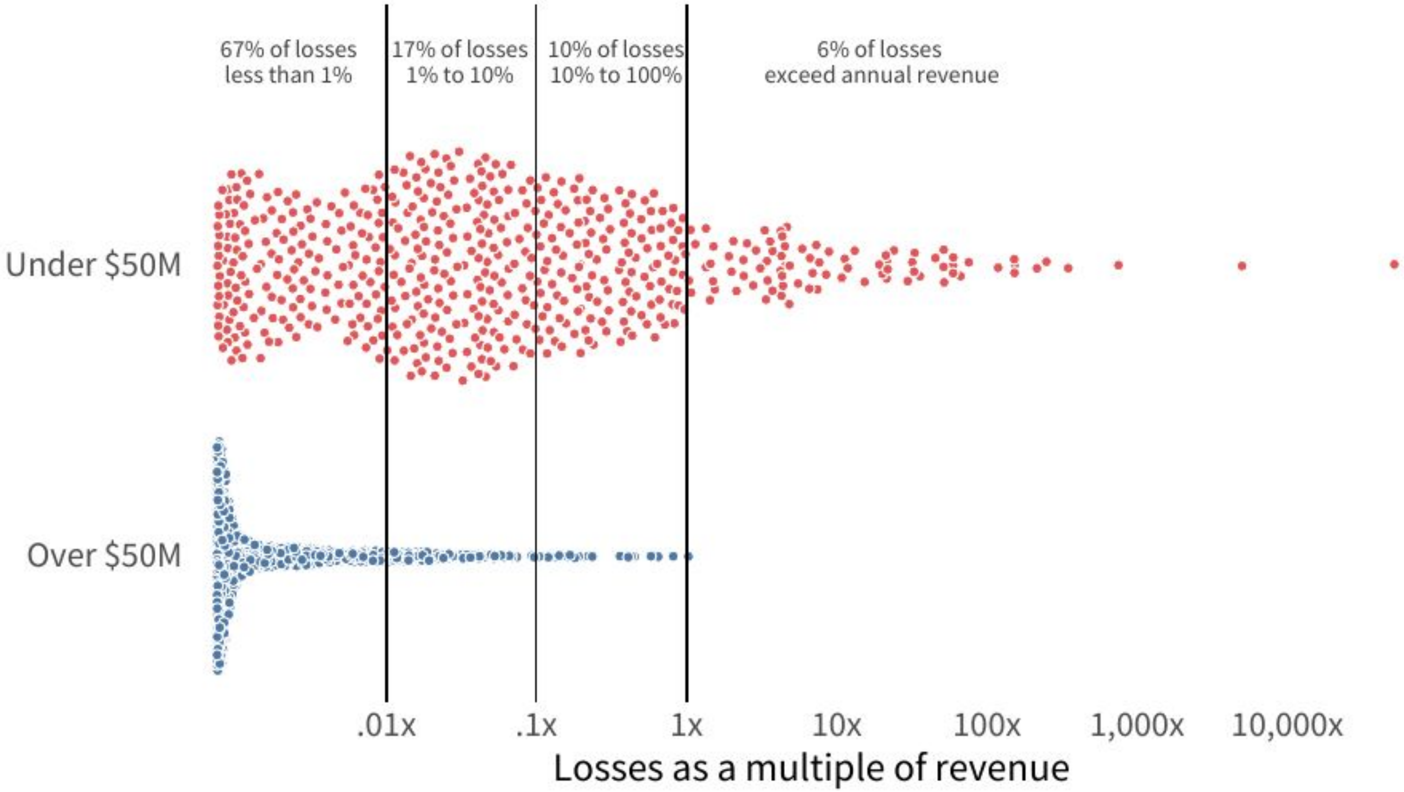
The typical and the extreme



Size continues to matter



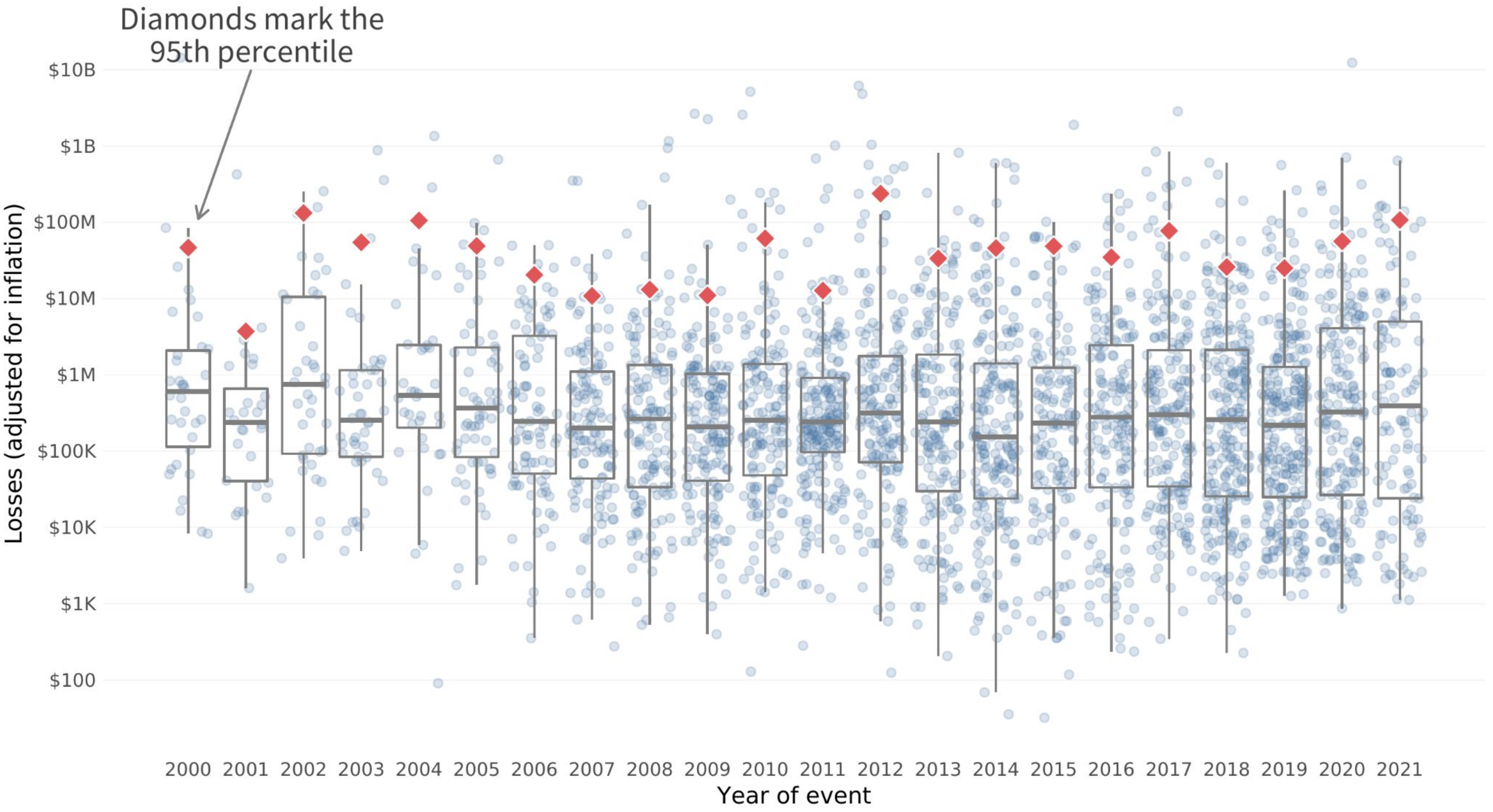
Losses as a percentage of revenue



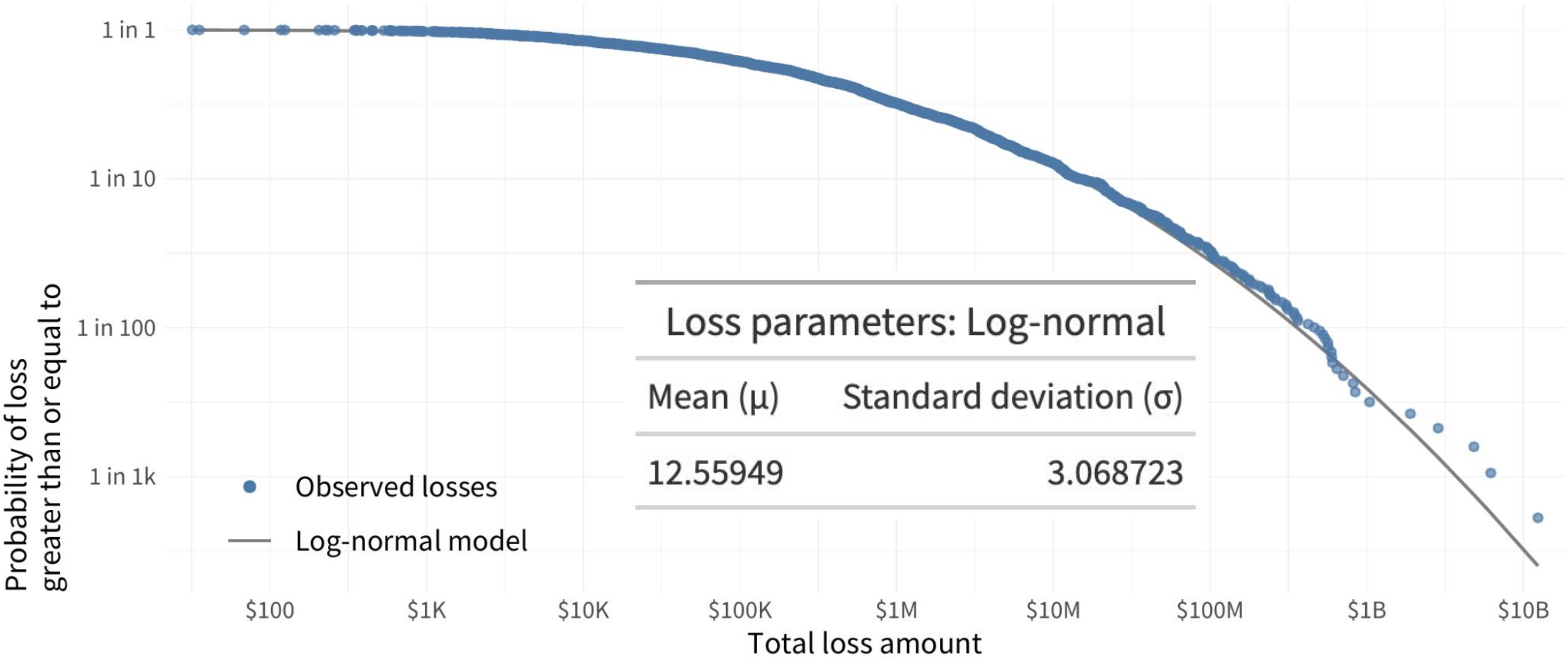
Of losses exceeding 10% of annual revenue, 89% occur among SMBs

All but 1 recorded loss over 100% of revenues occur among SMBs!

Distribution of losses



Parameters of loss

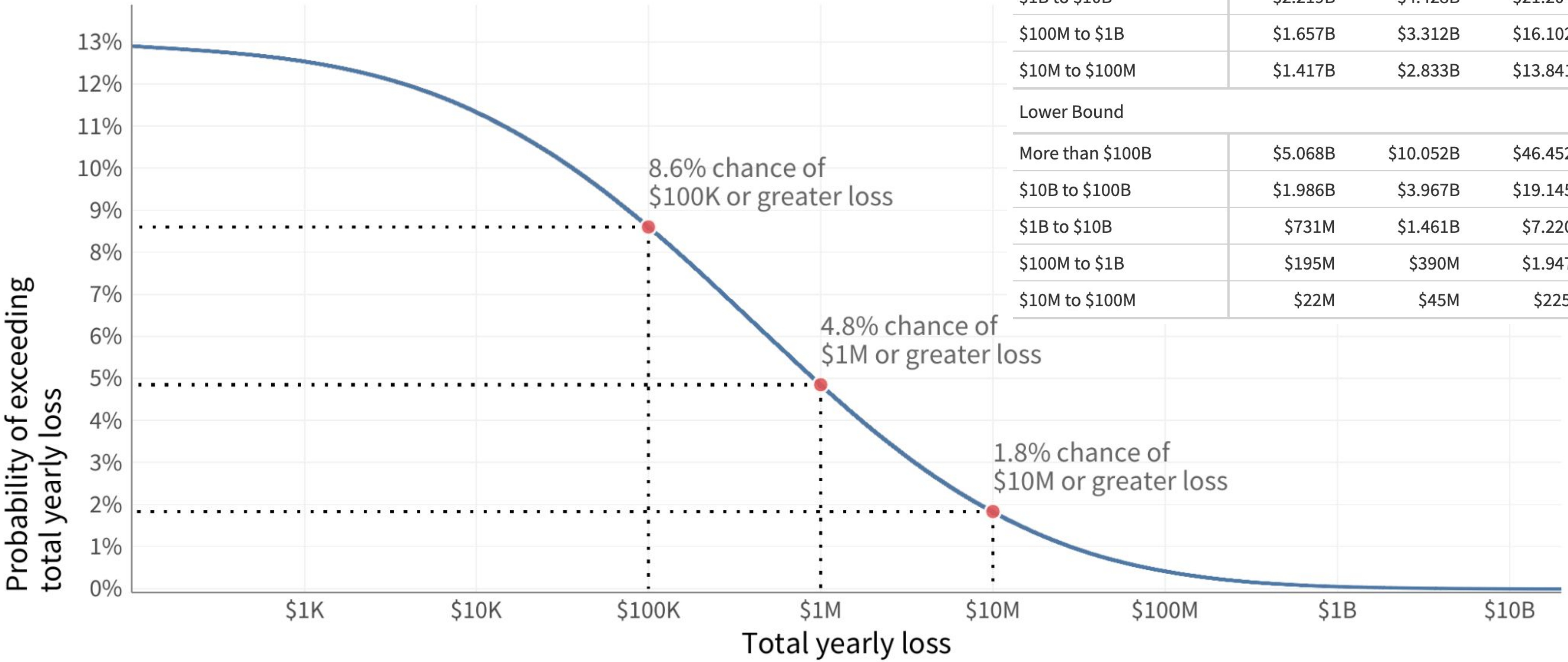


Loss parameters: Log-normal

Mean (μ)	Standard deviation (σ)
12.55949	3.068723

It’s all about the LEC…

	90%	95%	99%
Upper Bound			
More than $100B	$5.068B	$10.052B	$46.452B
$10B to $100B	$3.117B	$6.206B	$29.293B
$1B to $10B	$2.219B	$4.428B	$21.204B
$100M to $1B	$1.657B	$3.312B	$16.102B
$10M to $100M	$1.417B	$2.833B	$13.841B
Lower Bound			
More than $100B	$5.068B	$10.052B	$46.452B
$10B to $100B	$1.986B	$3.967B	$19.145B
$1B to $10B	$731M	$1.461B	$7.220B
$100M to $1B	$195M	$390M	$1.947B
$10M to $100M	$22M	$45M	$225M



Finding a Pattern of ATT&CK

IRIS 2022

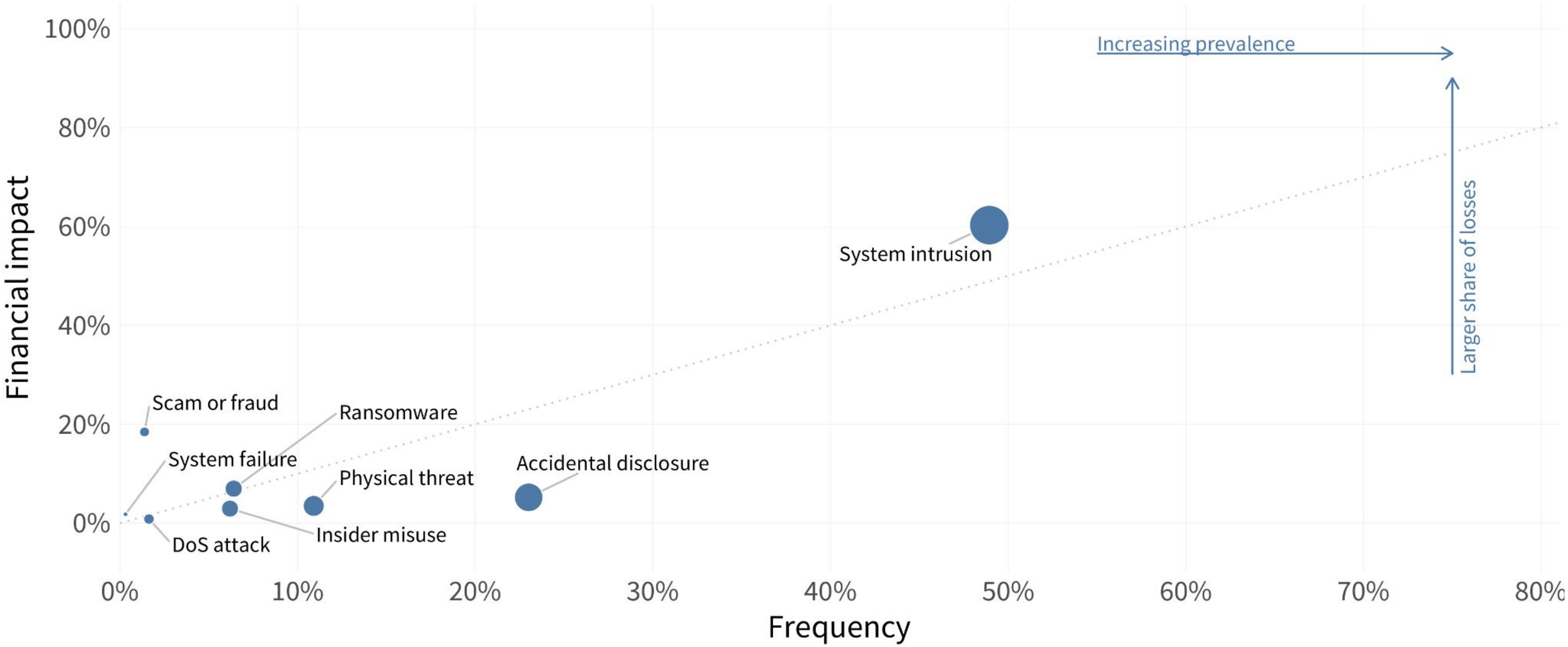
Hindsight 20/20: How can we scale?

1. The IRIS 20/20 focused mainly on LEF and LM.

2. In IRIS 20/20 Xtreme, we manually researched the 100 largest loss events and included details on threat actors and actions behind them.
    a. This is impossible for the entire dataset of >100k events.

3. So we spent 2 years on R&D to classify incident patterns, ATT&CK techniques, and VERIS actions at scale.

Incident patterns



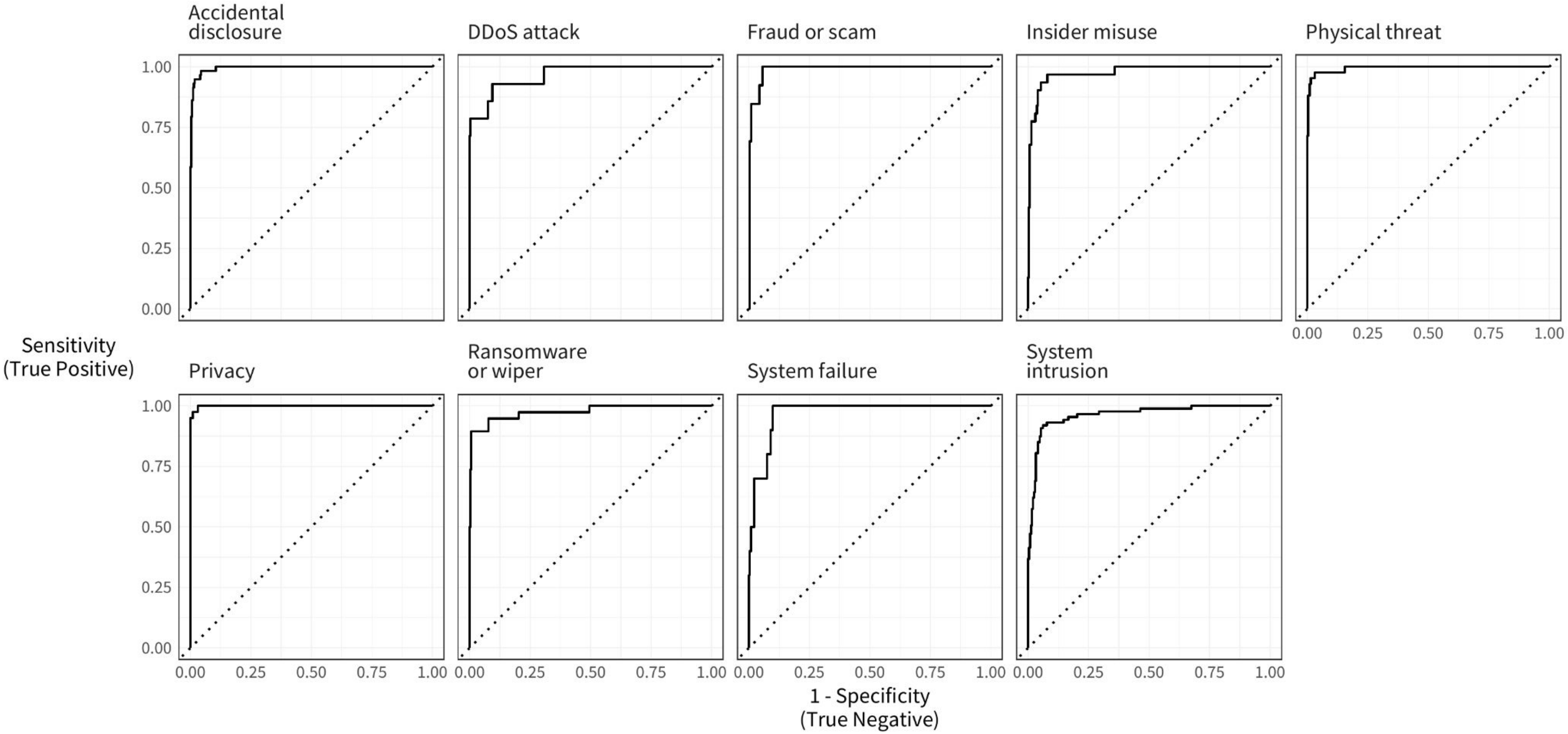
Modeling patterns at scale

1. Started with ground truth

   Hundreds of events manually labelled

2. Natural Language Process (NLP) decoding of available information on events
3. Multiple evaluations with dozens of different models
4. Evaluate performance
5. Monthly retrain with new data and new ground truth

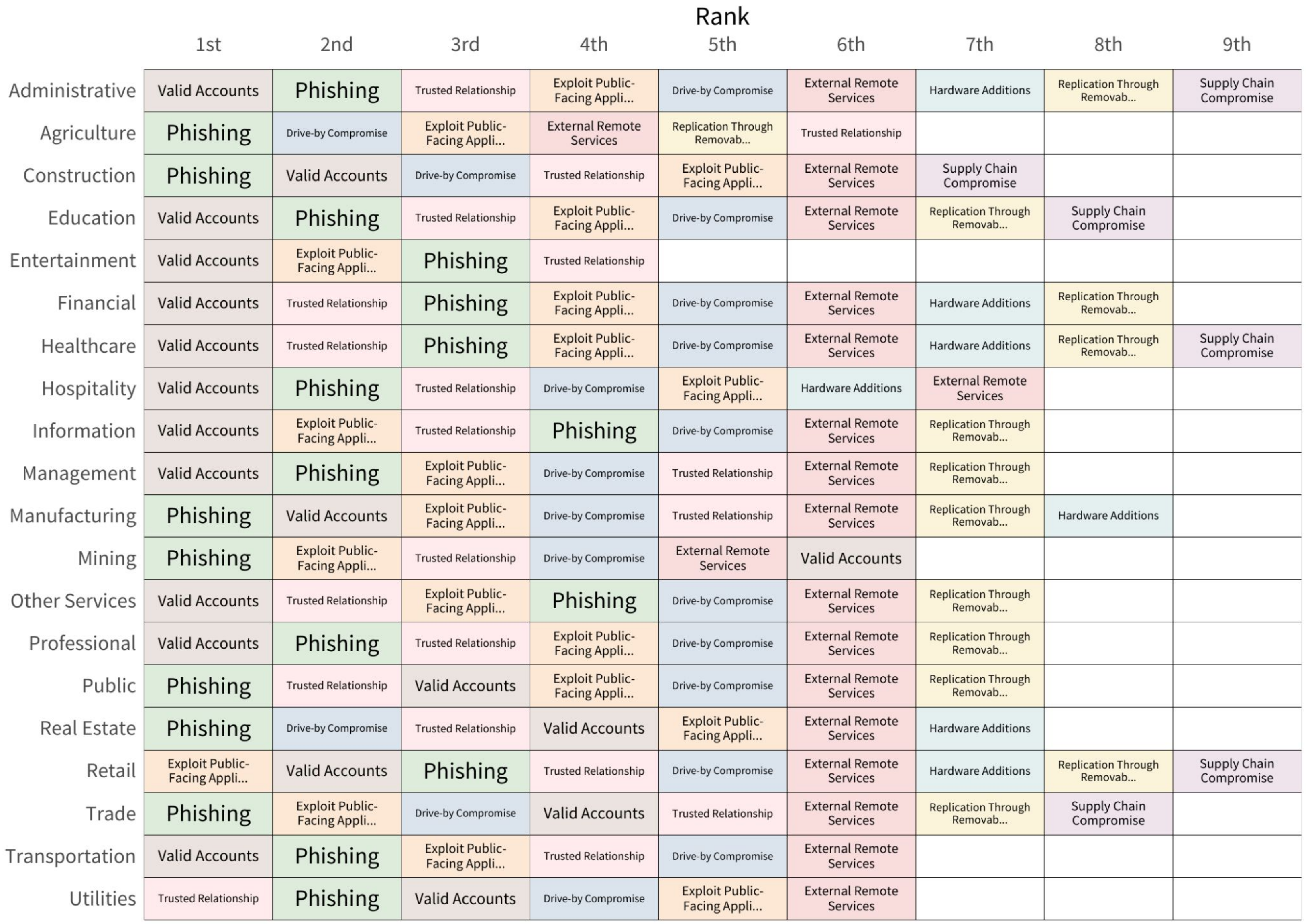
Evaluating model performance



ATT&CKing at scale

- Similar techniques to pattern recognition
- Initial ATT&CK compromise method
- Mitigating controls
- Additional lateral movement actions

Common initial access ATT&CK techniques

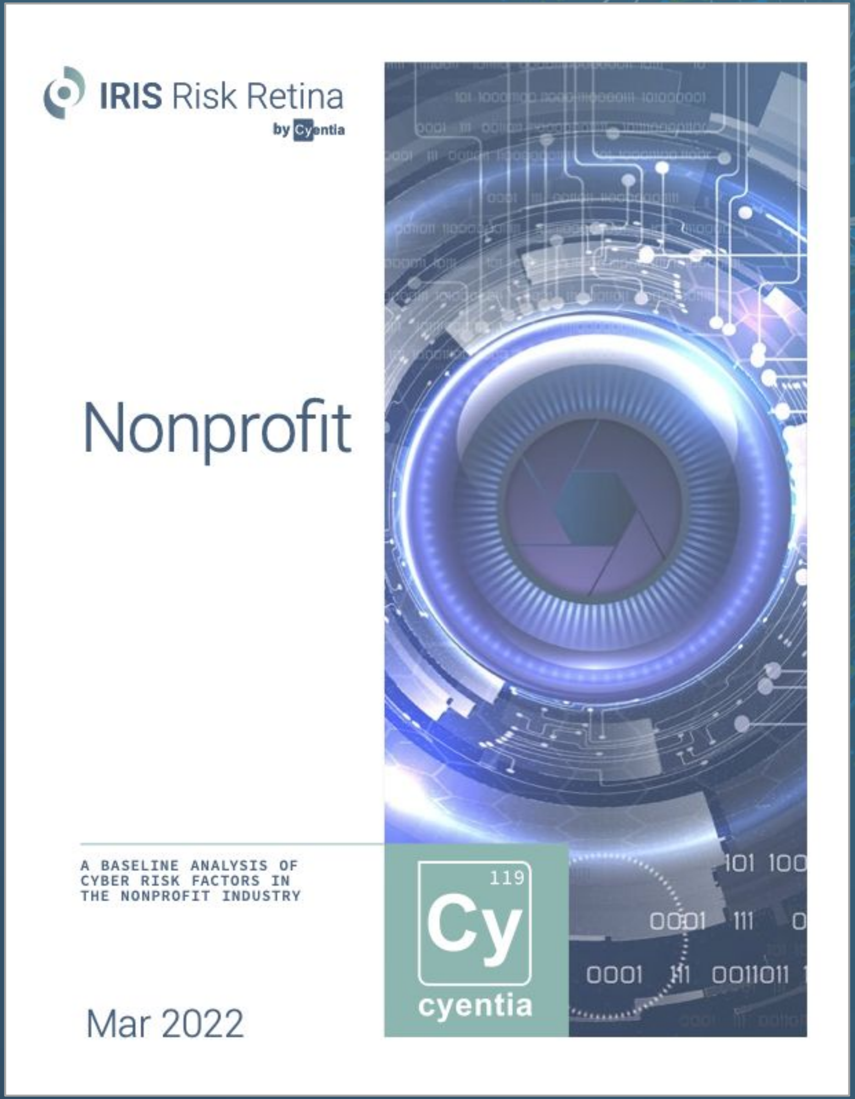


	Rank								
	1st	2nd	3rd	4th	5th	6th	7th	8th	9th
Administrative	Valid Accounts	Phishing	Trusted Relationship	Exploit Public-Facing Appli...	Drive-by Compromise	External Remote Services	Hardware Additions	Replication Through Removab...	Supply Chain Compromise
Agriculture	Phishing	Drive-by Compromise	Exploit Public-Facing Appli...	External Remote Services	Replication Through Removab...	Trusted Relationship			
Construction	Phishing	Valid Accounts	Drive-by Compromise	Trusted Relationship	Exploit Public-Facing Appli...	External Remote Services	Supply Chain Compromise		
Education	Valid Accounts	Phishing	Trusted Relationship	Exploit Public-Facing Appli...	Drive-by Compromise	External Remote Services	Replication Through Removab...	Supply Chain Compromise	
Entertainment	Valid Accounts	Exploit Public-Facing Appli...	Phishing	Trusted Relationship					
Financial	Valid Accounts	Trusted Relationship	Phishing	Exploit Public-Facing Appli...	Drive-by Compromise	External Remote Services	Hardware Additions	Replication Through Removab...	
Healthcare	Valid Accounts	Trusted Relationship	Phishing	Exploit Public-Facing Appli...	Drive-by Compromise	External Remote Services	Hardware Additions	Replication Through Removab...	Supply Chain Compromise
Hospitality	Valid Accounts	Phishing	Trusted Relationship	Drive-by Compromise	Exploit Public-Facing Appli...	Hardware Additions	External Remote Services		
Information	Valid Accounts	Exploit Public-Facing Appli...	Trusted Relationship	Phishing	Drive-by Compromise	External Remote Services	Replication Through Removab...		
Management	Valid Accounts	Phishing	Exploit Public-Facing Appli...	Drive-by Compromise	Trusted Relationship	External Remote Services	Replication Through Removab...		
Manufacturing	Phishing	Valid Accounts	Exploit Public-Facing Appli...	Drive-by Compromise	Trusted Relationship	External Remote Services	Replication Through Removab...	Hardware Additions	
Mining	Phishing	Exploit Public-Facing Appli...	Trusted Relationship	Drive-by Compromise	External Remote Services	Valid Accounts			
Other Services	Valid Accounts	Trusted Relationship	Exploit Public-Facing Appli...	Phishing	Drive-by Compromise	External Remote Services	Replication Through Removab...		
Professional	Valid Accounts	Phishing	Trusted Relationship	Exploit Public-Facing Appli...	Drive-by Compromise	External Remote Services	Replication Through Removab...		
Public	Phishing	Trusted Relationship	Valid Accounts	Exploit Public-Facing Appli...	Drive-by Compromise	External Remote Services	Replication Through Removab...		
Real Estate	Phishing	Drive-by Compromise	Trusted Relationship	Valid Accounts	Exploit Public-Facing Appli...	External Remote Services	Hardware Additions		
Retail	Exploit Public-Facing Appli...	Valid Accounts	Phishing	Trusted Relationship	Drive-by Compromise	External Remote Services	Hardware Additions	Replication Through Removab...	Supply Chain Compromise
Trade	Phishing	Exploit Public-Facing Appli...	Drive-by Compromise	Valid Accounts	Trusted Relationship	External Remote Services	Replication Through Removab...	Supply Chain Compromise	
Transportation	Valid Accounts	Phishing	Exploit Public-Facing Appli...	Trusted Relationship	Drive-by Compromise	External Remote Services			
Utilities	Trusted Relationship	Phishing	Valid Accounts	Drive-by Compromise	Exploit Public-Facing Appli...	External Remote Services			

But what about MY company?

Sorry - we can’t address all your CRQ needs in the IRIS alone

Example: Applying IRIS to a single firm for CRQ



IRIS Risk Retina

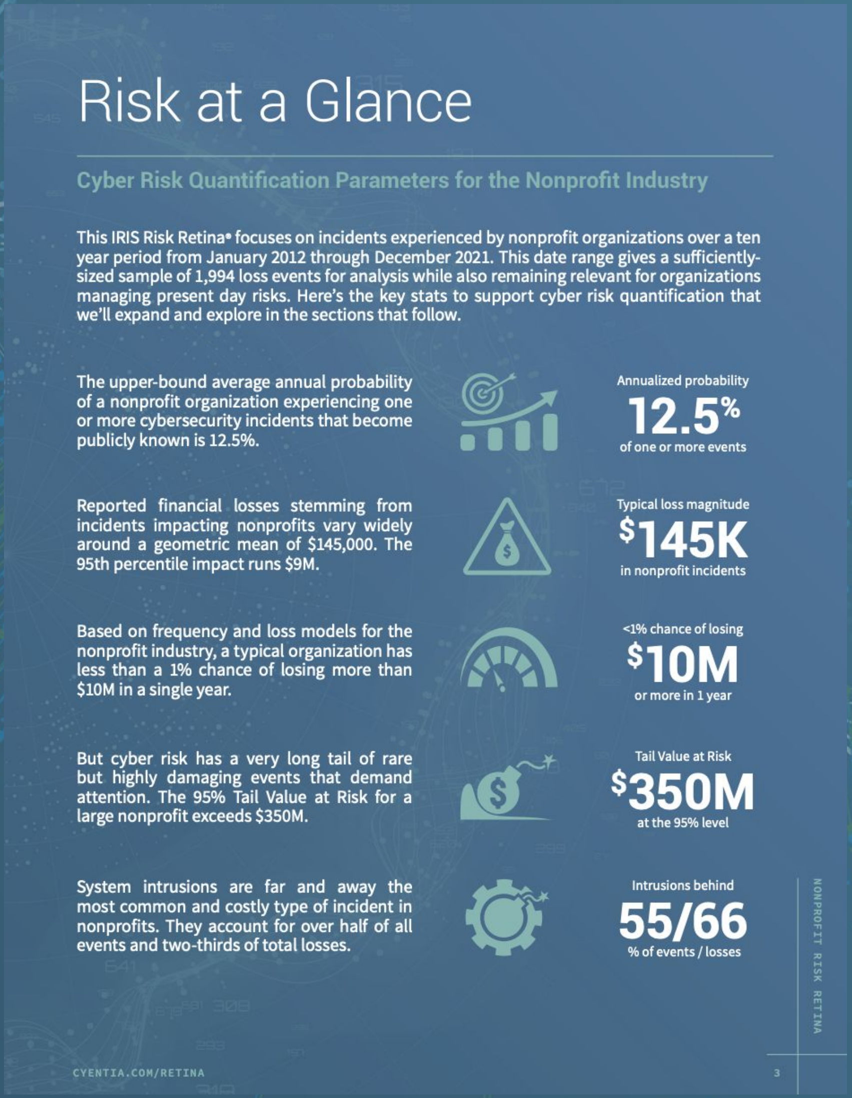
by Cyentia

Nonprofit

A BASELINE ANALYSIS OF CYBER RISK FACTORS IN THE NONPROFIT INDUSTRY

Cy 119 cyentia

Mar 2022



Risk at a Glance

Cyber Risk Quantification Parameters for the Nonprofit Industry

This IRIS Risk Retina® focuses on incidents experienced by nonprofit organizations over a ten year period from January 2012 through December 2021. This date range gives a sufficiently-sized sample of 1,994 loss events for analysis while also remaining relevant for organizations managing present day risks. Here's the key stats to support cyber risk quantification that we'll expand and explore in the sections that follow.

The upper-bound average annual probability of a nonprofit organization experiencing one or more cybersecurity incidents that become publicly known is 12.5%.

Annualized probability **12.5%** of one or more events

Reported financial losses stemming from incidents impacting nonprofits vary widely around a geometric mean of $145,000. The 95th percentile impact runs $9M.

Typical loss magnitude **$145K** in nonprofit incidents

Based on frequency and loss models for the nonprofit industry, a typical organization has less than a 1% chance of losing more than $10M in a single year.

<1% chance of losing **$10M** or more in 1 year

But cyber risk has a very long tail of rare but highly damaging events that demand attention. The 95% Tail Value at Risk for a large nonprofit exceeds $350M.

Tail Value at Risk **$350M** at the 95% level

System intrusions are far and away the most common and costly type of incident in nonprofits. They account for over half of all events and two-thirds of total losses.

Intrusions behind **55/66** % of events / losses

NONPROFIT RISK RETINA

CYENTIA.COM/RETINA

3

Download now to see exactly what a Risk Retina for your sector contains!

119 Cyentia INSTITUTE

Thank You!