RSAConference2019
San Francisco | March 4–8 | Moscone Center


SESSION ID: MASH-R03

# NONE of us are as smart as ALL of us

**Wade Baker, PhD**
Partner, Cyentia Institute

**Jay Jacobs**
Partner, Cyentia Institute

KENNA Security
CYENTIA INSTITUTE
PRIORITIZATION TO PREDICTION
Volume 2: Getting Real About Remediation
330

GLOBAL CYBER ALLIANCE
MEASURING THE IMPACT OF DMARC'S PART IN PREVENTING BUSINESS EMAIL COMPROMISE
Adam Shostack, Jay Jacobs and Wade Baker
WWW.GLOBALCYBERALLIANCE.ORG

CYBER BALANCE SHEET | 2018 REPORT
Finding the balance between the business of security and the security of the business.

KENNA Security
CYENTIA INSTITUTE
PRIORITIZATION TO PREDICTION
Analyzing Vulnerability Remediation Strategies

CYBRARY
DECLASSIFIED
UNRAVELING THE CYBER SKILLS GAP & TALENT SHORTAGE
2018
IN COLLABORATION WITH: CYENTIA INSTITUTE

STATE OF SOFTWARE SECURITY
VOLUME 9
ca | VERACODE

STRIKING SECURITY GOLD
Uncovering hidden insights in a decade's worth of RSA Conference abstracts.
As the premier security conference in the world, RSA Conference offers an excellent lens through which to study the topics and trends within our industry. The Conference's slogan of "Where the World Talks Security" shows that's not just an accident; it's the goal.
But what exactly do we talk about when we talk "security?" That's the question we seek to answer in this report, which has its roots in a similar question asked by an eight-year-old daughter two and a half years ago: "What's the RSA Conference about, Daddy?" That root sprouted into a four-part blog series and a panel discussion a year later where we analyzed 25 years of session titles in honor of the 25th anniversary of RSA Conference.
To really study the question, however, titles provide limited value. They're often created to grab attention rather than impart information. Call for Paper (CFP) submissions, by comparison, are a veritable goldmine of details and insight about the sessions just waiting to mined. Once again, RSA Conference was kind enough to supply the ore for our digital pickaxes. Did we strike gold and unearth valuable nuggets of insight about our industry? You'll have to read on to find out.
CYENTIA INSTITUTE
RSAConference | Where the world talks security

INTERNET RISK SURFACE REPORT PREVIEW
riskrecon in partnership with Cyentia
The Internet Risk Surface Report is a new research collaboration between RiskRecon and the Cyentia Institute. As the name implies, the focus of this initiative is to map, measure, and ultimately manage risk associated with the Internet-facing assets of a firm and its partners. This document previews some findings from the upcoming report.
A major challenge in measuring the risk surface of organizations stems from the fragmented nature of that surface across the Internet. This is particularly apparent in external assets, as the diagram below depicts. In it, we see heavy (yet varied) cloud dependency across all industries. A lack of clear visibility into all assets—wherever they're hosted—means a lack of visibility into a firm's true risk posture, as we will demonstrate in the following pages.
Information
Manufacturing
Prof. Services
Finance
Admin/Logistics
Hospitality
Retail/Wholesale
Real Estate
Education
Flows show the distribution of cloud-hosted assets by industry to the top providers.
Amazon
RISKRECON RISK SURFA

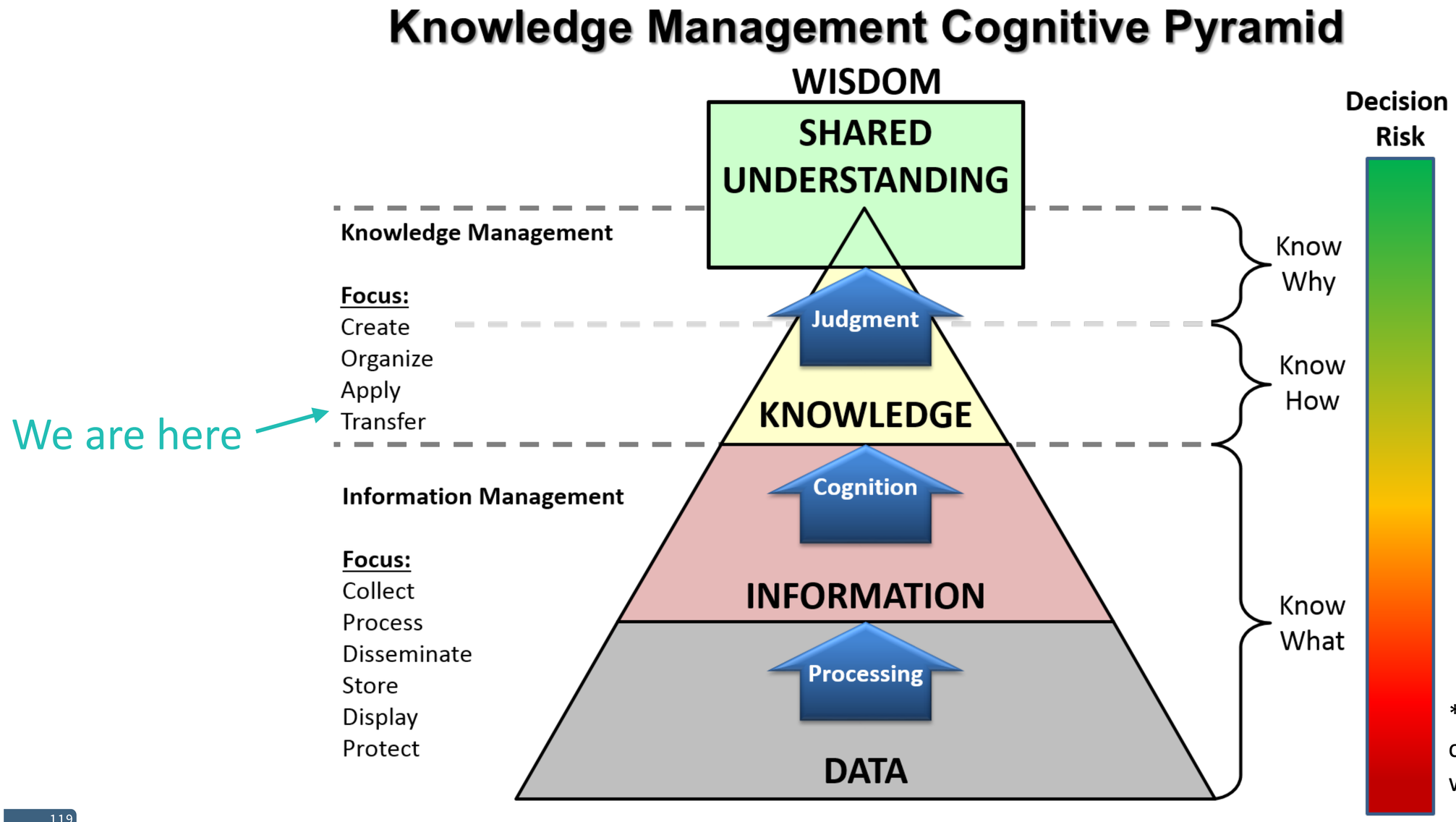
INSTITUTE
VOICE OF THE ANALYST STUDY
An Inside Perspective on Security Operations
Commissioned by respond

CYBER BALANCE SHEET
THE 2017 REPORT
5,096,300
14,020,000
9,107,700
60,400
Sponsored by FOCAL POINT DATA RISK

# The basis for this talk

- Once upon a time, our industry lacked data
- We no longer lack data; we're drowning in it
- Making sense of that data is now our challenge
  - quality, coherence, synthesis, inference, etc.
- **How to we turn abundant data into better decisions?**

# What do you mean by "data"?




*Apologies for the 90s-era clip art, but why recreate the wheel--er--pyramid?

Source: https://en.wikipedia.org/wiki/File:KM_Pyramid_Adaptation.png

# Toward "Shared Understanding"…

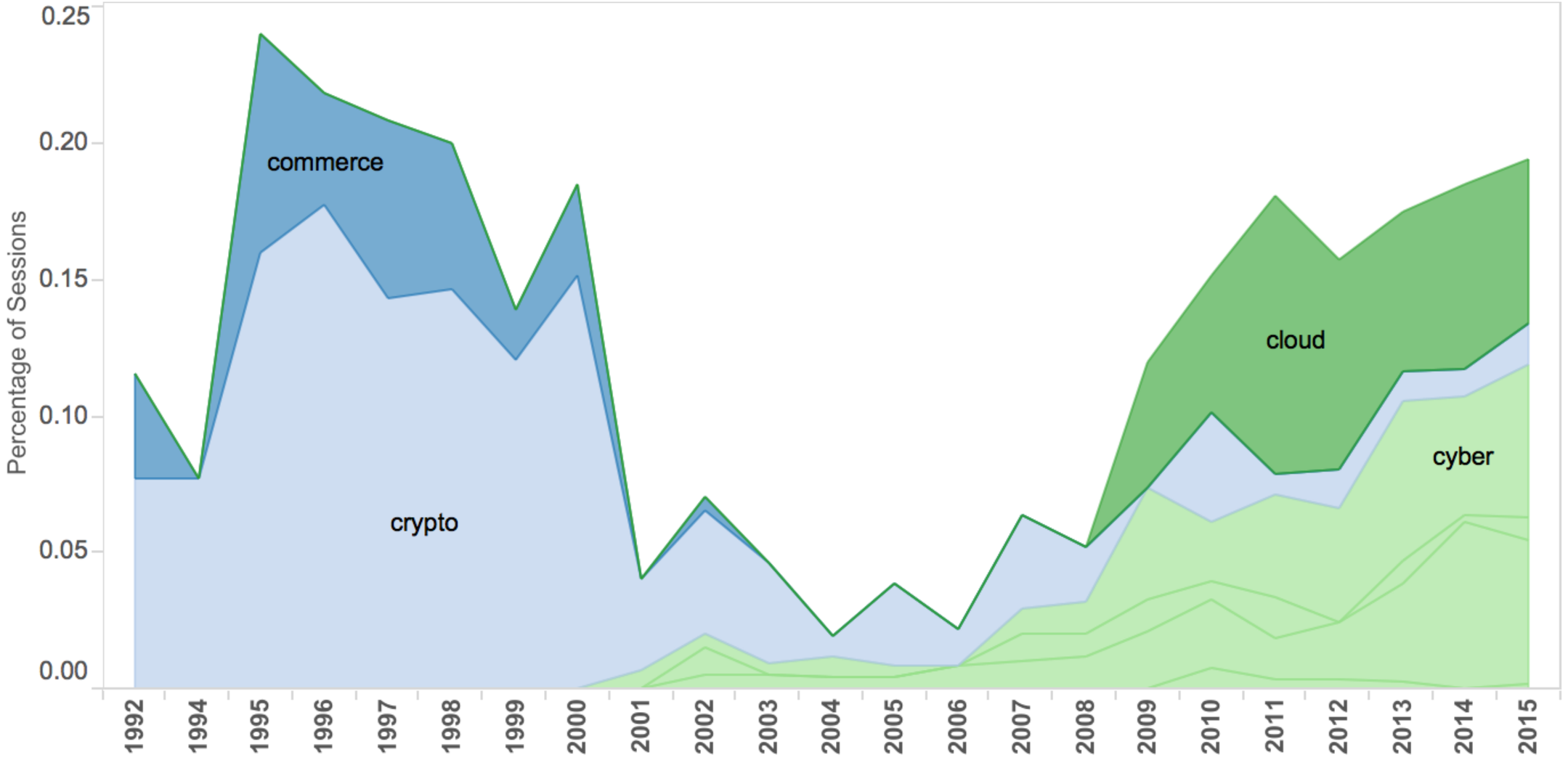
- …at the RSA Conference
- …in industry reports.
- …in meta-analysis
- …in original research

How do these help us "climb the pyramid”
toward greater shared understanding?

RSAConference2019

# Finding Shared Understanding at the RSA Conference

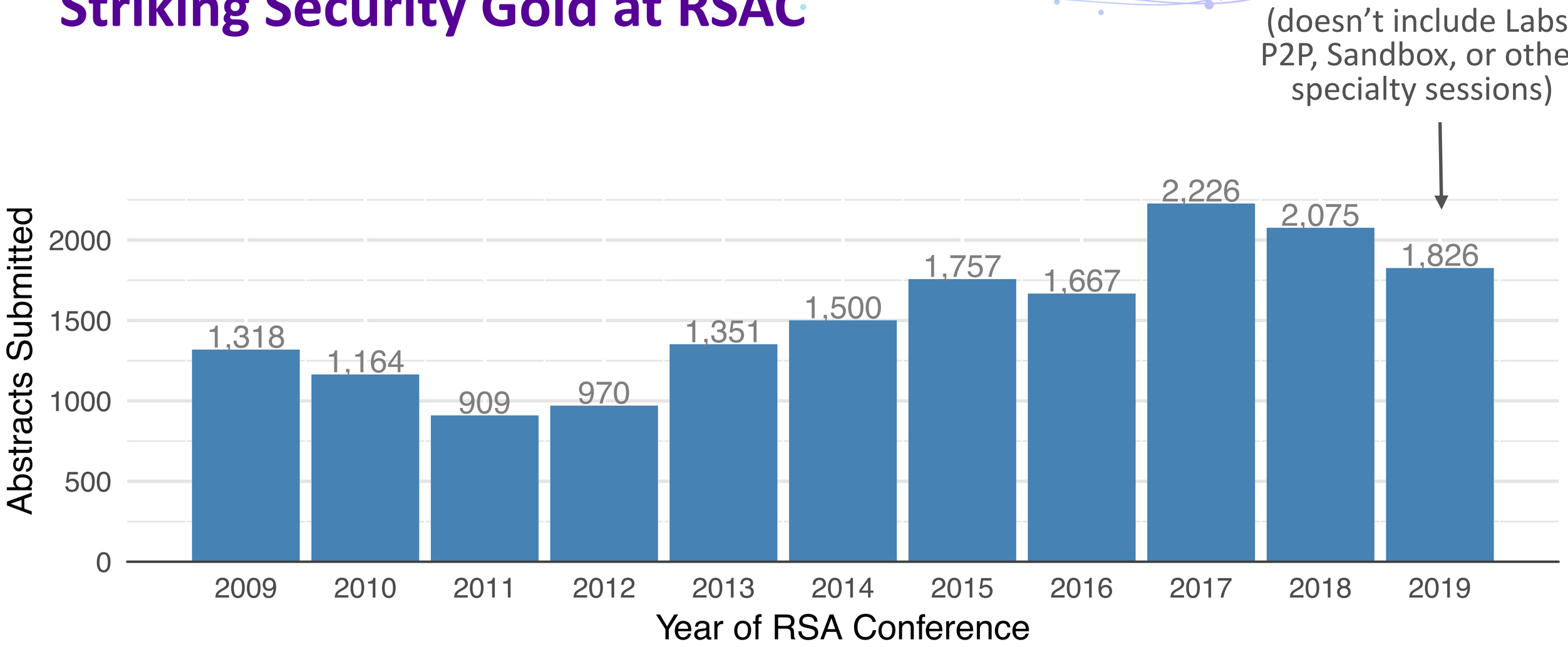
# 25 years of titles



# Making sense of the RSA Conference

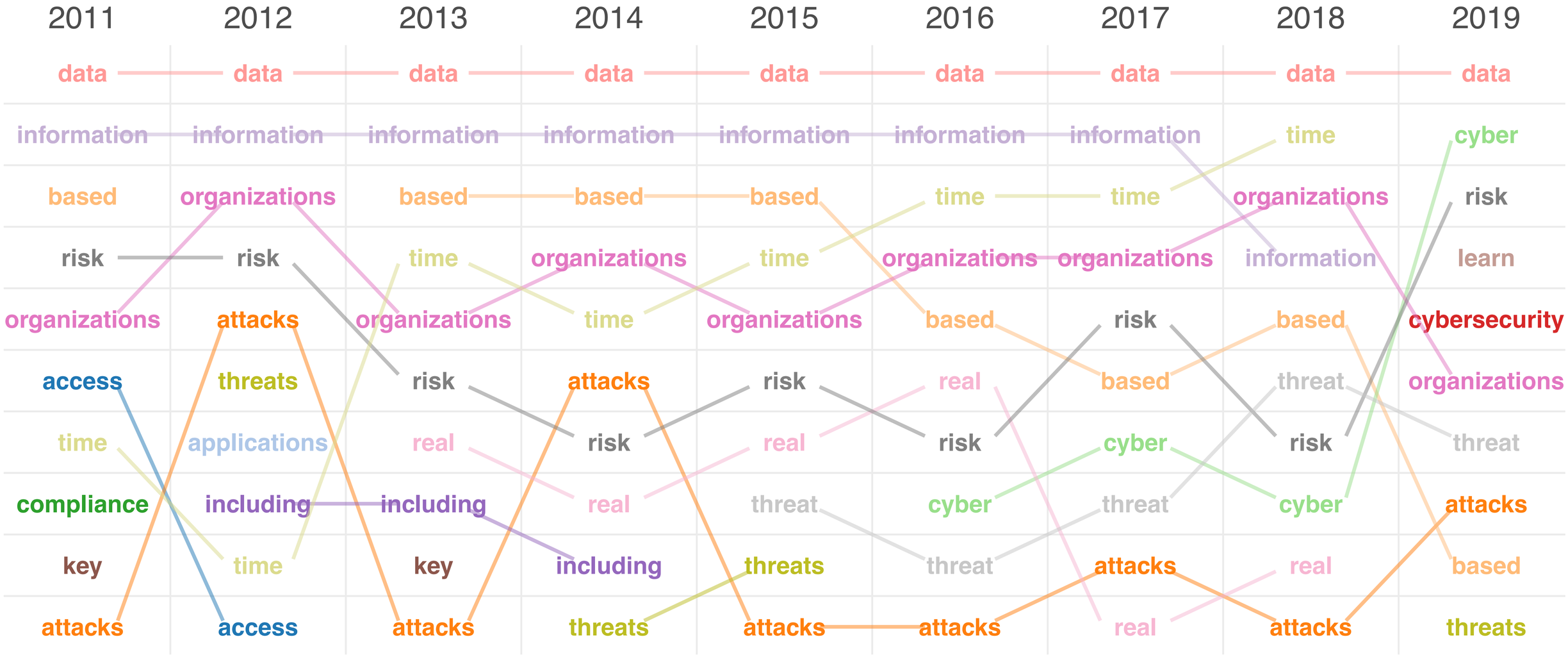
- The slogan of the RSA Conference is “Where the World Talks Security.” But have you ever wondered “how” the world talks about security?
- This report mines a decade’s worth (~15,000) of CFP submissions to help answer that question.
- Updated for this talk with 2019 CFPs!

# Striking Security Gold at RSAC




*Source: Cyentia Institute with data from RSA Conference*

# Striking Security Gold at RSAC



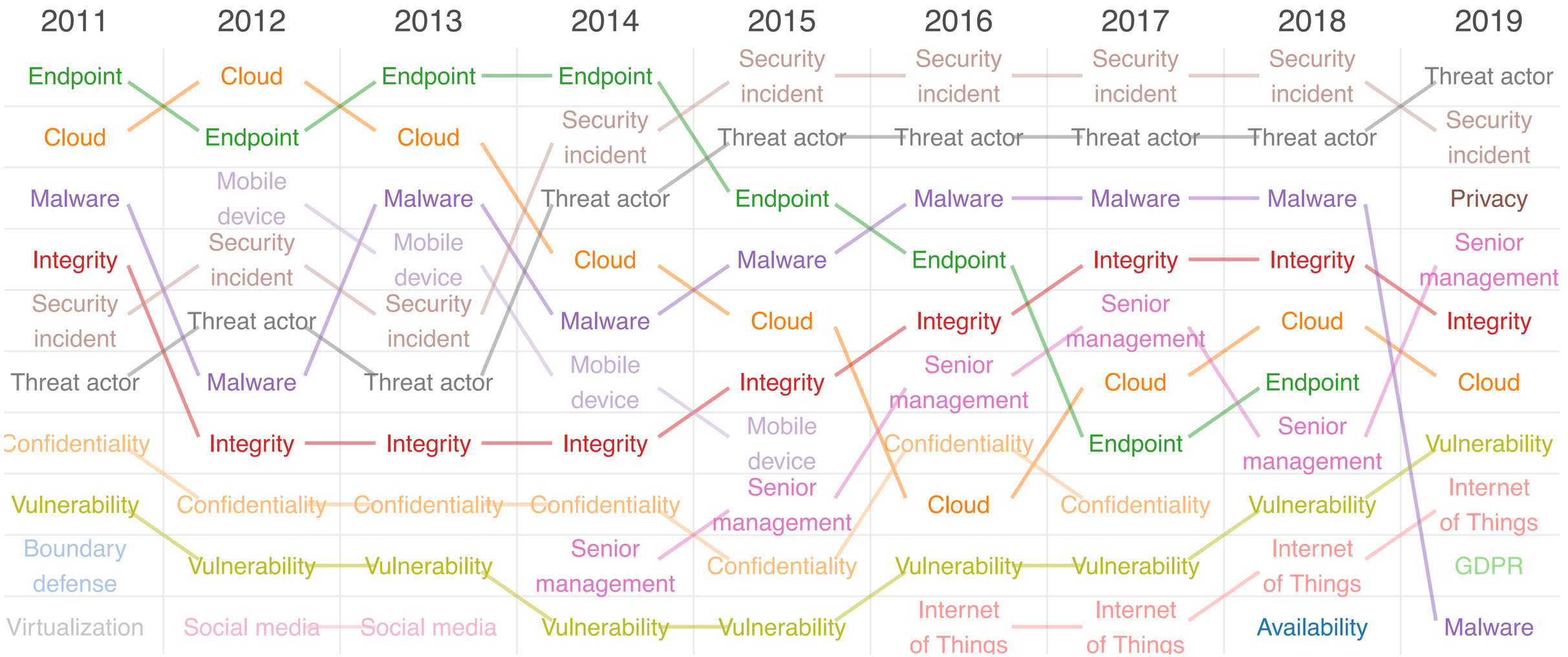

*Source: Cyentia Institute with data from RSA Conference*

# Striking Security Gold at RSAC

| 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|
| data | real–world | BYOD | APT | BYOD | IoT | IoT | IoT | IoT |
| risk | real–time | tablet | BYOD | IoT | threat actors | ransomware | ransomware | GDPR |
| organizations | cloud–based | APT | security analytics | security analytics | BYOD | devops | GDPR | blockchain |
| access | third–party | anti–virus | mobile apps | threat actors | security analytics | threat actors | iot devices | devops |
| compliance | in–depth | MDM | software–defined | home depot | kill chain | kill chain | devops | devsecops |
| key | high–profile | iOS | MDM | snowden | devops | GDPR | blockchain | ransomware |
| attacks | real–life | stuxnet | iOS | software–defined | OPM | blockchain | equifax | artifical intelligence |
| applications | Epsilon | Flame | stuxnet | data science | software–defined | cyber insurance | wannacry | cryptocurrency |
| control | end–user | mobile apps | tablets | devops | NIST CSF | security analytics | threat hunting | digital transformation |
| process | enterprise–wide | advanced malware | prism | heartbleed | iot security | NIST CSF | bitcoin | women |
| enterprise | zero–day | kill chain | advanced malware | kill chain | anthem | dark web | deep learning | containers |
| environment | cost–effective | software–defined | dropbox | ransomware | dark web | bitcoin | devsecops | consumer privacy |

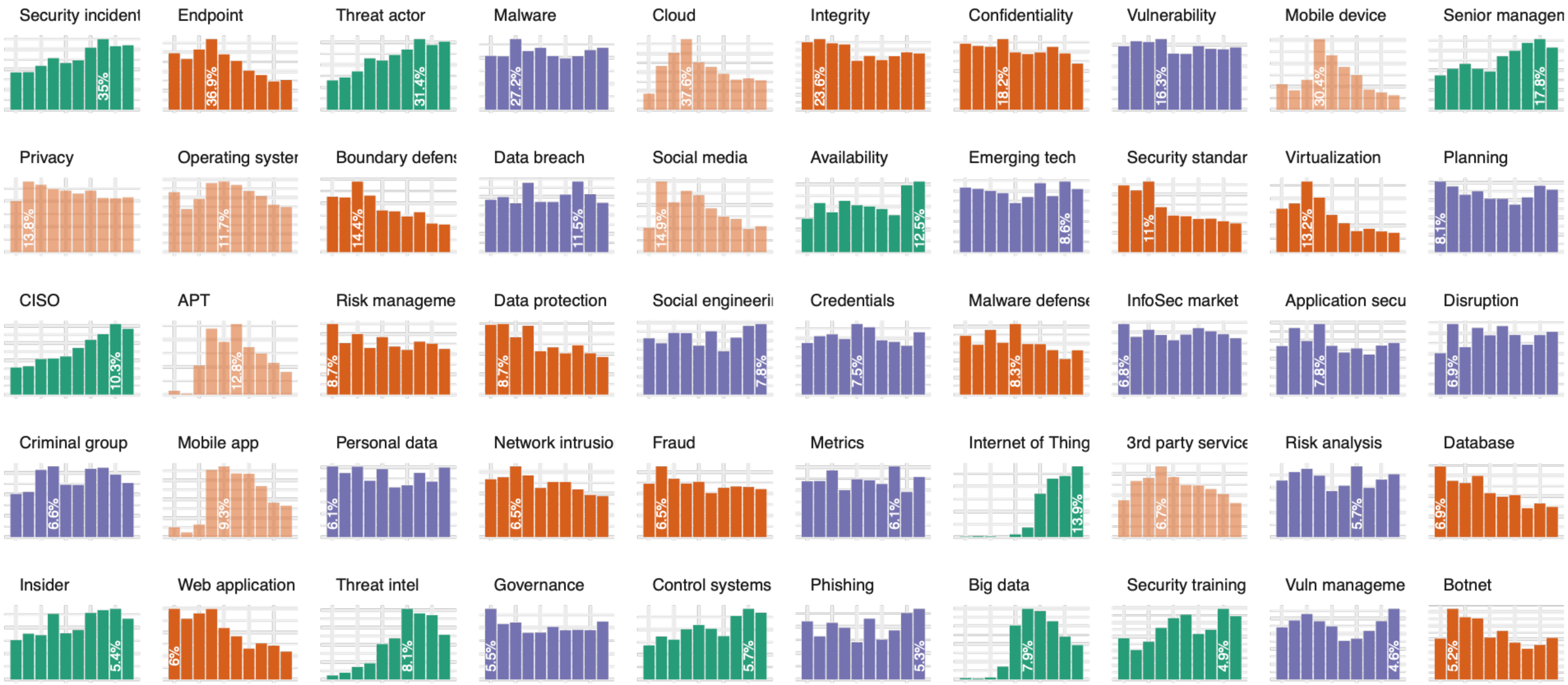
*Source: Cyentia Institute with data from RSA Conference*

# Striking Security Gold at RSAC

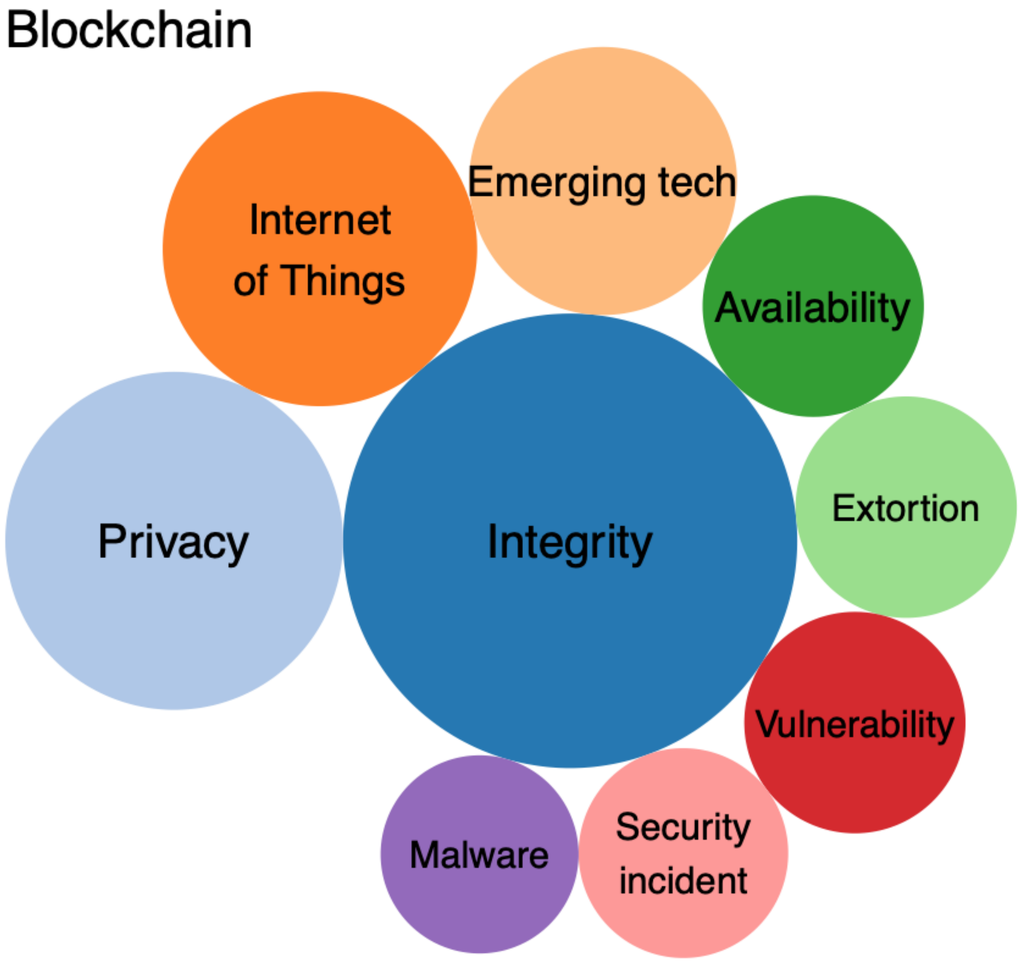


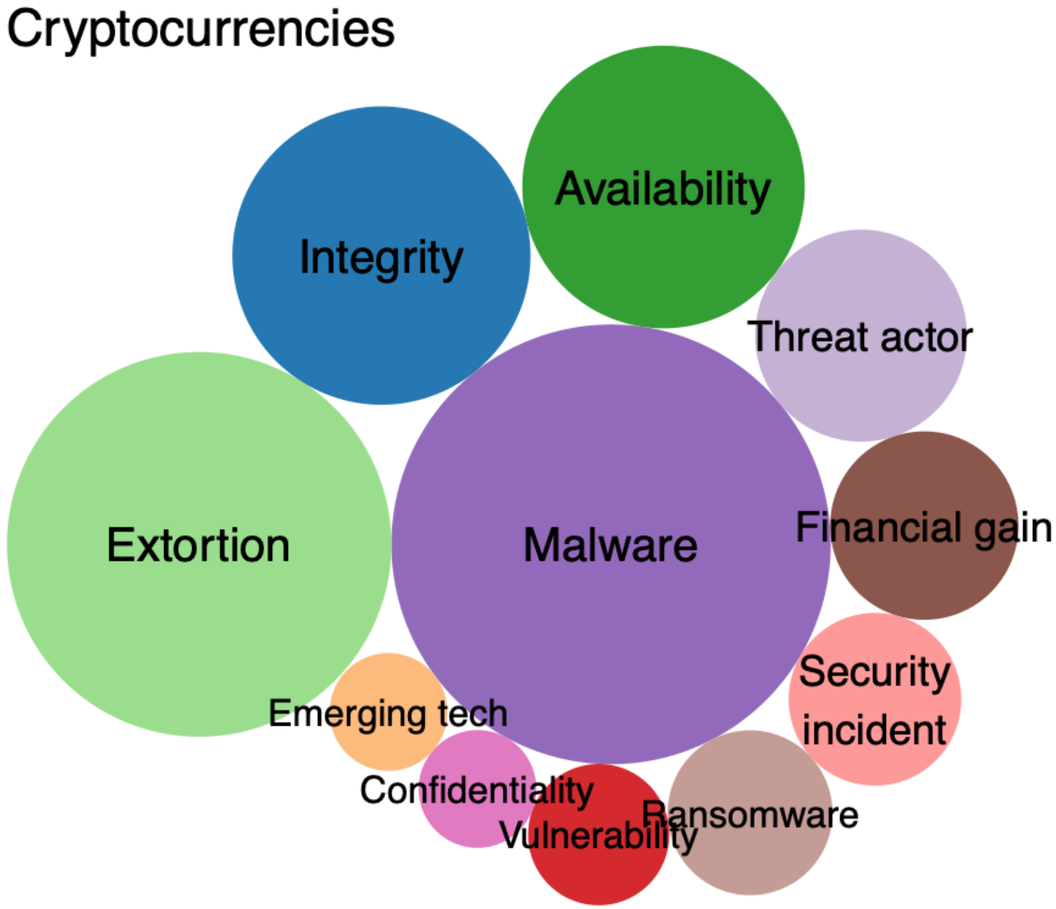

*Source: Cyentia Institute with data from RSA Conference*

# Striking Security Gold at RSAC



# Striking Security Gold at RSAC




*Source: Cyentia Institute with data from RSA Conference*

RSAConference2019

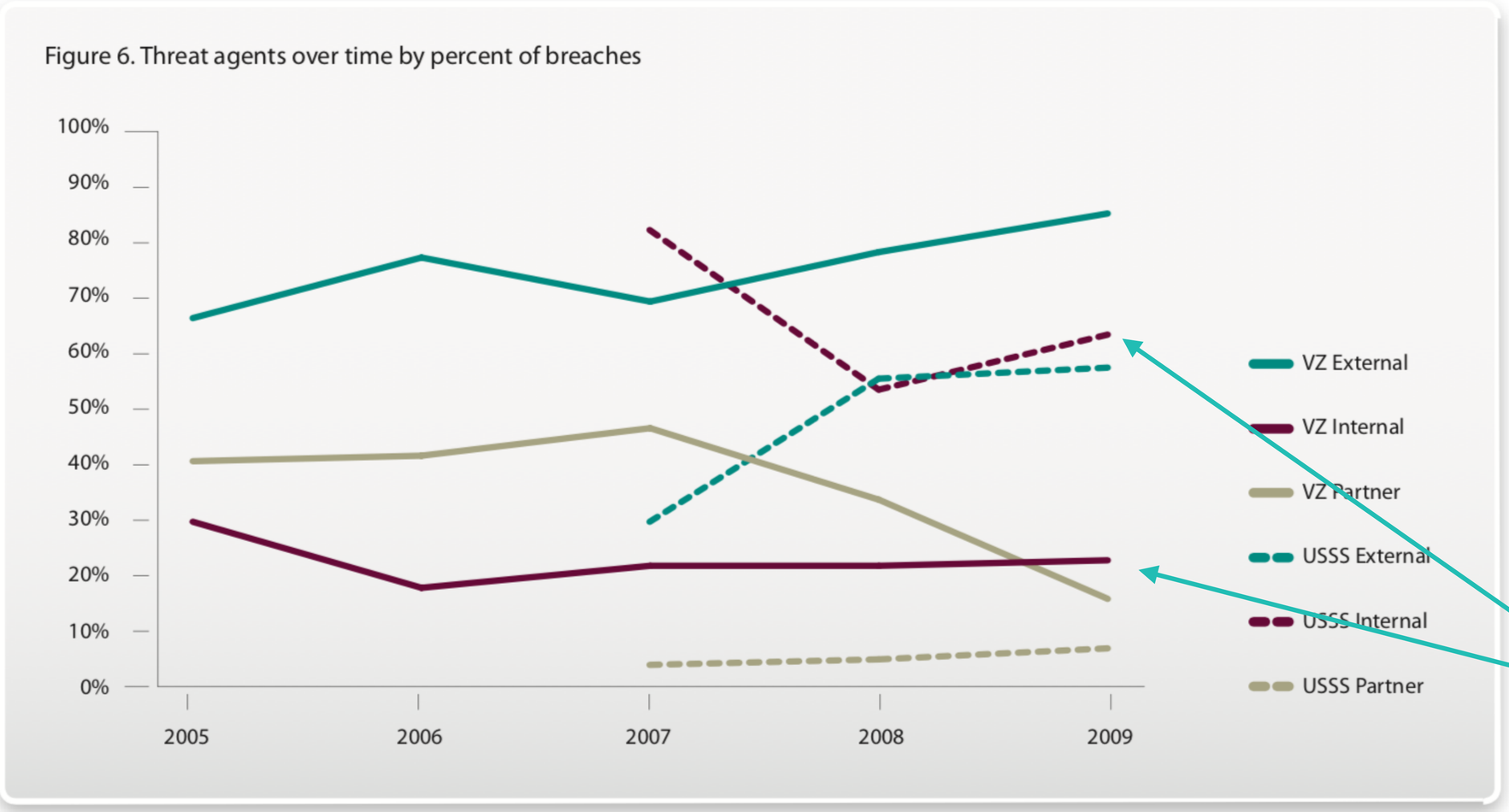
# Finding Shared Understanding in Industry Reports

# A (very) brief history of industry reports

- pre 2000: The CSI/FBI Report
- 2000s: Major vendors start dropping knowledge
  - Riptech/Symantec Internet Threat Report
  - Microsoft Security Intelligence Report
  - Verizon Data Breach Investigations Report
- 2010s: The "Cambrian Explosion" of cybersecurity reports

# A quick aside - Verizon DBIR...

# A quick aside - Verizon DBIR




## Shared Understanding

We need more sources and data!

## Knowledge

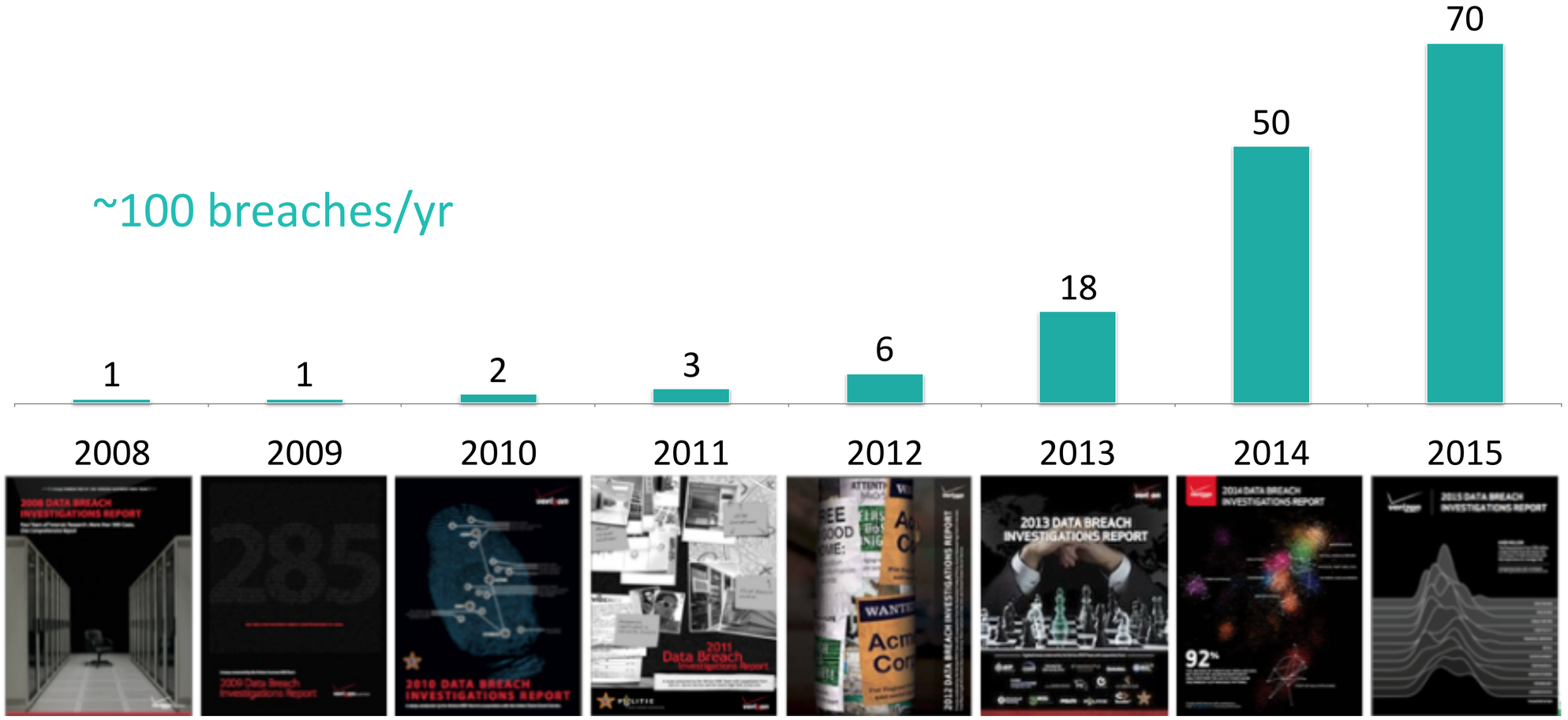
How do breach datasets differ? Why?

## Information

# A quick aside - Verizon DBIR

100,000+ incidents/yr

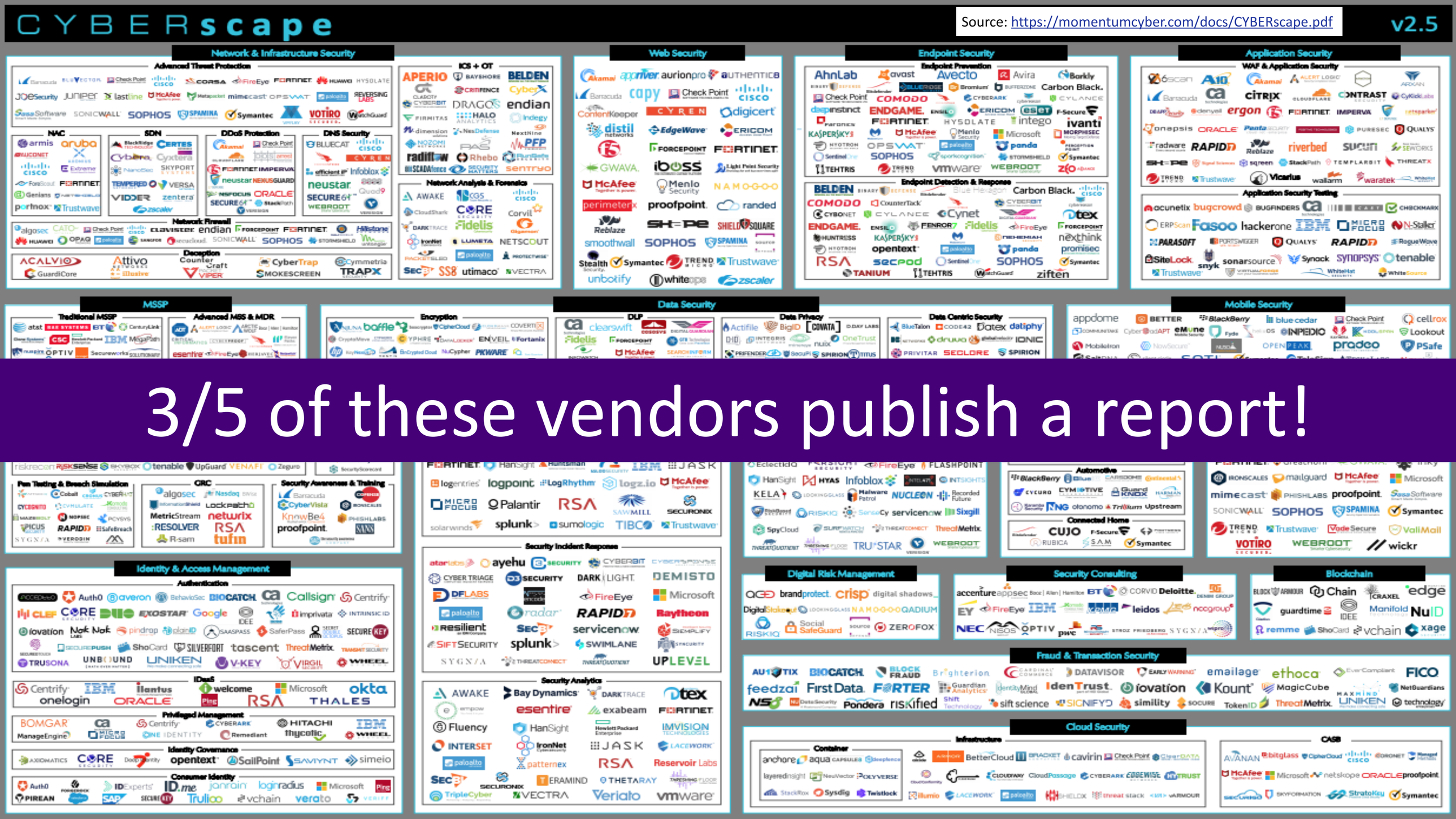
~100 breaches/yr



# A quick aside - Verizon DBIR

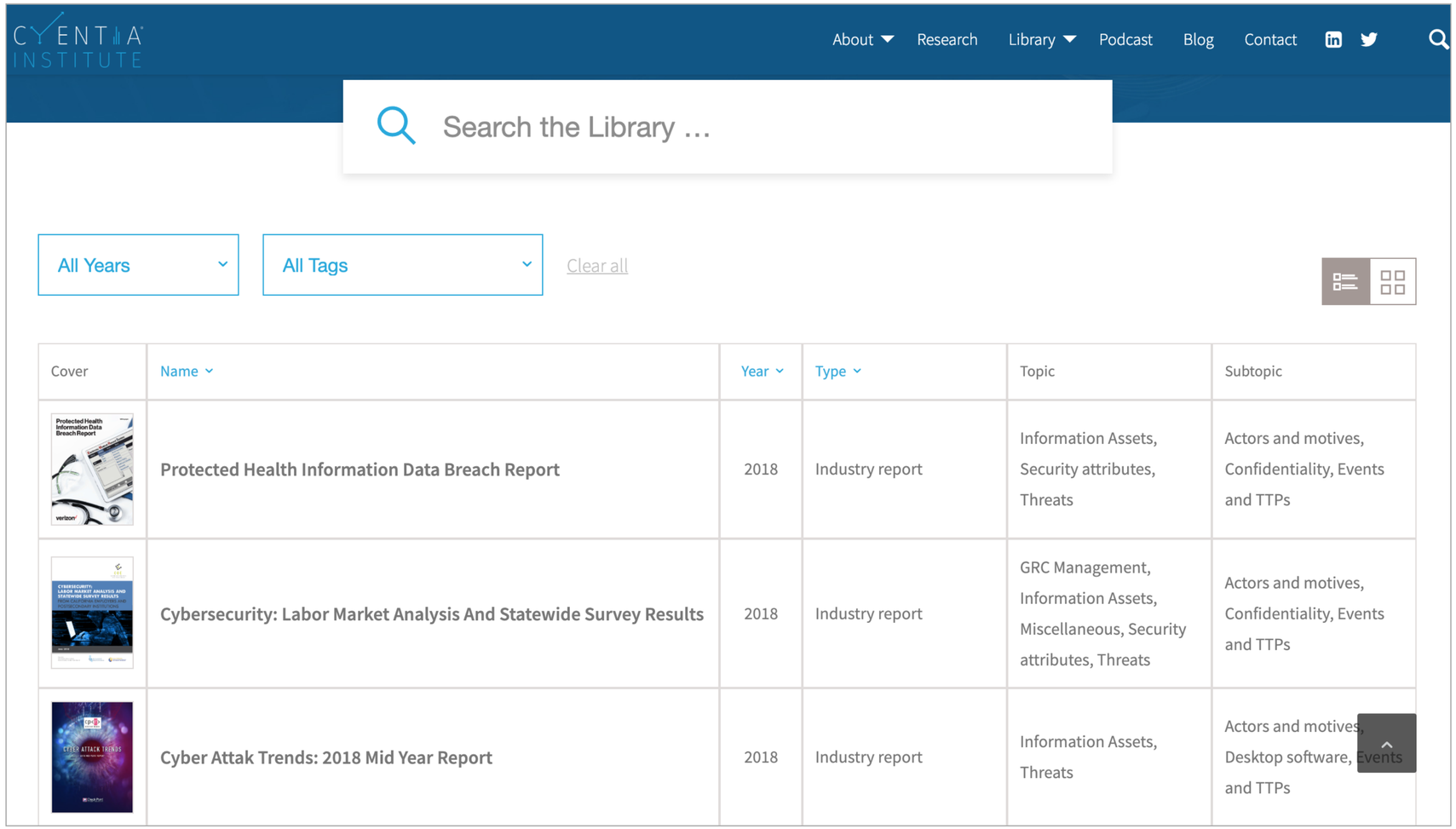

## DBIR = Shared Understanding

# Now back to the Cambrian Explosion...


CYBERscape
Source: https://momentumcyber.com/docs/CYBERscape.pdf
v2.5
Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Firewall
Deception
ICS + OT
Network Analysis & Forensics
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
3/5 of these vendors publish a report!
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Incident Response
Automotive
Connected Home
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB

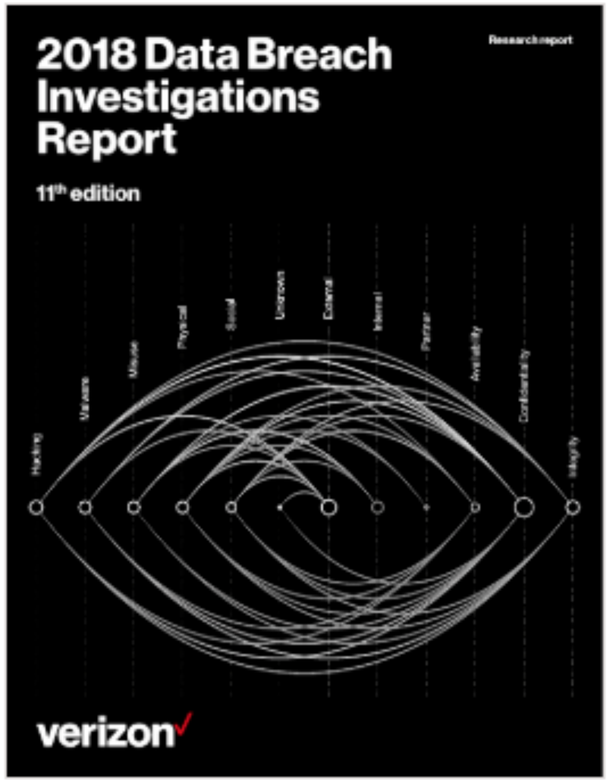
# Cyentia Library: Curating Industry Knowledge

- ~ 650 sources
- 1,800+ reports
- 44,000 pages
- 12m words
- 645k sentences
- 2,000+ Acronyms Defined
- 100% Free!




Source: https://www.cyentia.com/library/

# "What's this report about?"




## 2018 Data Breach Investigations Report

Industry report

## Summary

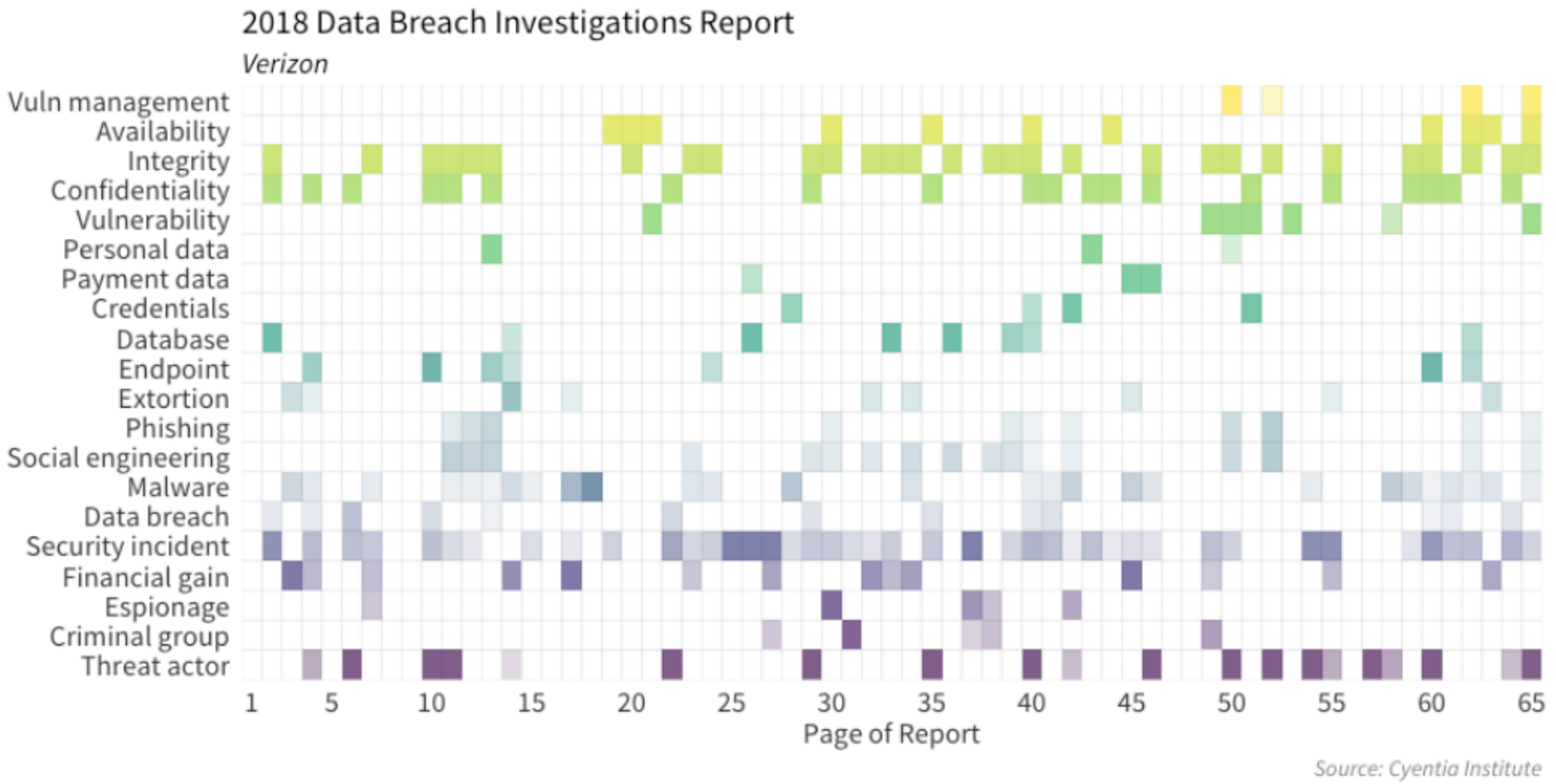
Verizon's annual report on data breaches in 2018

**Source(s):** Verizon

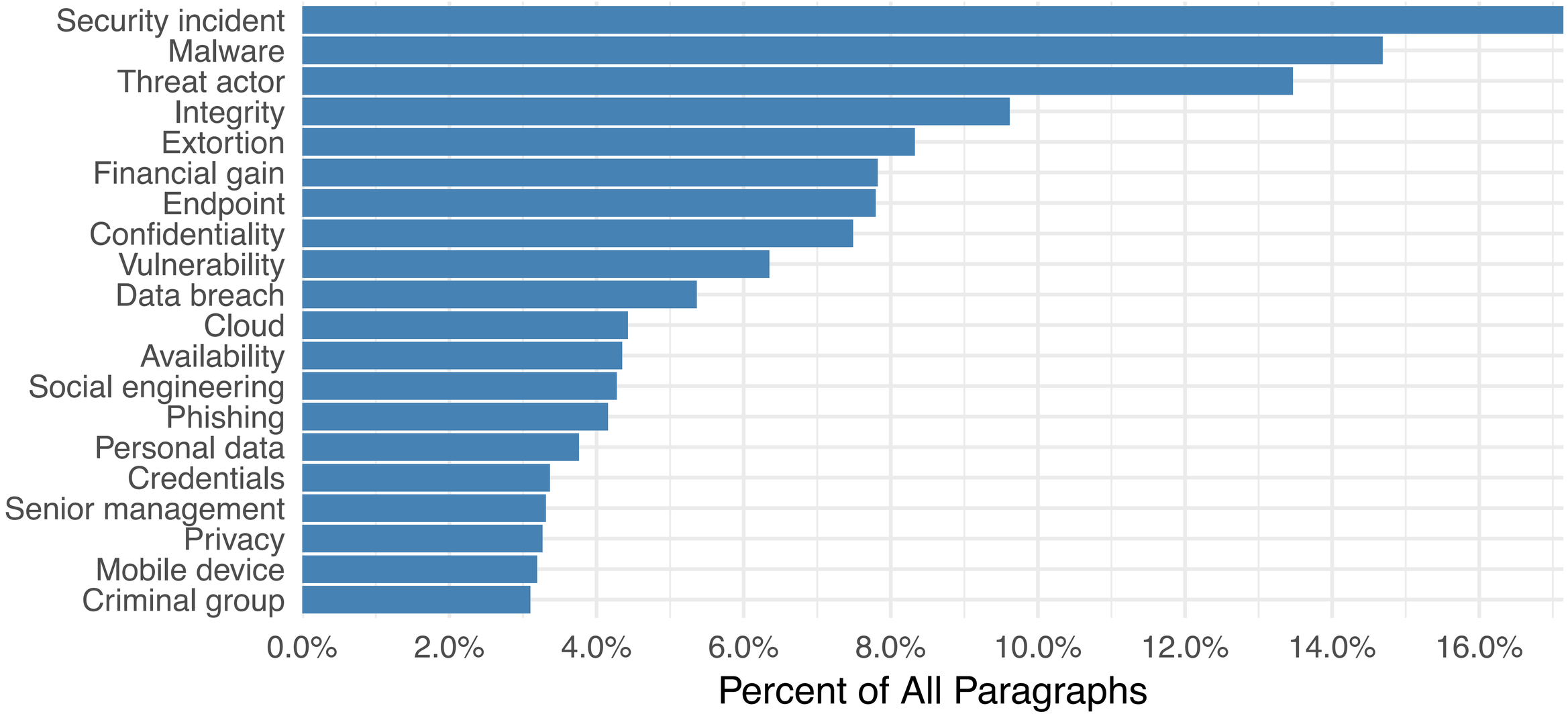
**Topic(s):** Controls, GRC Management, Information Assets, Market trends, Security attributes, Threats

**Subtopic(s):** Actors and motives, Availability, CIS "Top20" Controls, Compliance, Confidentiality, Data, Desktop software, Emerging tech, Events and TTPs, External services, Governance, InfoSec market, Infrastructure, Integrity, Intelligence, Vulnerability

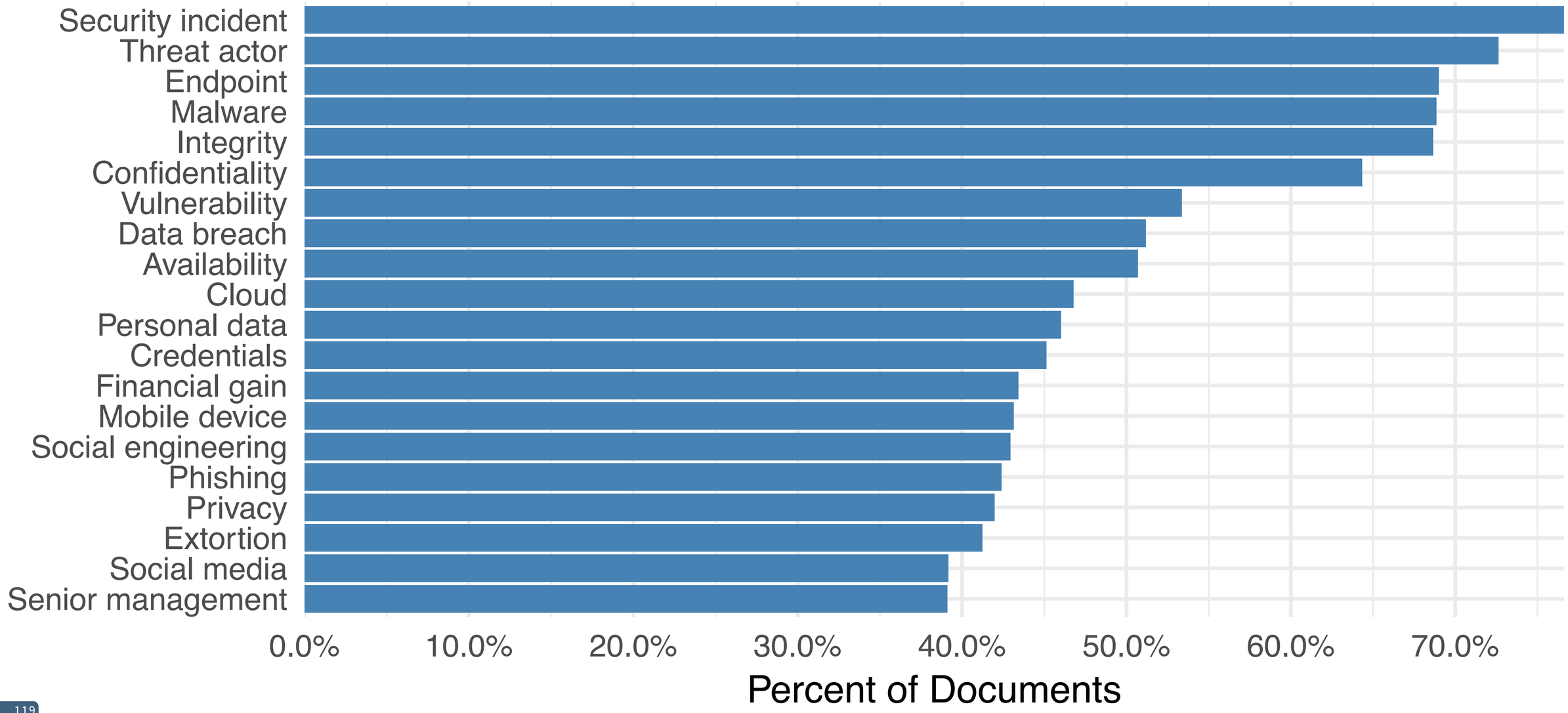
# "What's this report about?"

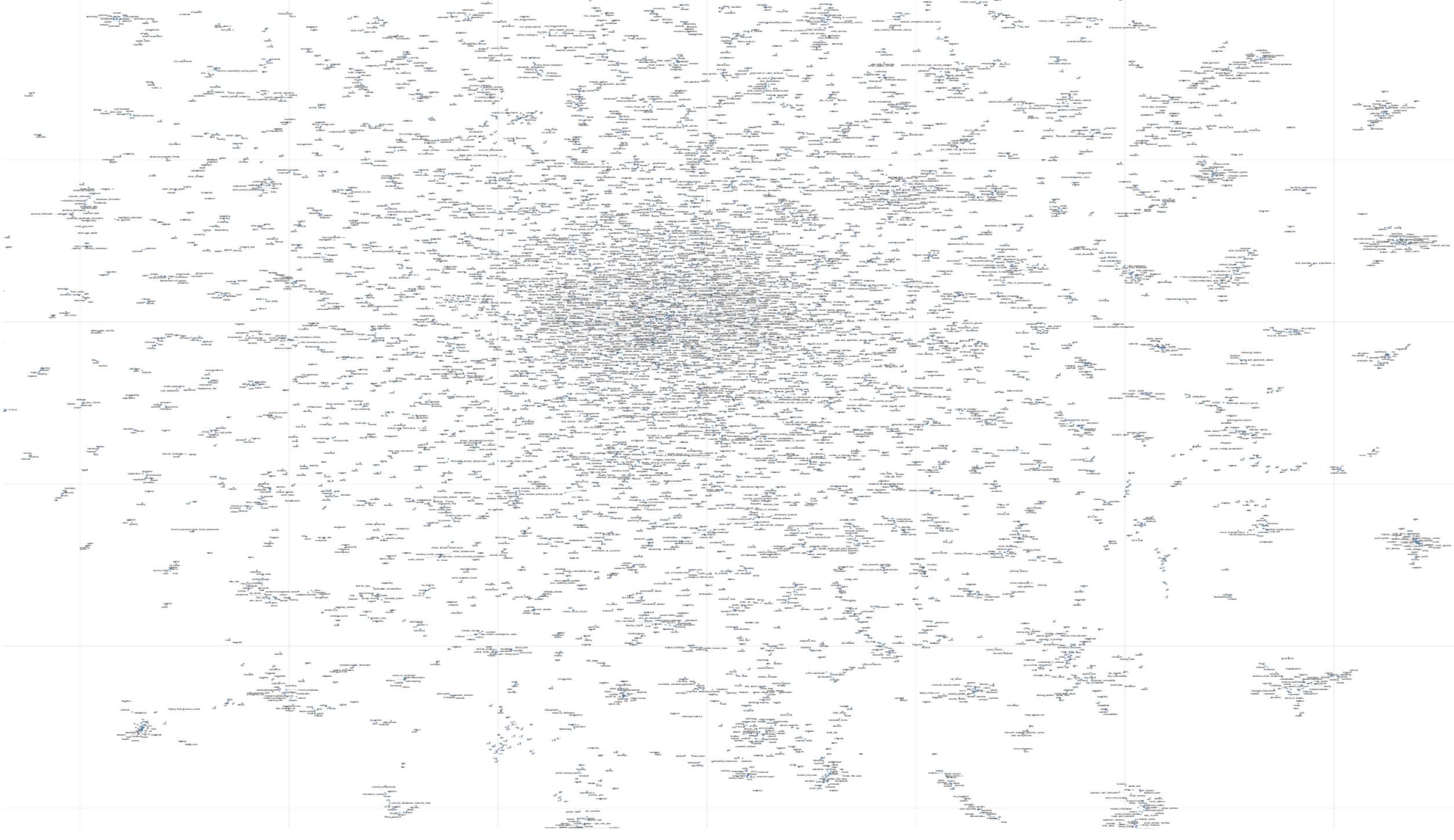


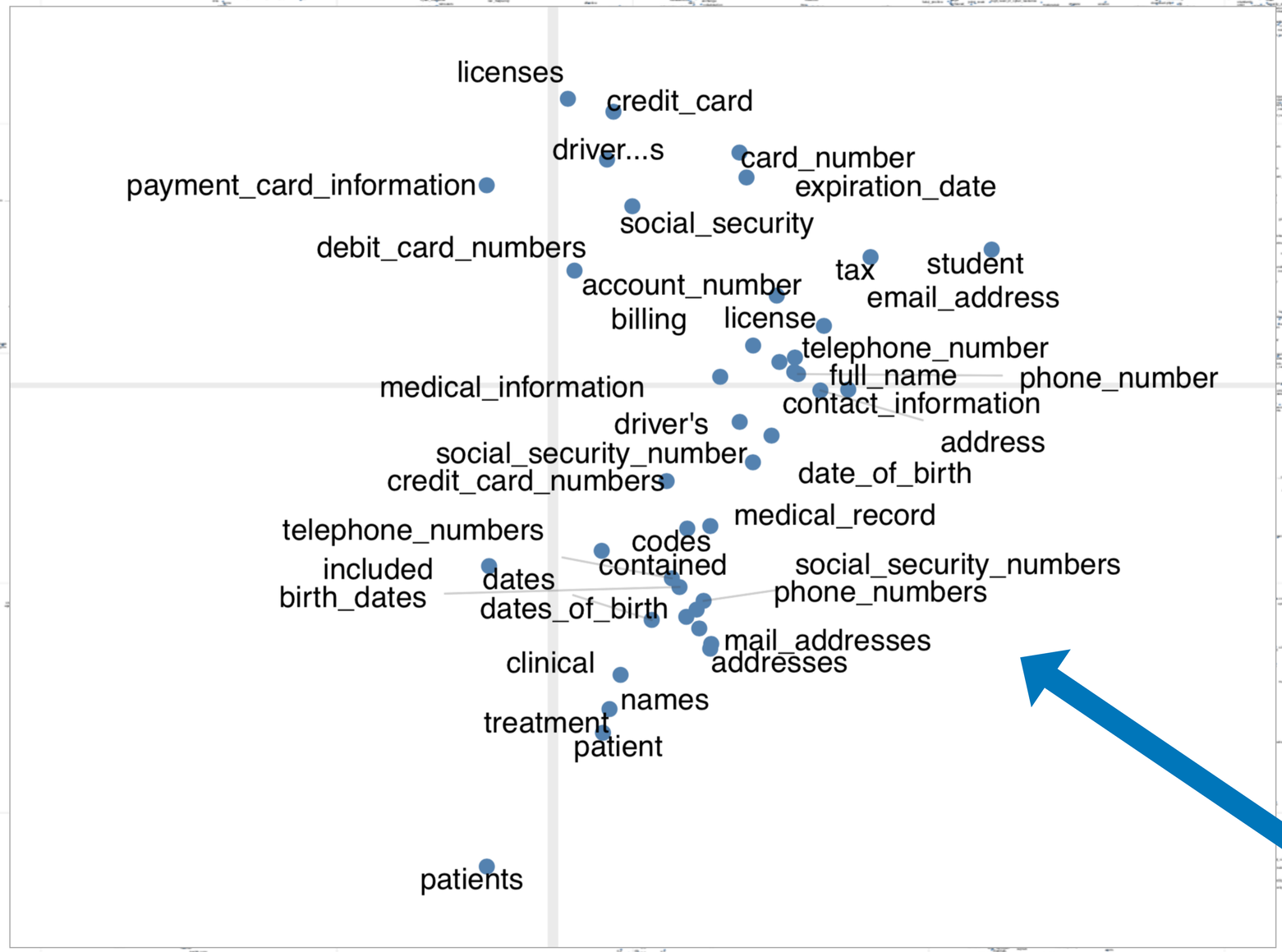
# Security Topics by Paragraph

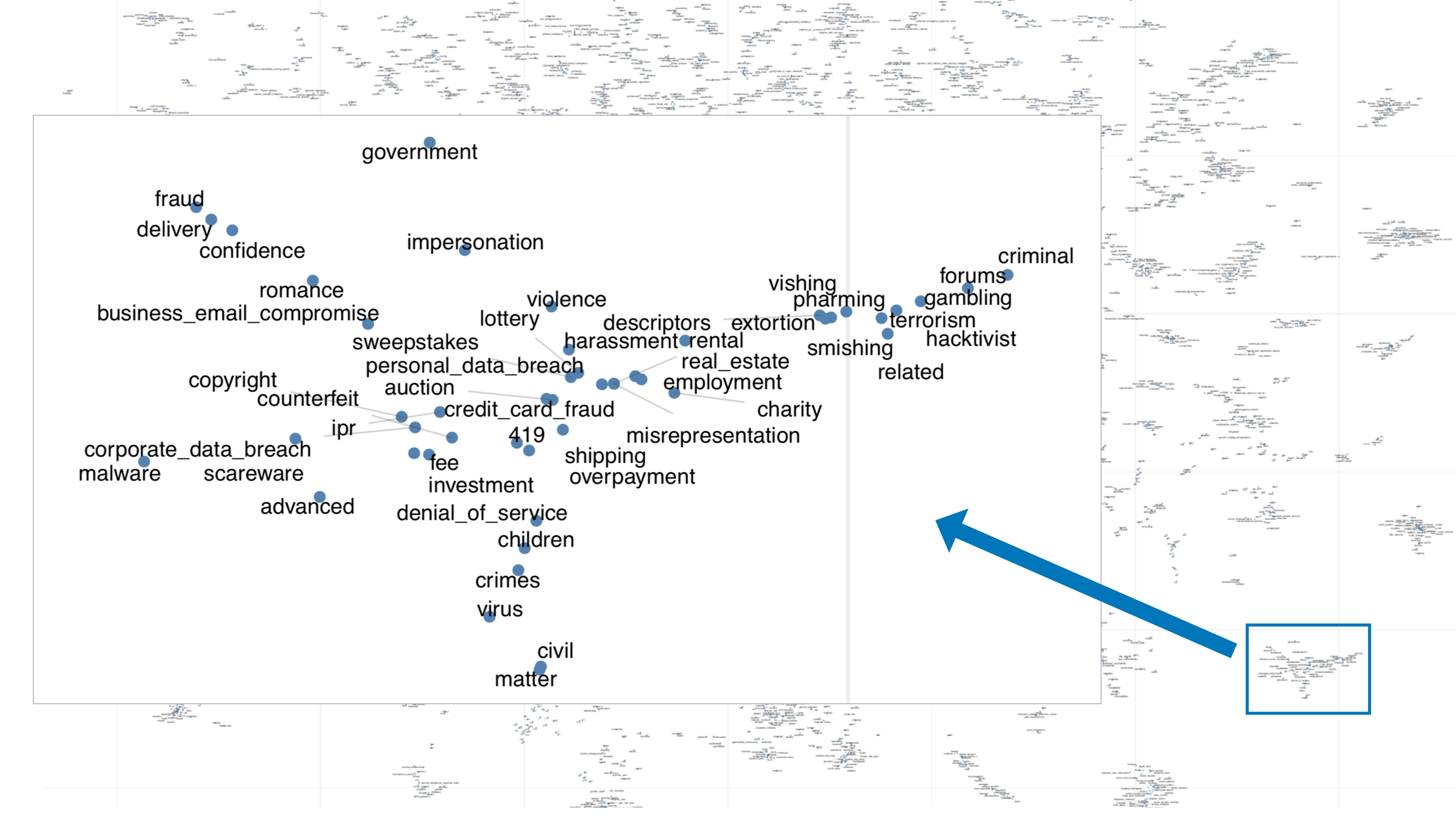


# Security Topics by Report

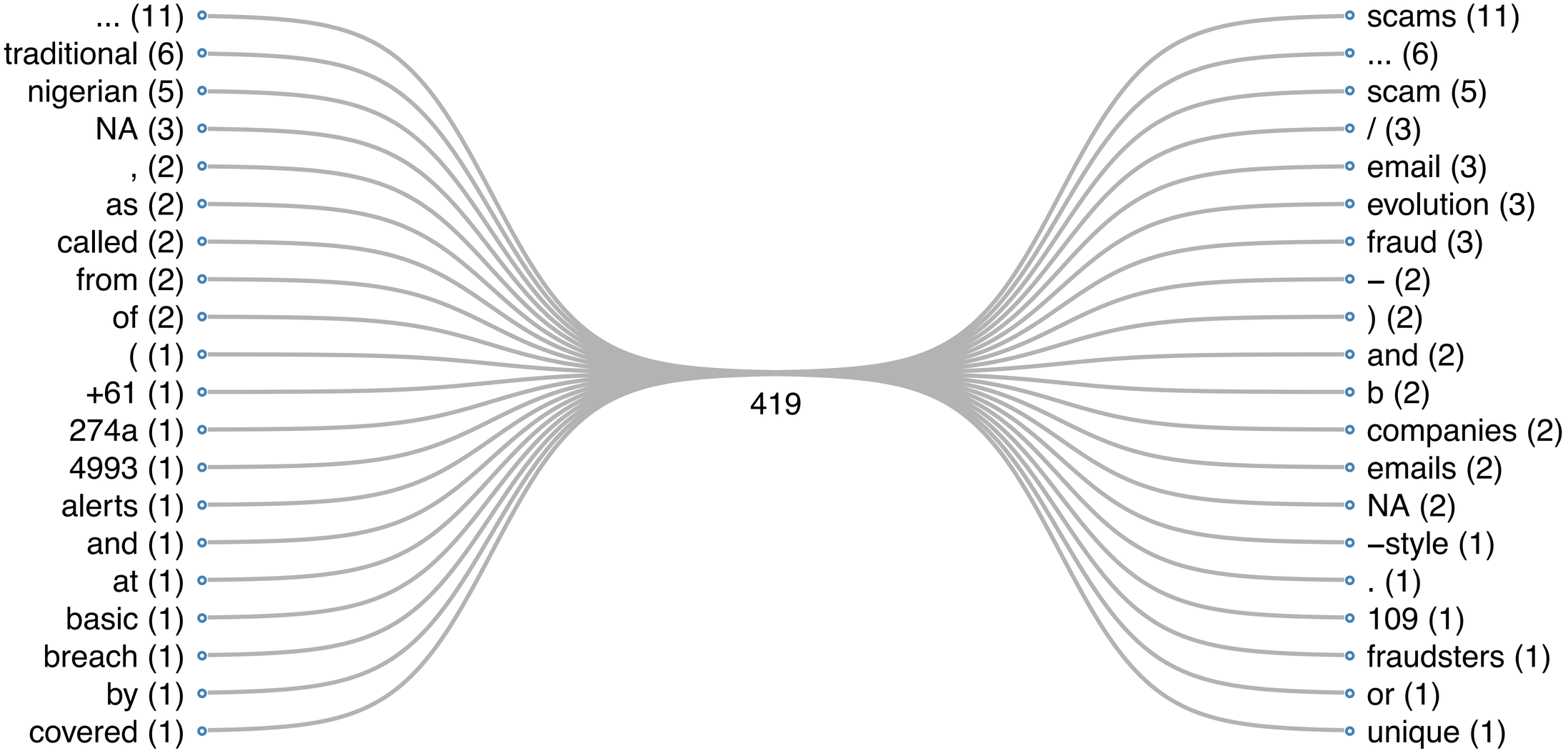




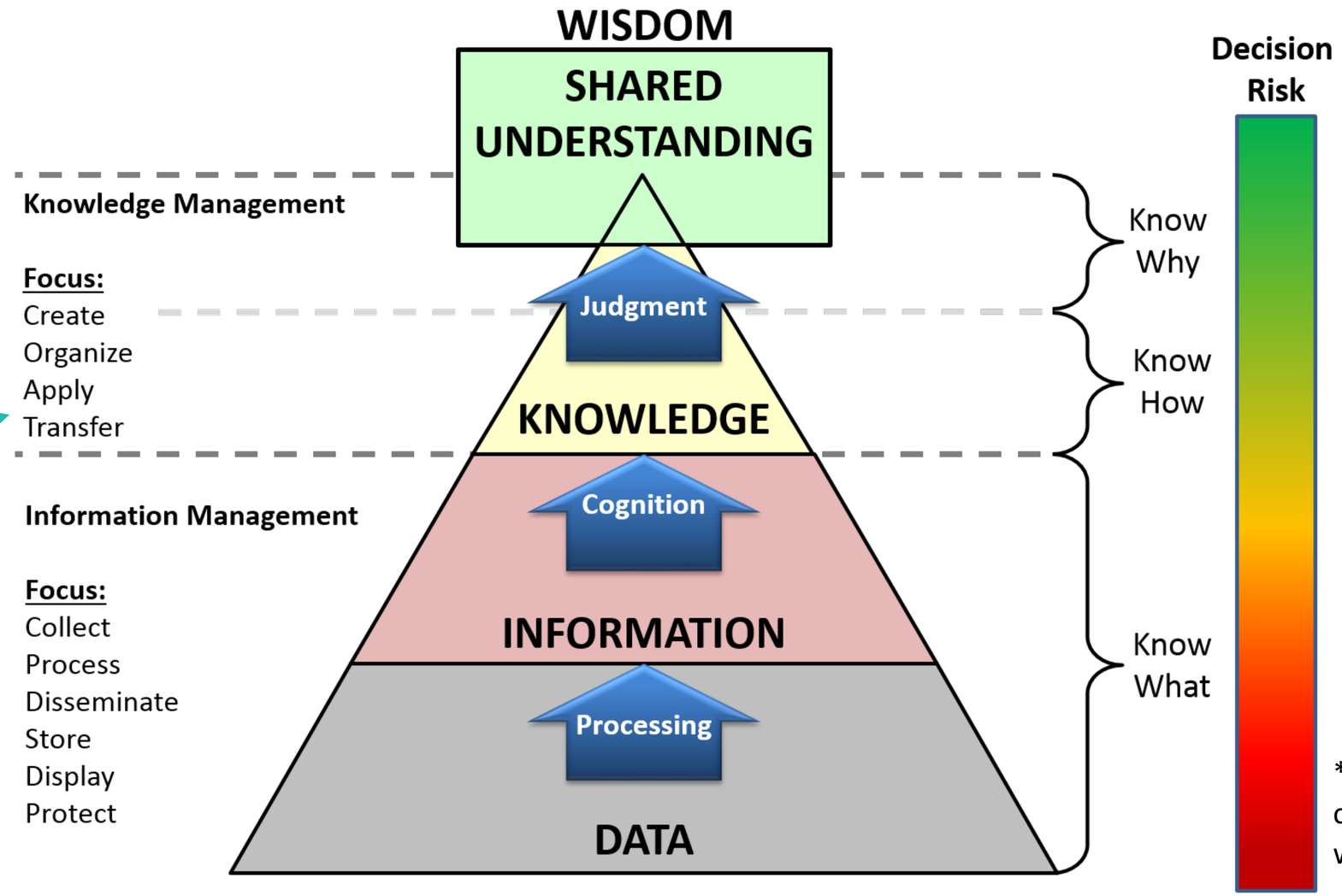

licenses
credit_card
driver...s
card_number
payment_card_information
expiration_date
social_security
debit_card_numbers
tax
student
account_number
email_address
billing
license
telephone_number
full_name
phone_number
medical_information
contact_information
driver's
address
social_security_number
date_of_birth
credit_card_numbers
medical_record
telephone_numbers
codes
included
contained
social_security_numbers
dates
birth_dates
phone_numbers
dates_of_birth
mail_addresses
addresses
clinical
names
treatment
patient
patients


government
fraud
delivery
confidence
impersonation
criminal
forums
vishing
pharming
gambling
romance
violence
business_email_compromise
lottery
descriptors
extortion
terrorism
hacktivist
sweepstakes
harassment
rental
smishing
personal_data_breach
real_estate
related
copyright
auction
employment
counterfeit
credit_card_fraud
charity
ipr
419
misrepresentation
corporate_data_breach
shipping
fee
malware
scareware
overpayment
investment
advanced
denial_of_service
children
crimes
virus
civil
matter

# Specific Context for “419”



# Knowledge Management Cognitive Pyramid

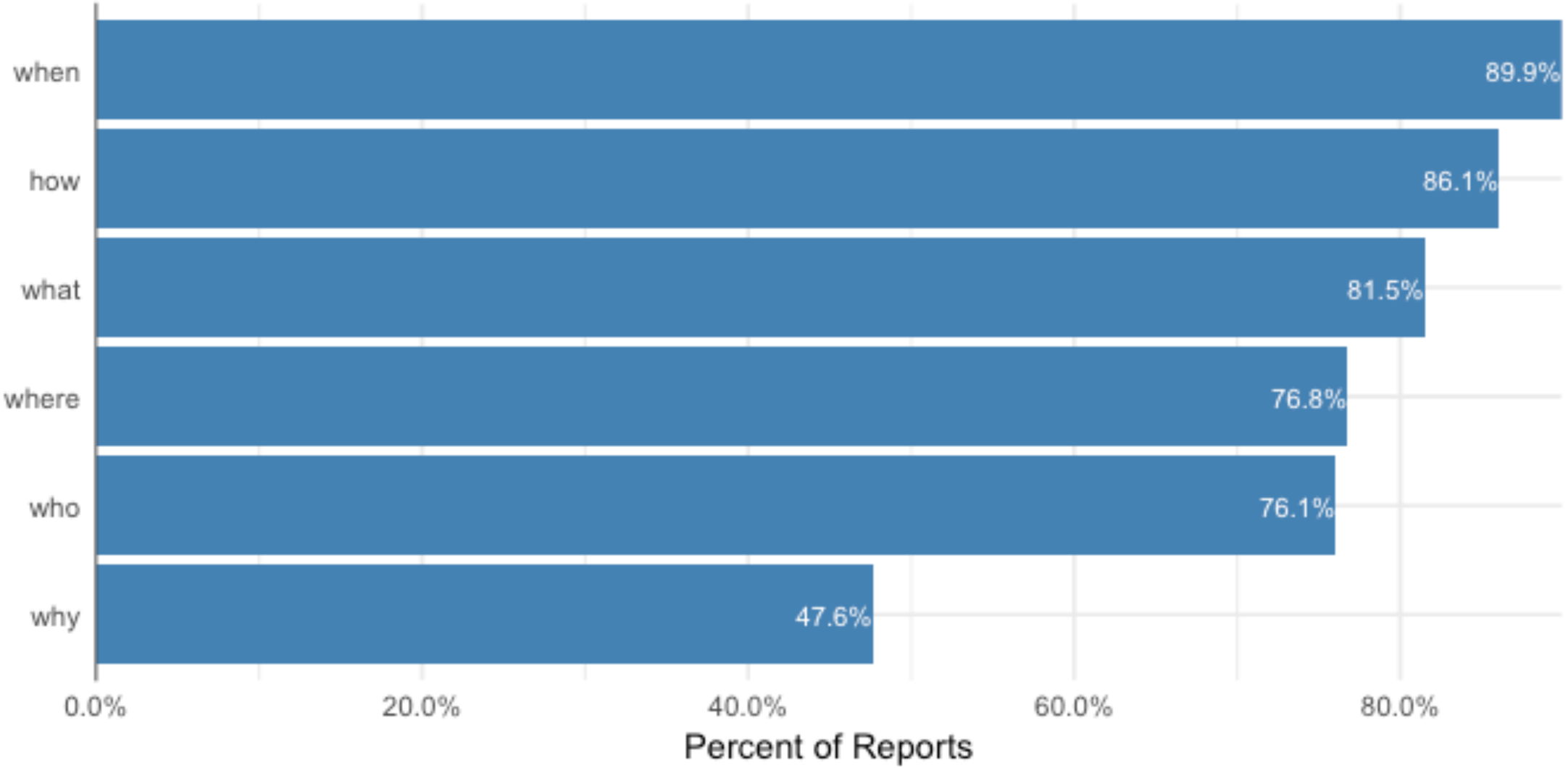



We are here

*Apologies for the 90s-era clip art, but why recreate the wheel--er--pyramid?

Source: https://en.wikipedia.org/wiki/File:KM_Pyramid_Adaptation.png

# Lacking some “why”



# Declaritive Statements: “blockchain is…”

- “Blockchain is a hot technology topic, yet 36% of respondents admit they don’t understand its mechanism.”
- “A blockchain is a distributed, verifiable datastore.”
- “A blockchain is a distributed ledger system that records online transactions.”
- “A blockchain is a verifiable transaction database carrying an ordered list of all transactions that ever occurred.”
- “…the only valid blockchain is the one with most blocks in it.”
- “A blockchain is a series of records or transactions, collected together in a block that defines a portion of a ledger.”
- “Blockchain is no magic bullet.”

RSAConference2019

# Finding Shared Understanding in Meta-Analysis

# Modern meta-analysis


Trusted evidence.
Informed decisions.
Better health.

## What is a systematic review?

A systematic review attempts to identify, appraise and synthesize all the empirical evidence that meets pre-specified eligibility criteria to answer a given research question. Researchers conducting systematic reviews use explicit methods aimed at minimizing bias, in order to produce more reliable findings that can be used to inform decision making. (See Section 1.2 in the ***Cochrane Handbook for Systematic Reviews of Interventions***.)

# Modern meta-analysis

"A systematic review attempts to identify, appraise and synthesize all the empirical evidence that meets pre-specified eligibility criteria to answer a given research questions."

Given a Research Question:

- Identify sources of evidence
- Appraise the quality of evidence
- Aggregate and synthesize evidence (meta-analysis)

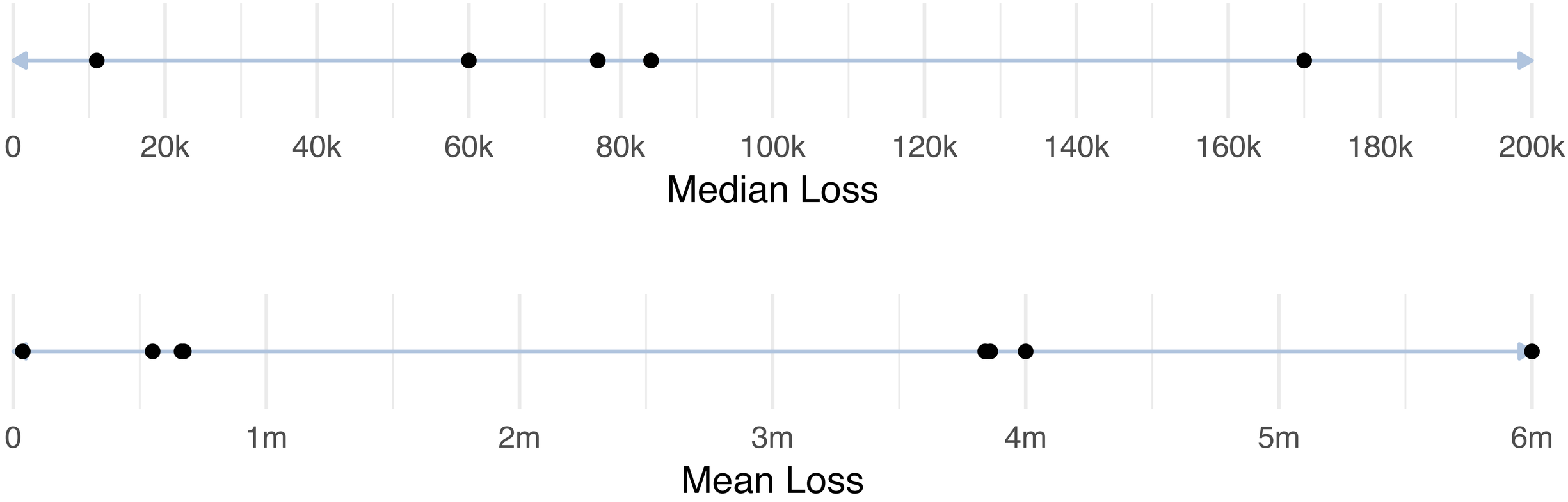
# "What's the impact of a data breach?

| Year | Source | Median | Mean |
|---|---|---|---|
| 2015 | Kaspersky (Survey) - SMBs | 11,000 | 38,000 |
| 2015 | Kaspersky (Survey) - Enterprise | 84,000 | 551,000 |
| 2015 | NetDiligence (Insurance Claims) | 76,984 | 673,767 |
| 2016 | NetDiligence (Insurance Claims) | 60,000 | 665,000 |
| 2016 | Romanosky (Advisen) | 170,000 | 6 mil |
| 2017 | SailPoint (Survey) | | 4 mil |
| 2018 | Ponemon (Survey) | | 3.86 mil |
| 2017 | Ponemon (Survey) | | 3.62 mil |
| 2016 | Ponemon (Survey) | | 4 mil |

Table 1: Sources and statistics for losses associated with data breaches.

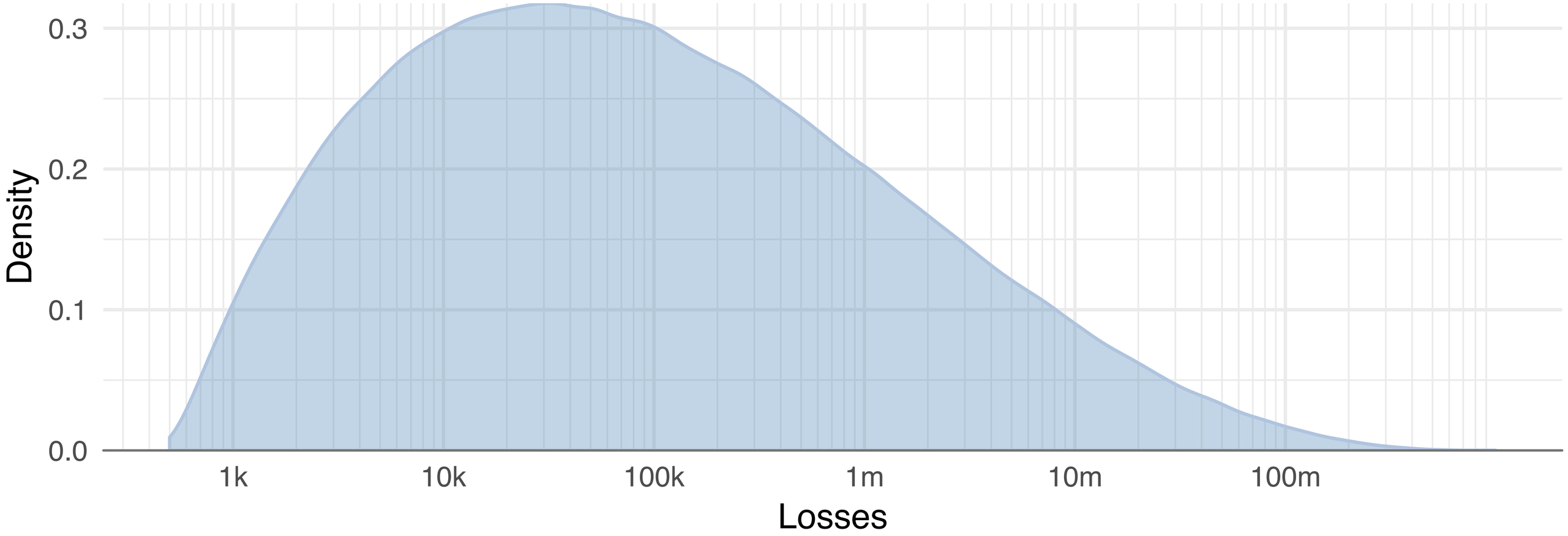
Source: Upcoming report from Global Cyber Alliance (will be out by RSAC)

# "What's the impact of a data breach?




Source: Upcoming report from Global Cyber Alliance (will be out by RSAC)

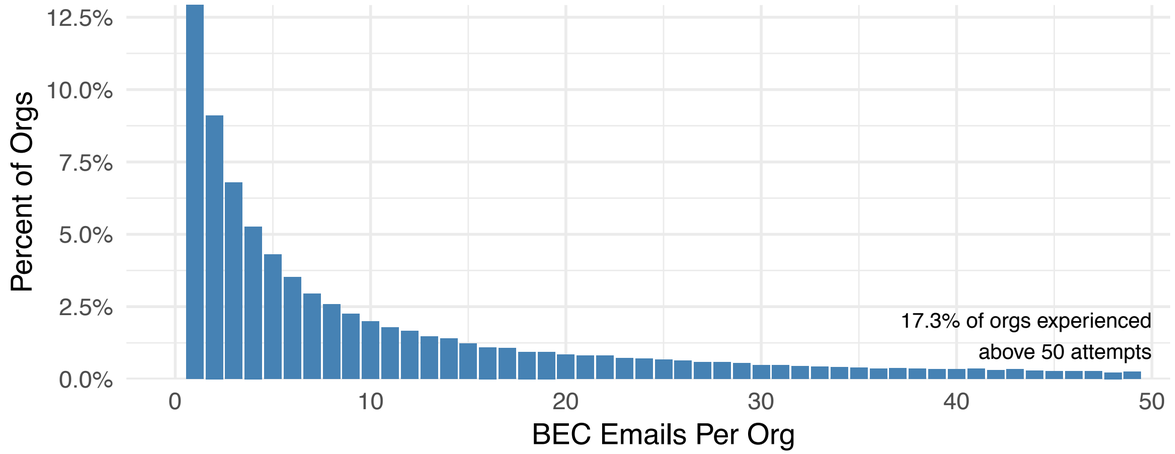
# "What's the impact of a data breach?

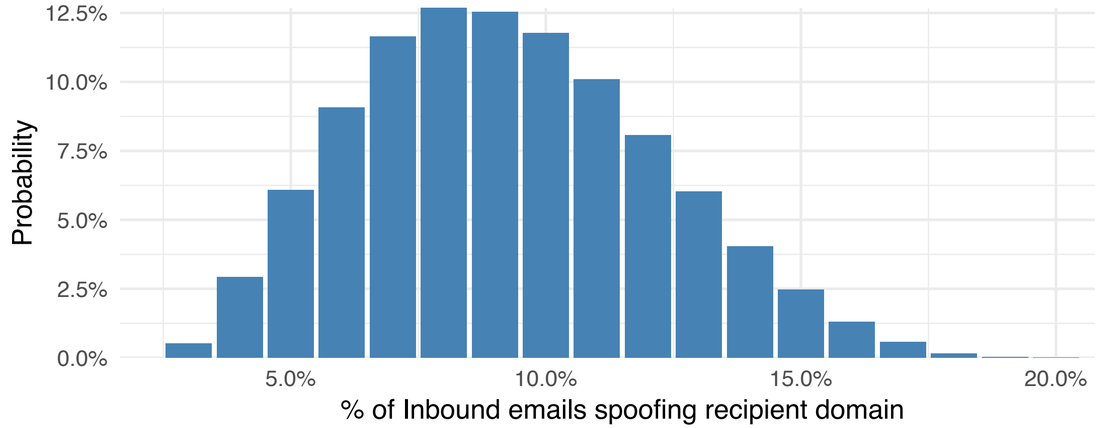



Source: Upcoming report from Global Cyber Alliance (will be out by RSAC)

# And a talk later today (1:30 in 2011)

- Jay and Adam Shostack will talk about measuring DMARC ROI

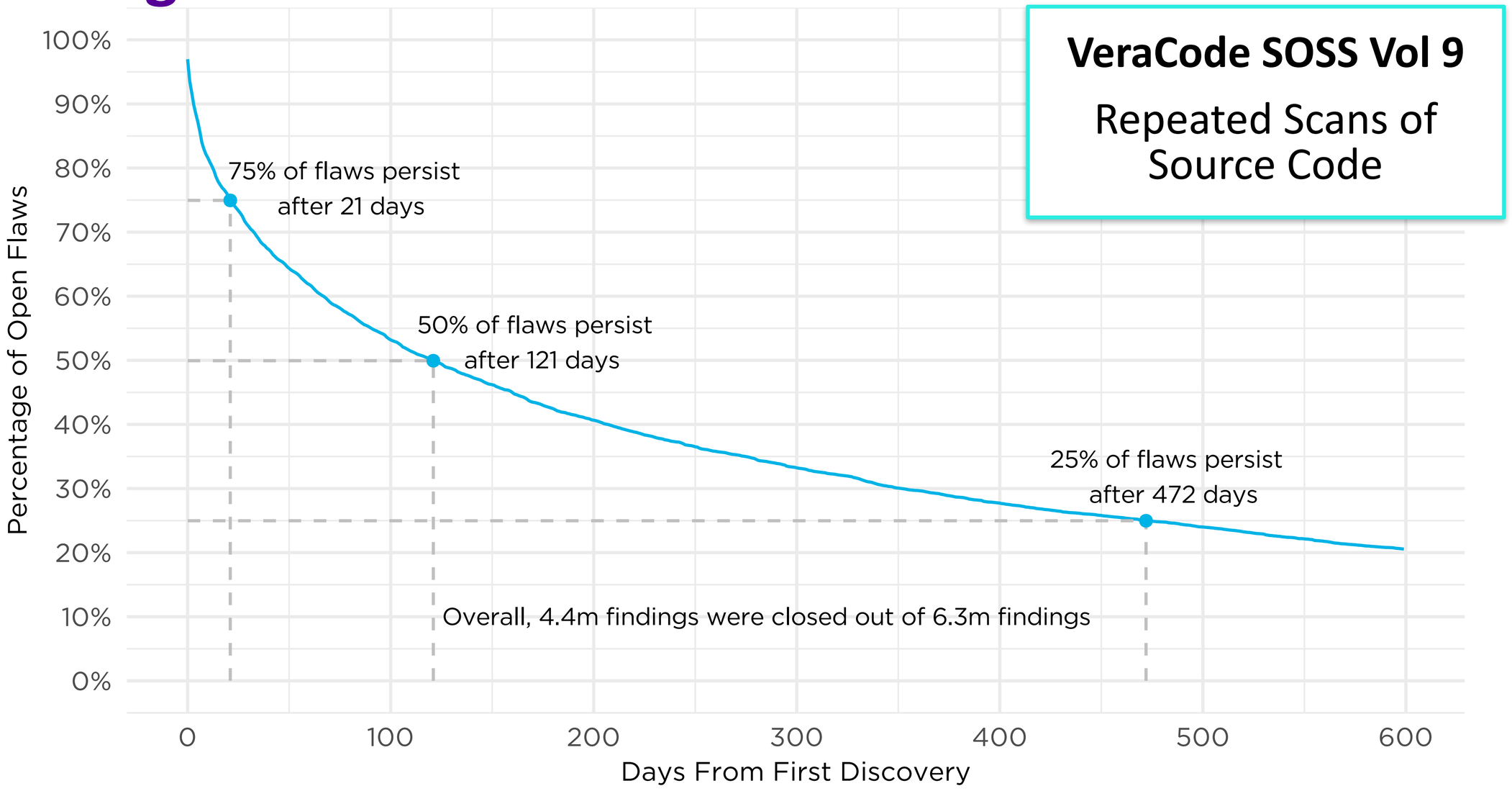



RSAConference2019

# Finding Shared Understanding in Original Research

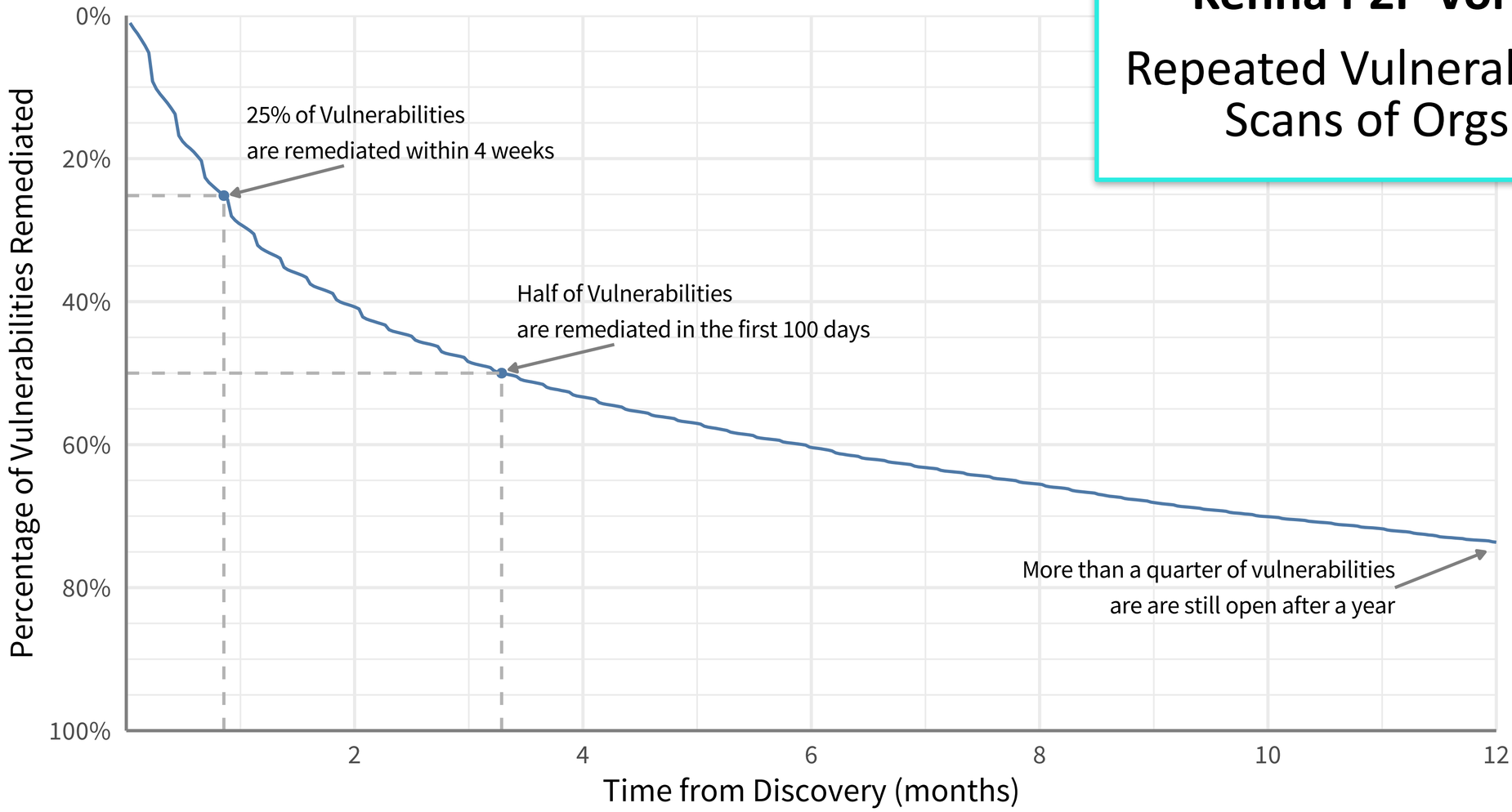
# How long do Flaws Survive?



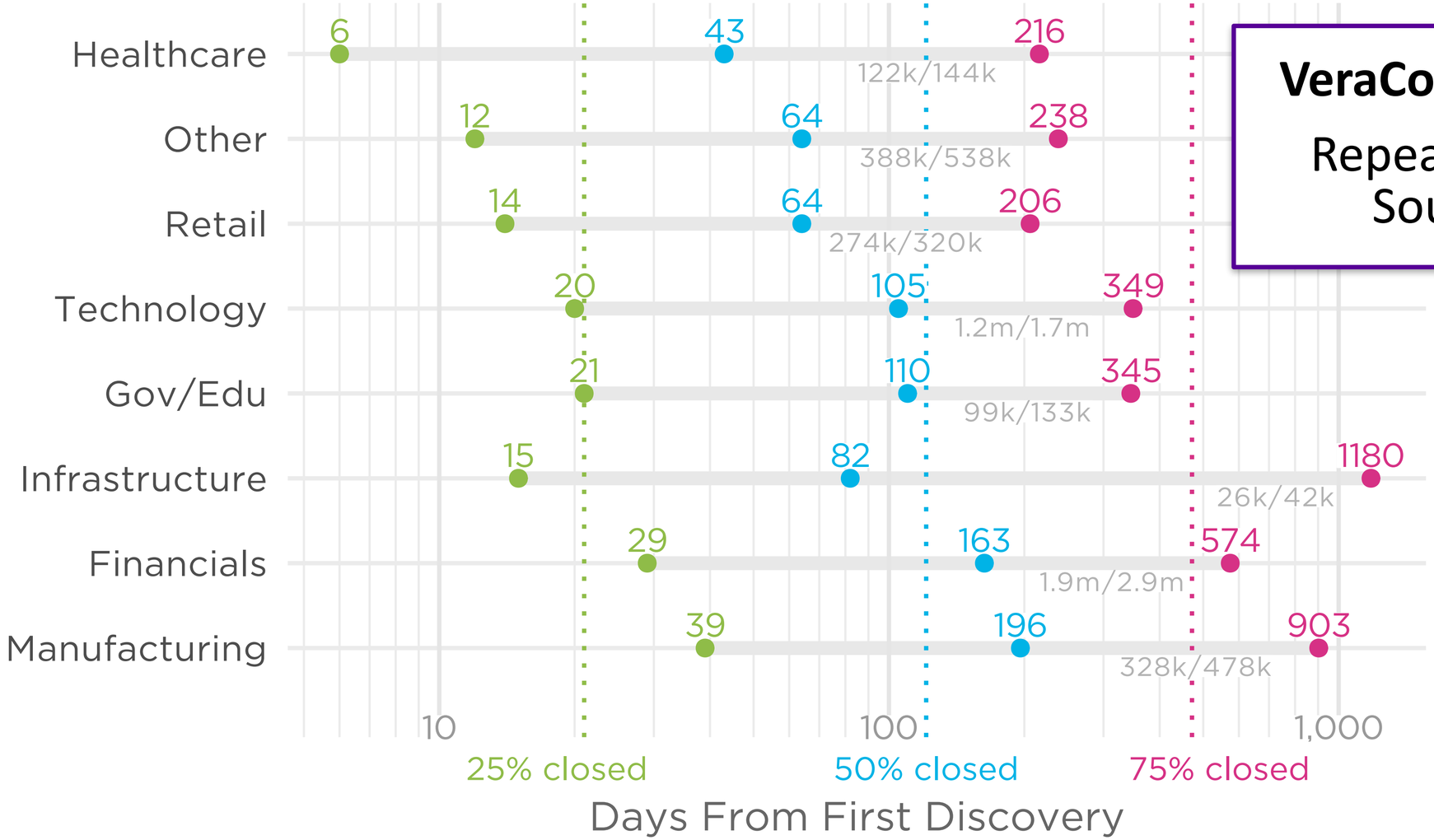
# How long do Flaws Survive?

**Kenna P2P Vol 3**

Repeated Vulnerability Scans of Orgs



# Comparing Industries

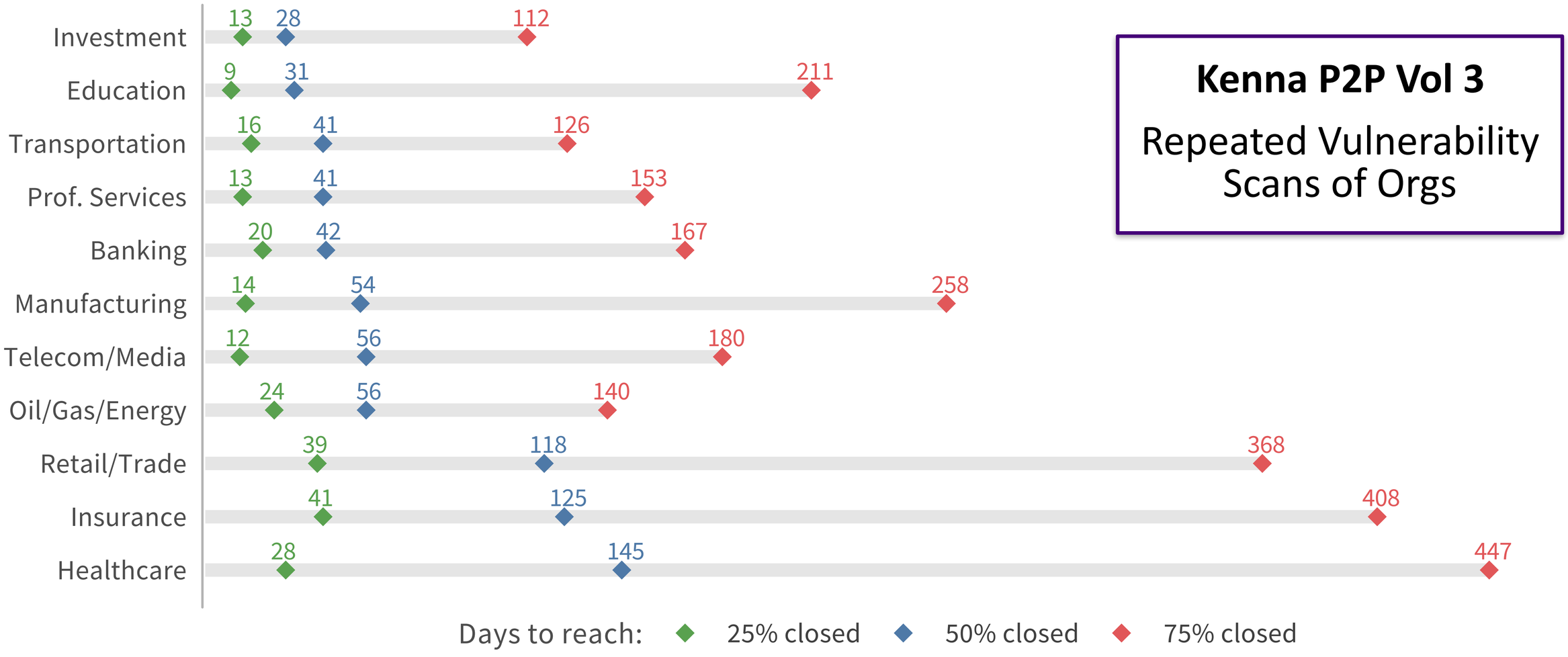



**VeraCode SOSS Vol 9**

Repeated Scans of Source Code

Source: Veracode SOSS Volume 9

# Comparing Industries

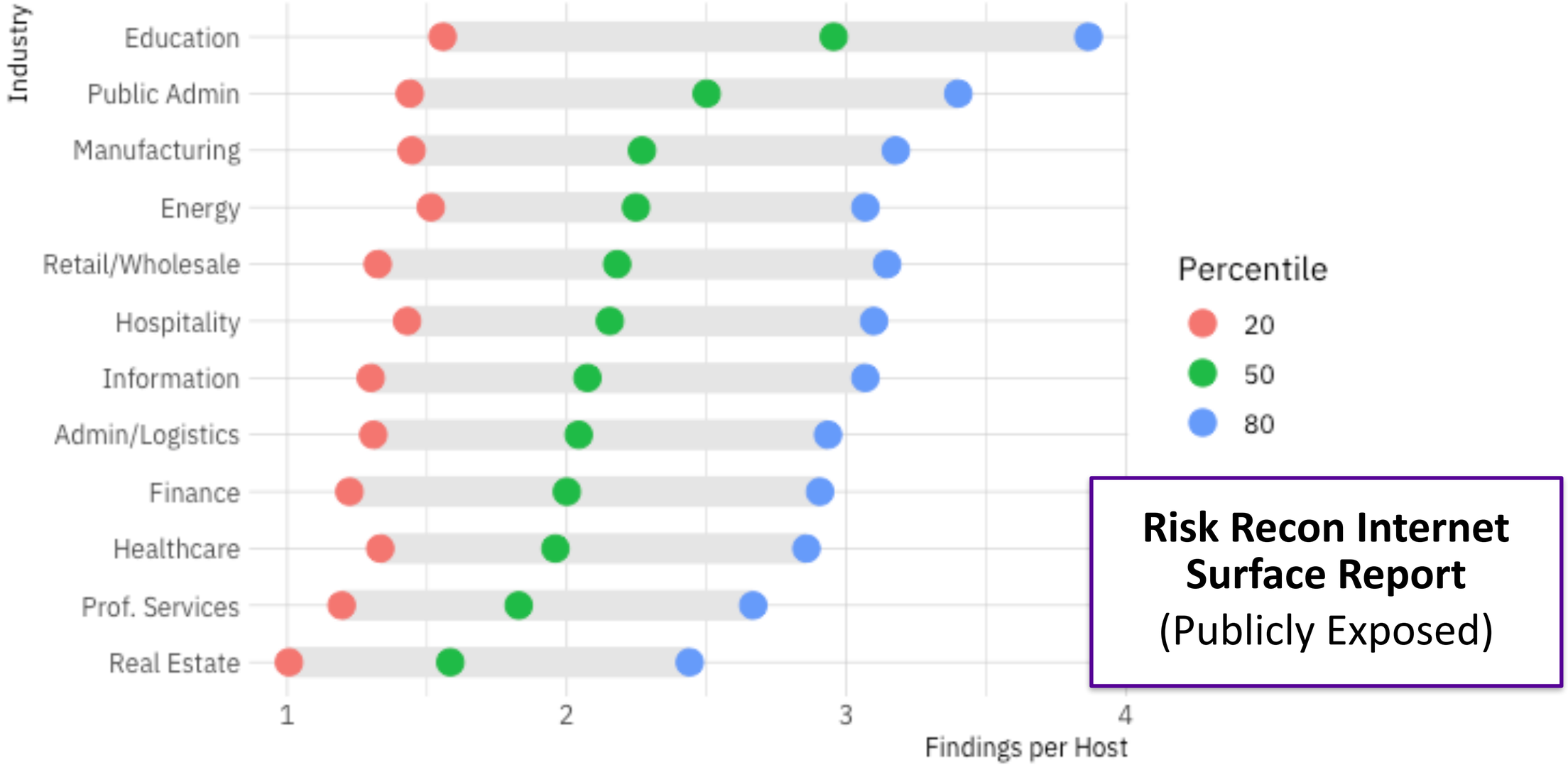



**Kenna P2P Vol 3**

Repeated Vulnerability Scans of Orgs

*Source: Kenna / Cyentia*

# Comparing Industries




**Risk Recon Internet Surface Report**
(Publicly Exposed)

RSAConference2019

San Francisco | March 4–8 | Moscone Center

# How you can be… BETTER.

# From now on…

- Next time you read an industry report...

  Learn to be appropriately critical of research

  Demand minimum of things of your vendors research

- Next time you're looking for information on a topic...

  Use the Open and Free Cyentia Library

- Next time you're looking for stats to support a decision...

  Don't be satisfied with a single data point

RSA®Conference2019
San Francisco | March 4 – 8 | Moscone Center


SESSION ID: MASH-R03

**Wade Baker, PhD**
Partner, Cyentia Institute

**Jay Jacobs**
Partner, Cyentia Institute