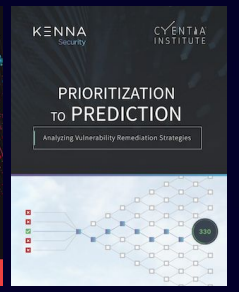
Real Data Science for Practical Risk Management

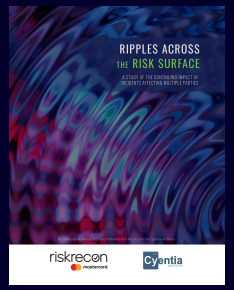
with Cyentia's IRIS Risk Retina

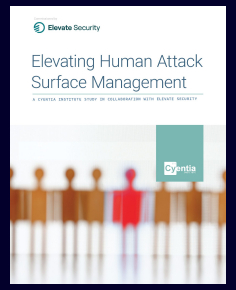
FAIR21 CONFERENCE

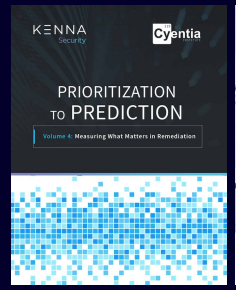
Cyentia Institute

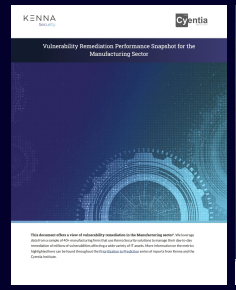
You know us from such hits as...

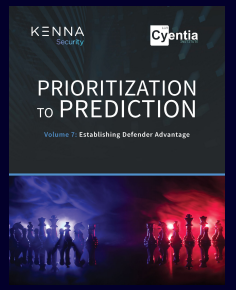


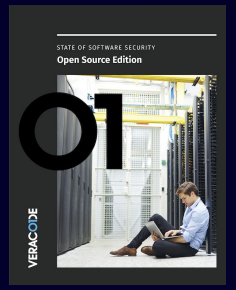


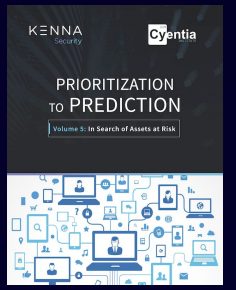


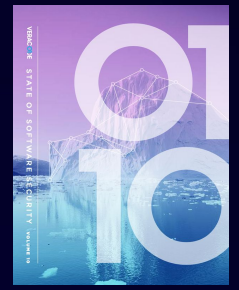


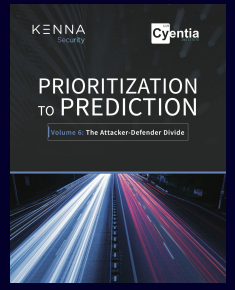


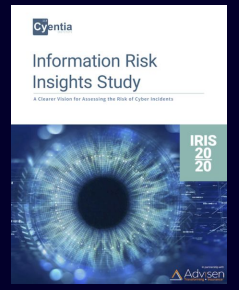


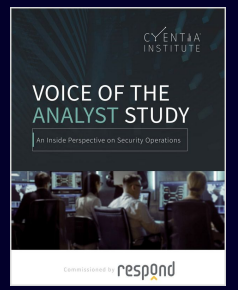


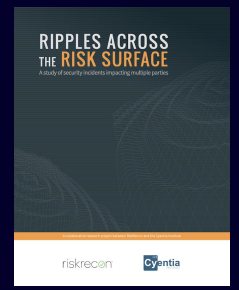


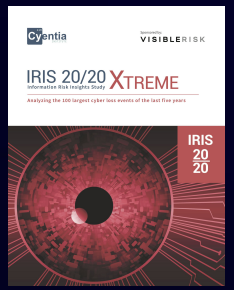


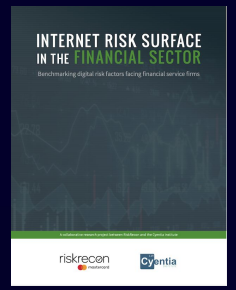


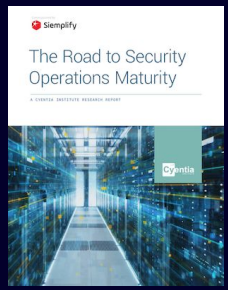


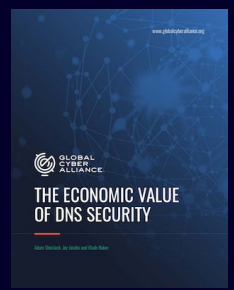


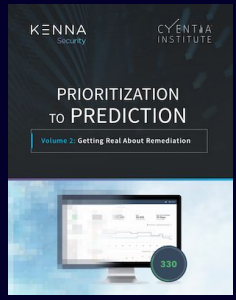






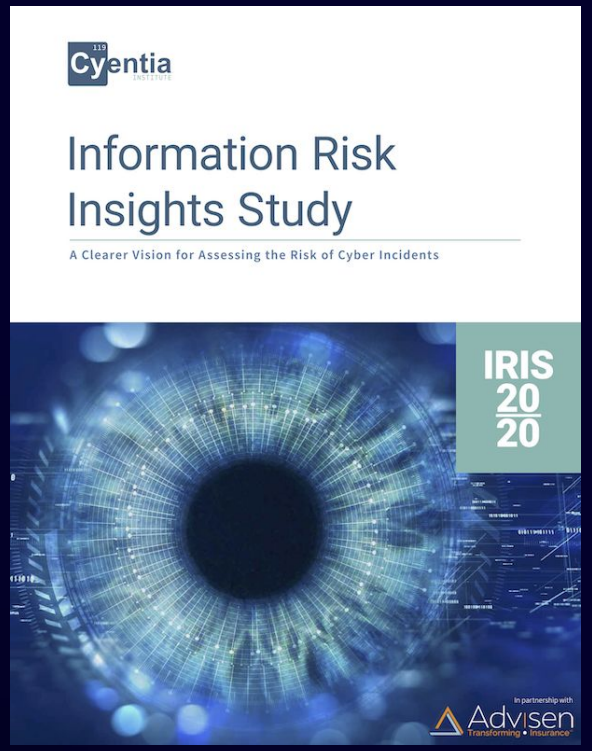


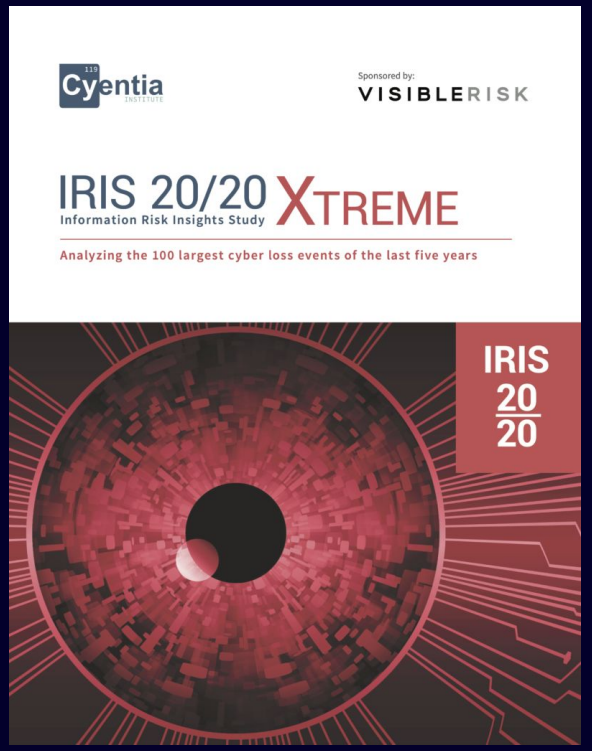




FAIR21 CONFERENCE

Information Risk Insights Studies (IRIS)

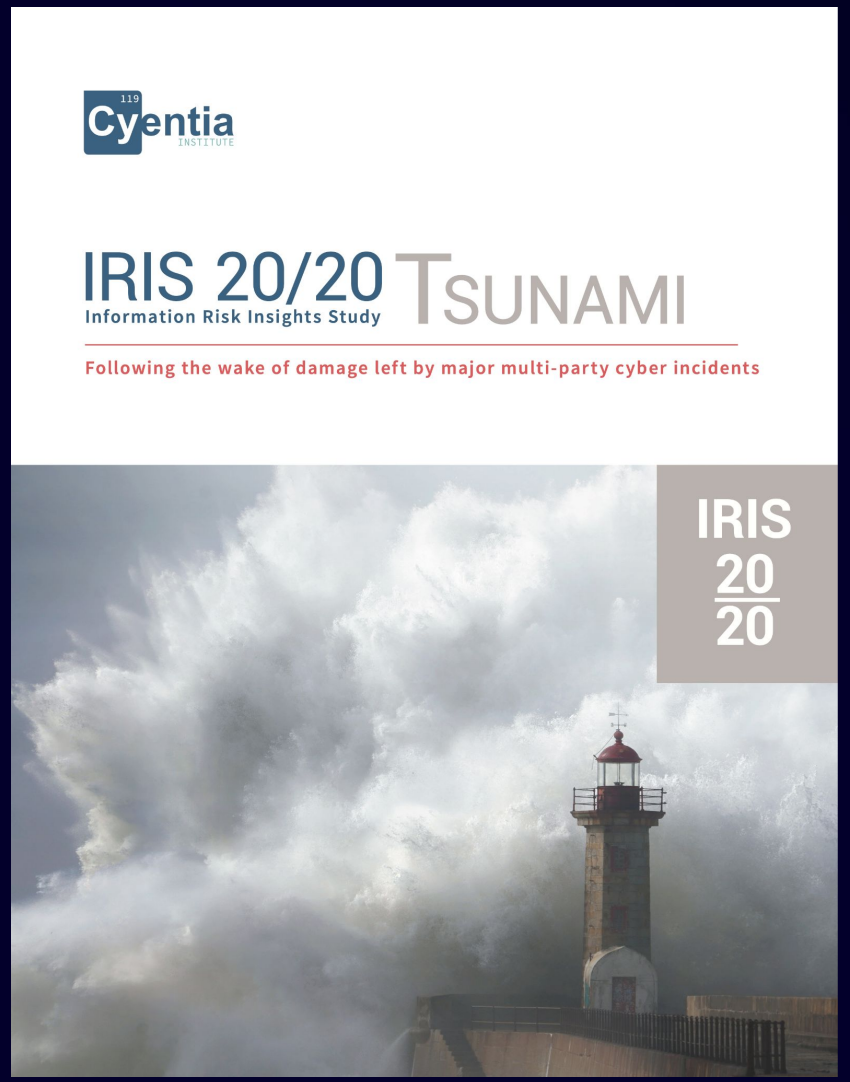




?

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

New IRIS peering into mega multi-party cyber incidents



IRIS Tsunami: Skimming the Surface

FIGURE 1: NUMBER OF SECONDARY FIRMS IMPACTED BY EXTREME MULTI-PARTY CYBER INCIDENTS

IRIS Tsunami: Skimming the Surface

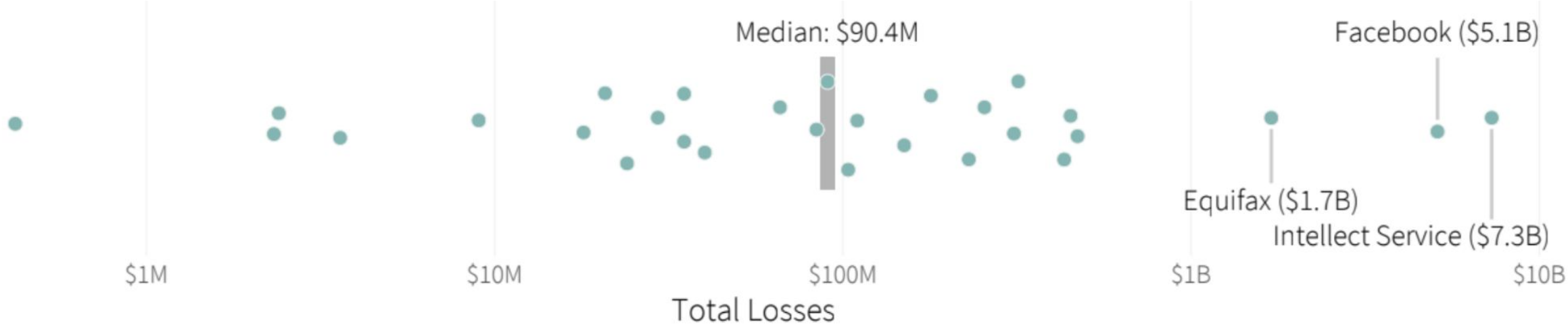


FIGURE 3: TOTAL RECORDED FINANCIAL LOSSES FOR EXTREME MULTI-PARTY CYBER INCIDENTS

IRIS Tsunami: Skimming the Surface

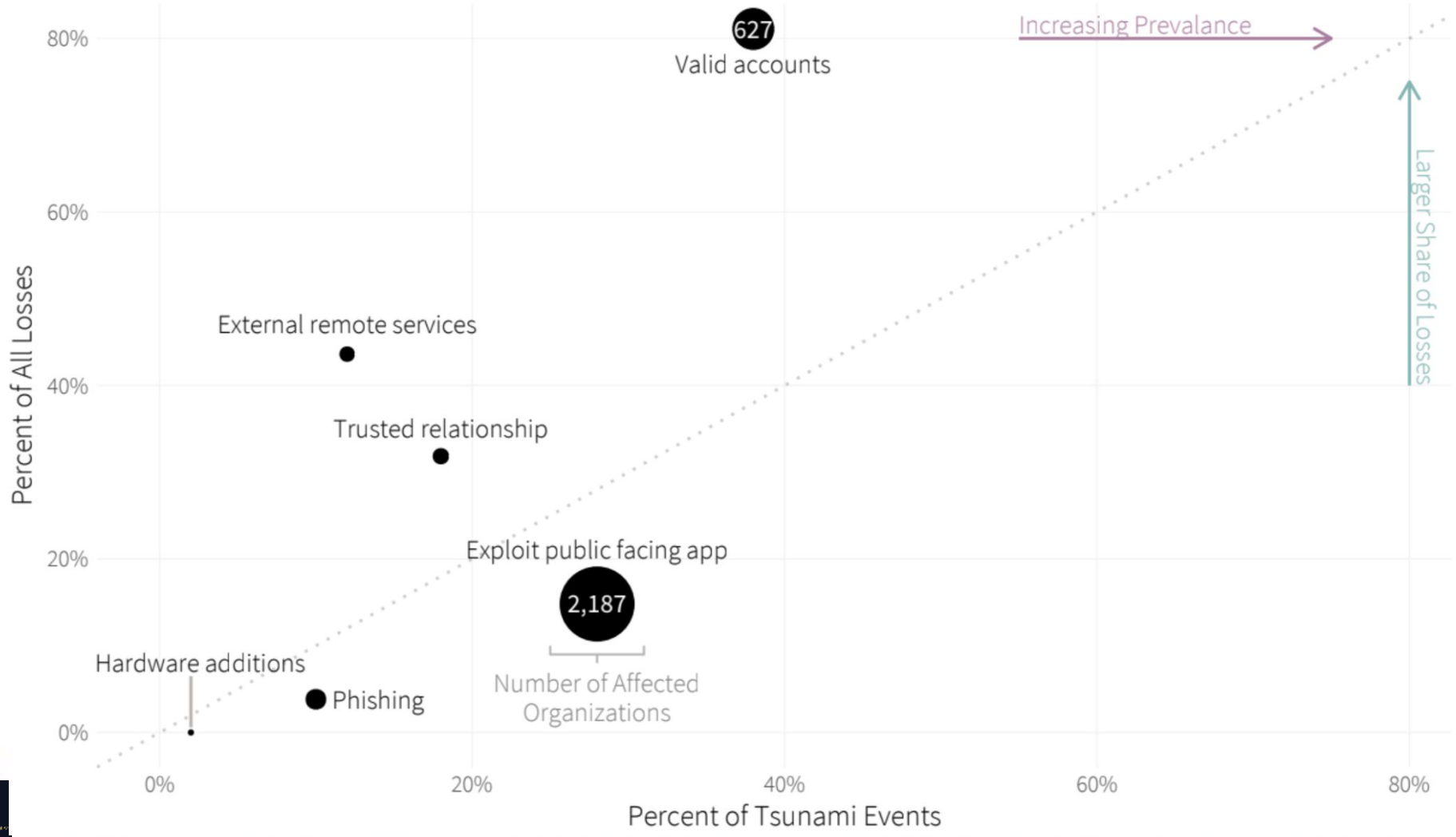


FIGURE 7: ATT&CK INITIAL ACCESS TECHNIQUES IN EXTREME MULTI-PARTY CYBER INCIDENTS

IRIS Tsunami: Skimming the Surface

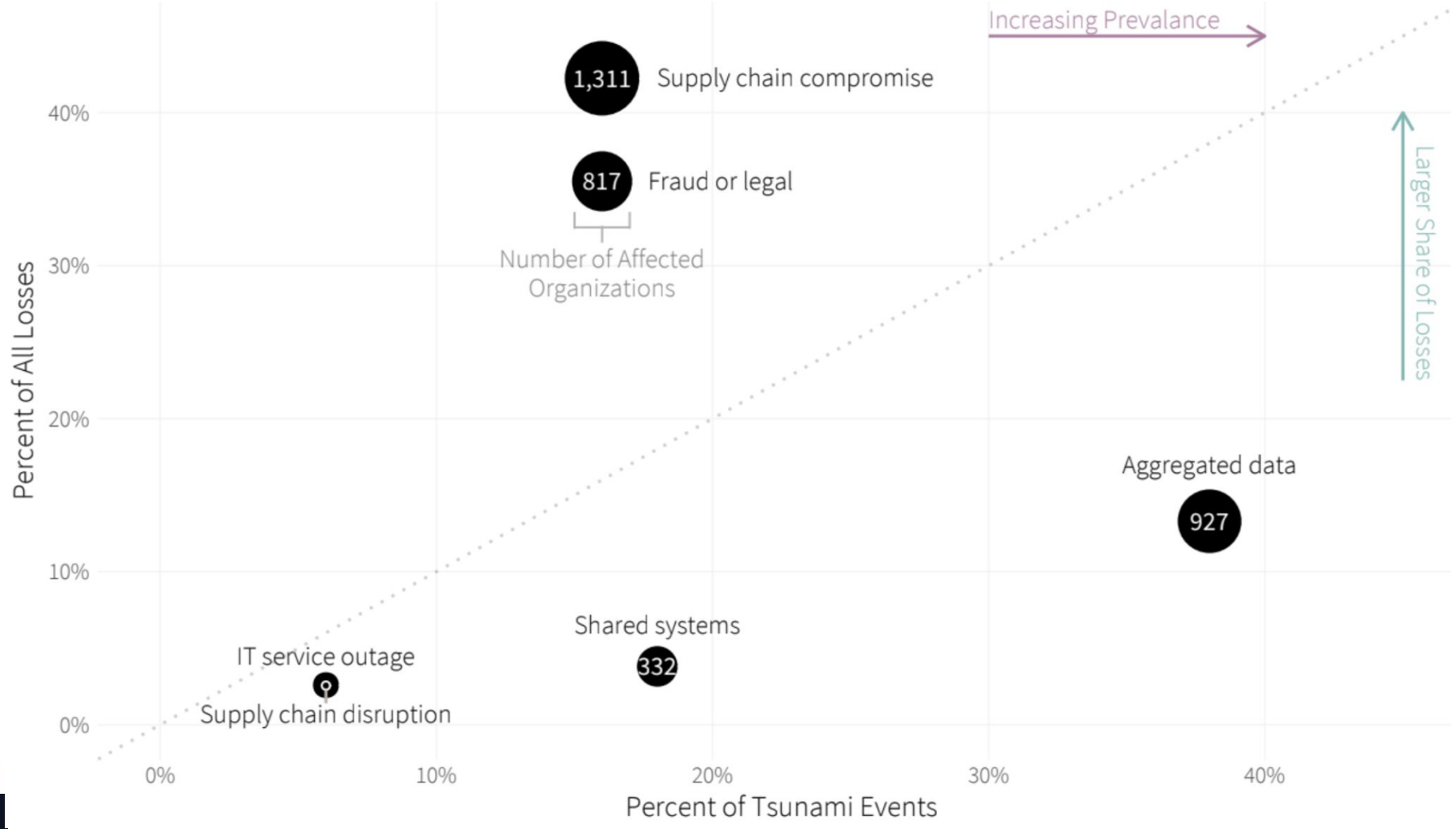


FIGURE 8: DOWNSTREAM PROPAGATION METHODS IN EXTREME MULTI-PARTY CYBER INCIDENTS

IRIS Risk Retina

by Cyentia

IRIS Risk Retina

by Cyentia

- Lack of data for estimating risk parameters is a major roadblock to adopting FAIR & other cyber risk quant methods.
- The IRIS Series aims to clear the fog of FUD surrounding cyber risk so managers see their way to better decisions.
- Risk Retina provides IRIS-style analytical reports focused on your company and the risk dimensions that matter most.
- Can be used with any risk management platform or framework.

Risk Retina Dimensions in Focus

- Multi-party incidents
  - *Ripples Across the Risk Surface*; *IRIS Tsunami*
- Extreme loss events
  - *IRIS 20/20 Xtreme*; +100 events since publication
- Industry and subsectors (e.g., Nonprofit)
- Organization size (employees and/or revenue)
- VERIS classification and scenarios
- MITRE ATT&CK mappings
- And more to come!

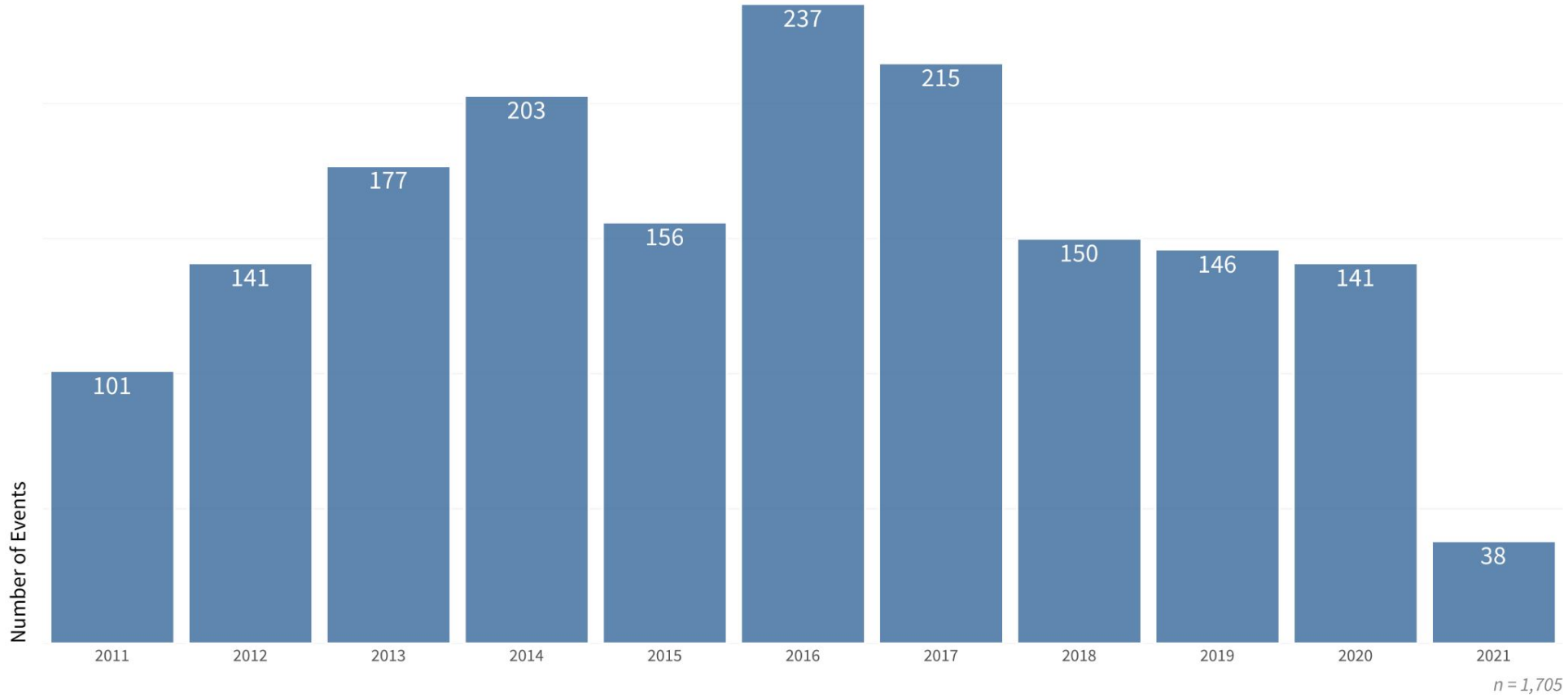
Risk Retina for the Nonprofit Sector

- Coming soon as a free public offering
- NAICS subsector 813
- Will include the risk parameters shown in the following slides (and more)

Learning to Count: Total number of events

Insight: "Organizations in our sector don't have as many incidents as Finance."

Learning to Count: Number of events over time



Insight: "At least the frequency of events doesn't appear to be increasing lately."

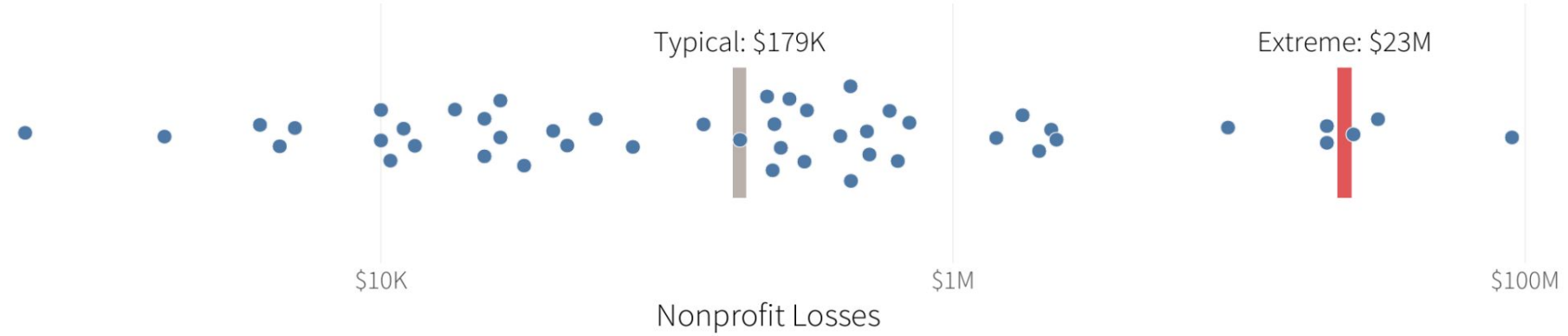
Learning to Count: Probability of occurrence

Probability of a Nonprofit Firm Experiencing a Given Number of Events Measured Against Number of Known Firms					
Number of Events					
1 or more	2 or more	3 or more	4 or more	5 or more	10 or more
0.224%	0.030%	0.006%	0.003%	0.003%	0.002%

Probability of a Nonprofit Firm Experiencing a Given Number of Events Measured Against Population of Nonprofit Firms Ever Experiencing an Event					
Number of Events					
1 or more	2 or more	3 or more	4 or more	5 or more	10 or more
12.393%	1.655%	0.355%	0.159%	0.138%	0.138%

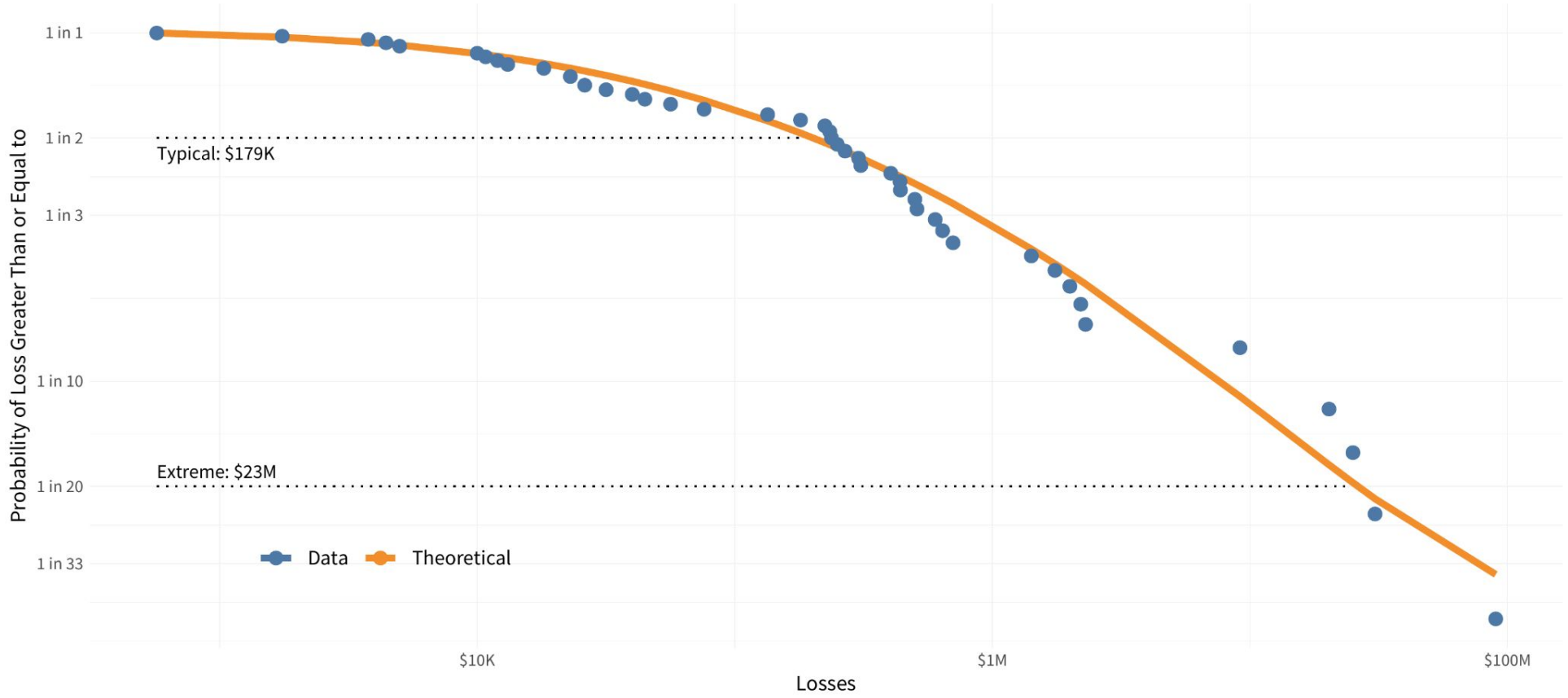
Insight: "Here's the estimated likelihood that we'll have at least x events in a year."

Understanding the Shape of Losses



Nonprofit Loss Summary						
Minimum	1st Quartile	Median	Geometric Mean	3rd Quartile	Extreme	Maximum
$570	$23K	$236K	$179K	$657K	$23M	$90M

Confirming the Quality of Parameters



Putting Frequency and Loss Magnitude Together

Risk Reporting Categories

Risk reporting categories should be...

- A manageable number of things to track/report
- Identifiable and measurable from available data
- Meaningful and compelling to the target audience
- Capture the top cyber risks to the organization
- More strategic in nature than tactical or trendy
- Differentiated based on control relevance and efficacy

IRIS Incident Patterns

DDoS attack: *Any attack intended to render online systems, applications, or networks unavailable, typically by consuming processing or bandwidth resources.*

Exposed data: *Data stores that are inadvertently left accessible to unauthorized parties, typically through misconfigurations on the part of the data custodian.*

Scam or fraud: *Incidents that primarily employ various forms of deception to defraud the victim of money, property, identity, information, etc.*

System intrusion: *All attempts to compromise systems, applications, or networks by subverting logical access controls, elevating privileges, deploying malware, etc.*

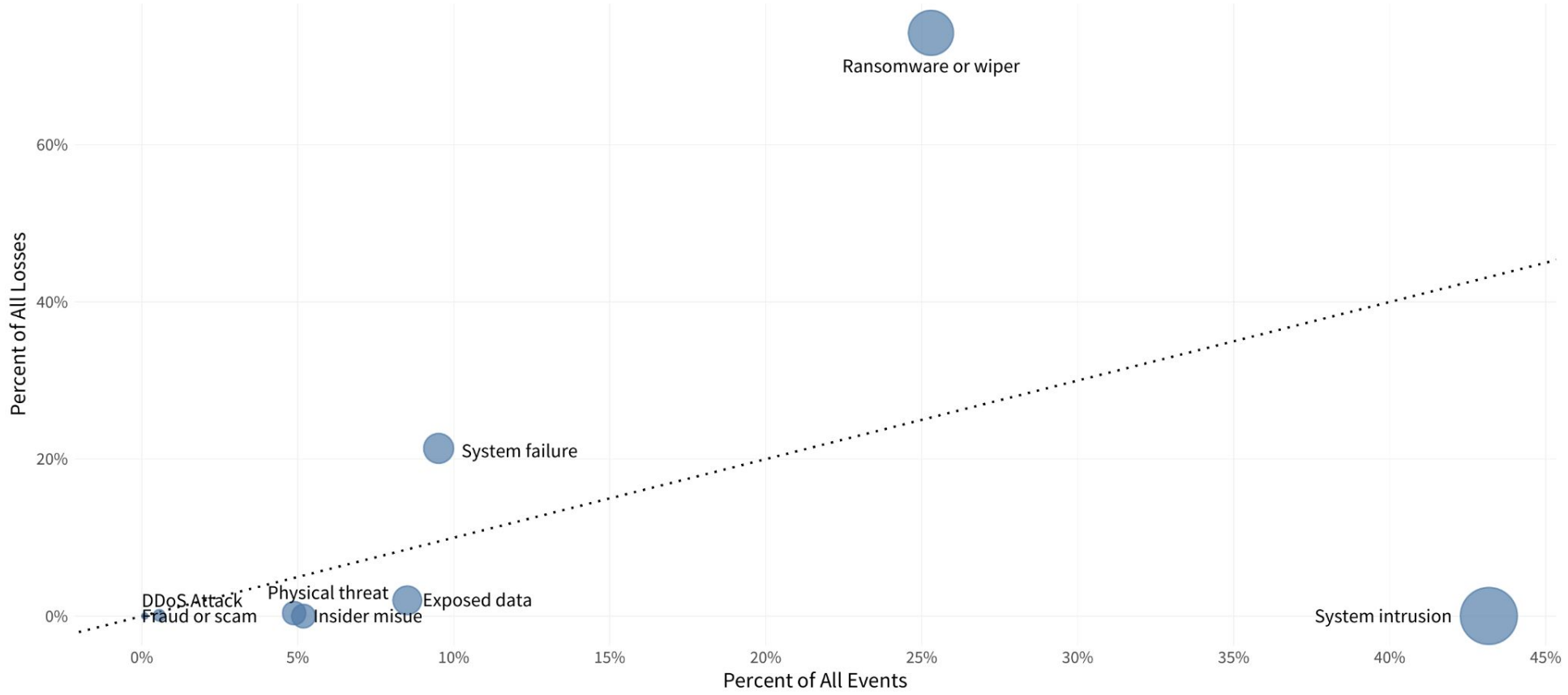
Insider misuse: *Inappropriate use of privileged access, either by an organization's own employees and contractors, or a trusted third party.*

Physical threat: *Threats that occur via a physical vector, such as device tampering, snooping, theft, loss, sabotage, assault.*

Ransomware: *The broad family of malware which seeks to encrypt data with the promise to unlock upon payment or seeks to completely eradicate data/systems without the pretense of collecting payment.*

System failure: *All unintentional service disruptions resulting from system, application, or network malfunctions or environmental hazards.*

Patterns of Activity Matter



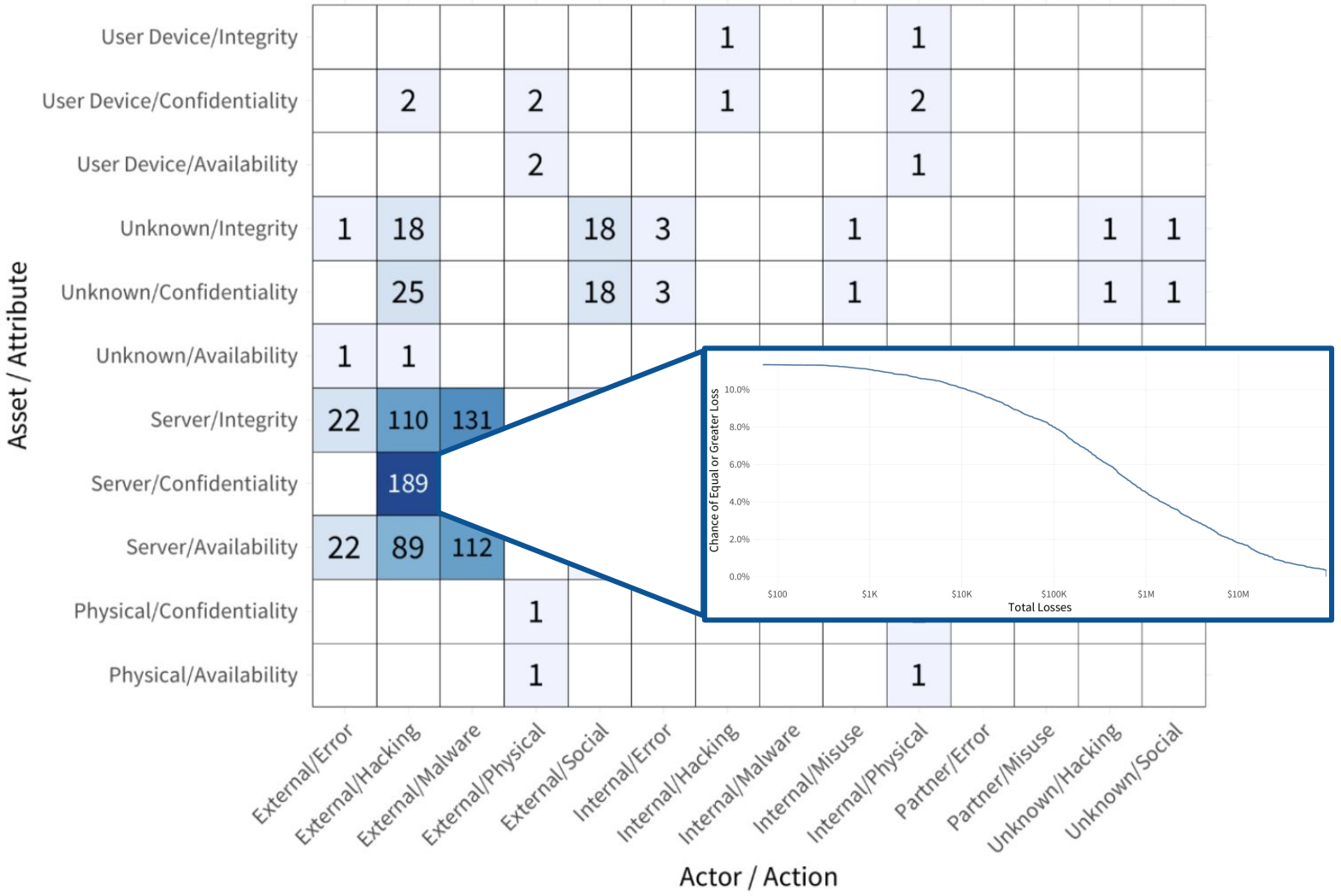
VERIS Classification & Scenarios

Going Old Skool: The VERIS A4 Threat Matrix

		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Conf	319	1		369						10	50	1			1						
	Poss																					
	Integ	323	1		353	2					3	43										
	Auth	2			16	2					3	16										
	Avail	3			4						2	1										
	Util																					
Networks	Conf	1			1												11					
	Poss																					
	Integ	1			1												11					
	Auth																					
	Avail																					
	Util																					
User Devices	Conf	214	1		174						2	4					201					
	Poss																					
	Integ	214	2		173							3					201	4				
	Auth	2			2												2	1				
	Avail				2												1					
	Util																					
Offline Data	Conf	1										87				1	1					
	Poss																					
	Integ	1																				
	Auth																					
	Avail																					
	Util																					
People	Conf							8	1													
	Poss																					
	Integ							72	24													
	Auth																					
	Avail																					
	Util																					

"*From a threat management standpoint, it is interesting that only 55 of the 630 possible threat events have a value greater than 0. This means over 90% of the threat-space was not in play at all.*" - 2011 Verizon DBIR

It’s Back! VERIS A4 Threat Matrix for Nonprofits



Get IRIS Risk Retina for your organization!

Would you like to know more?

✉️ info@cyentia.com
🔗 https://cyentia.com

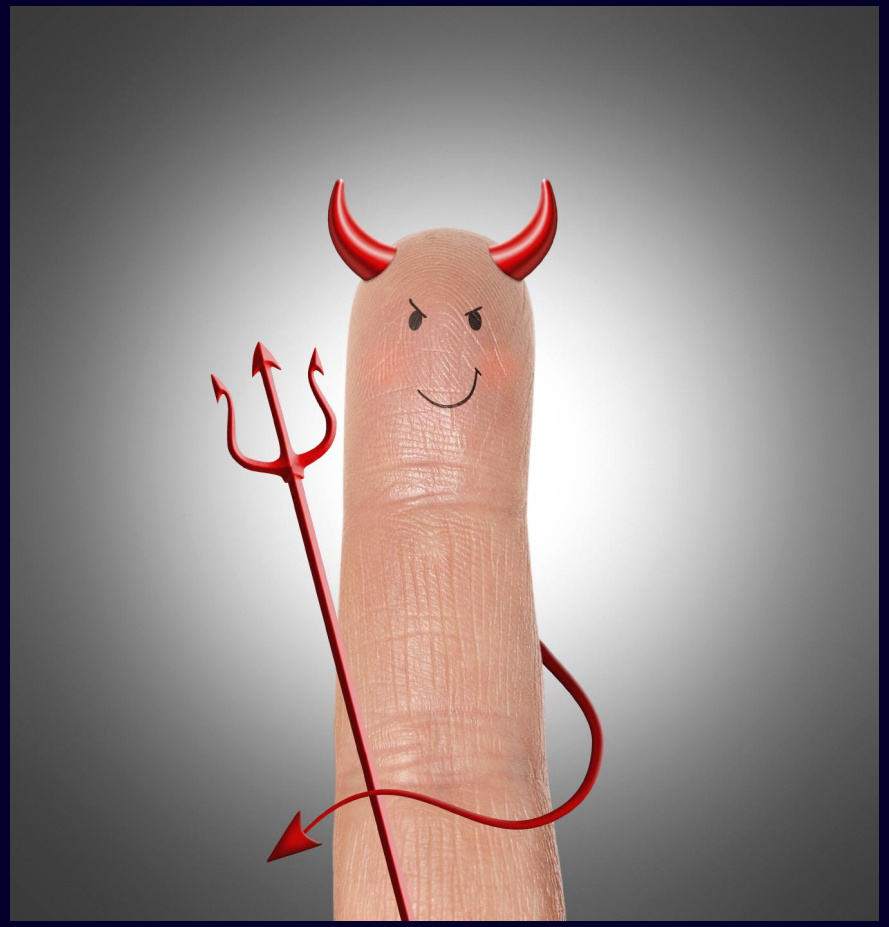
⭐ Special offer for FAIRcon attendees:

Schedule an info session by Nov 31st, mention FAIR, and get a 20% discount on an initial sector-based Retina!

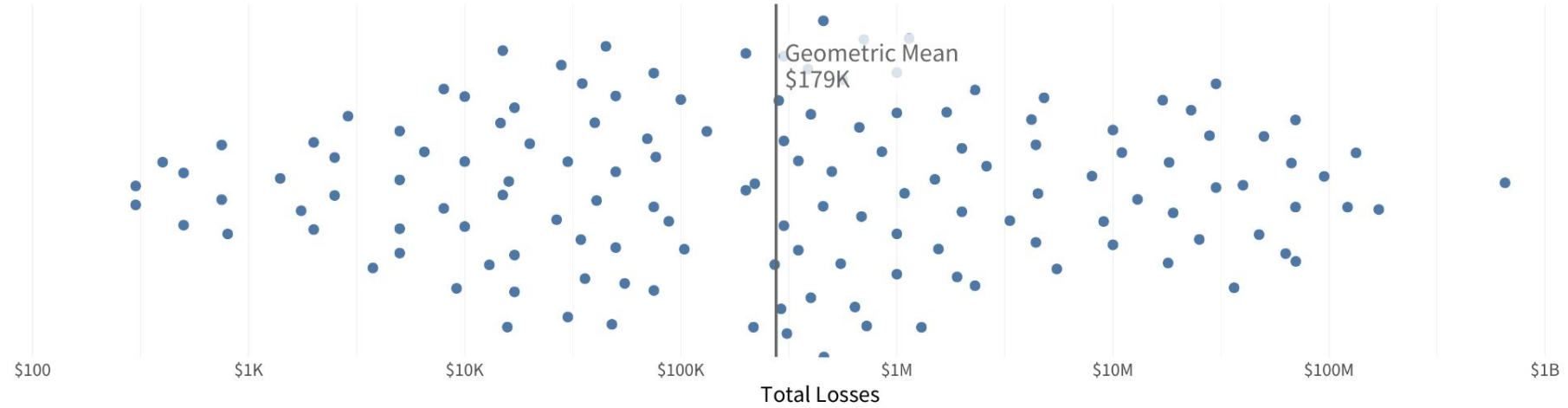
📅 https://calendly.com/cyentia/

FAIR21 CONFERENCE

Cyentia Institute



Exploring Ransomware



IRIS Risk Retina for the Nonprofit Sector

LEF, LM, LEC for select A4 scenario

- Service/Confidentiality - External/Hacking