RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: GRC-T09

We're Not in Kansas Anymore: Measuring the Impact of a Data Breach

Suzanne Widup

Senior Analyst
Verizon Enterprise Solutions
@SuzanneWidup

#RSAC

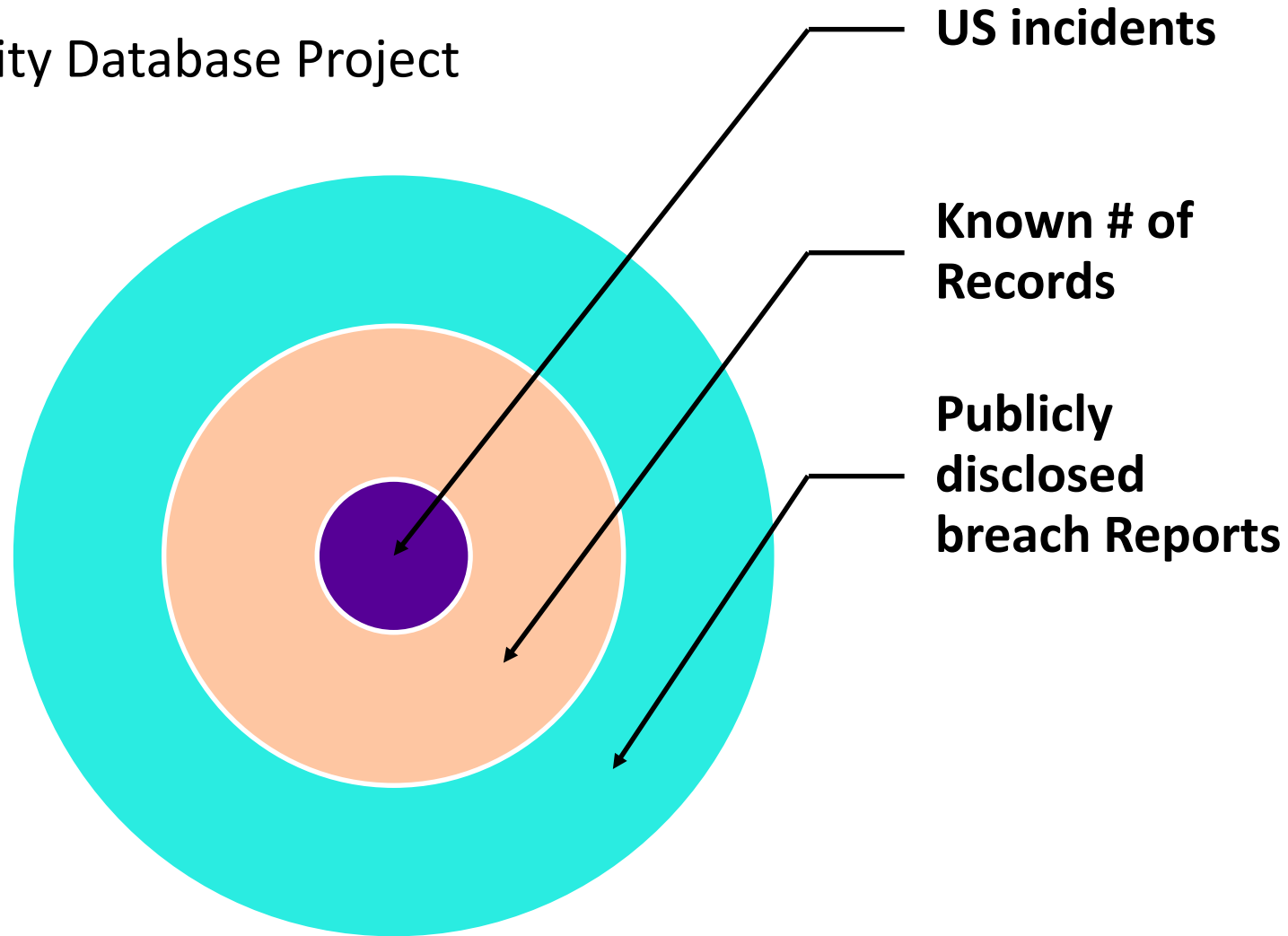# How Breach Impact Has Been Measured in the Past
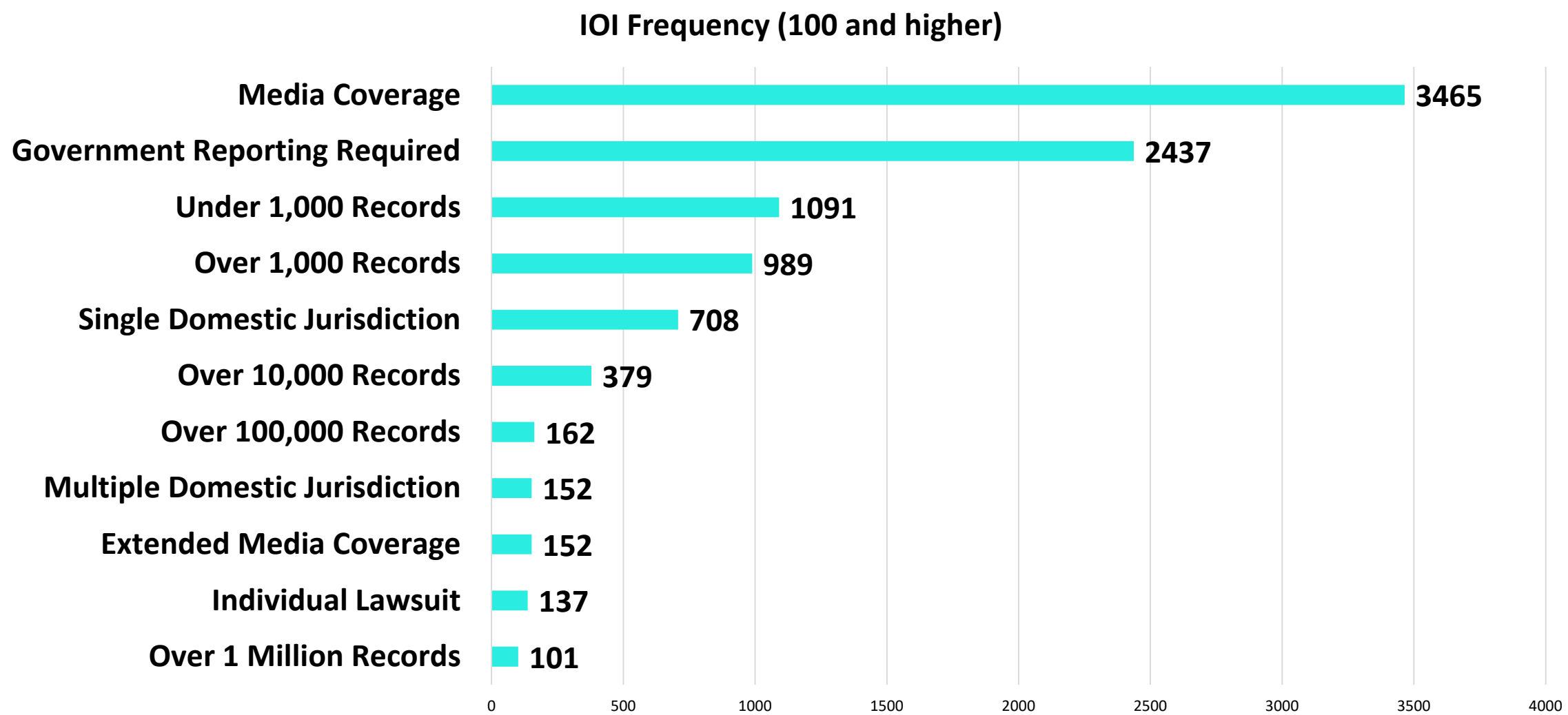
How This Study Measures Impact

Methodology
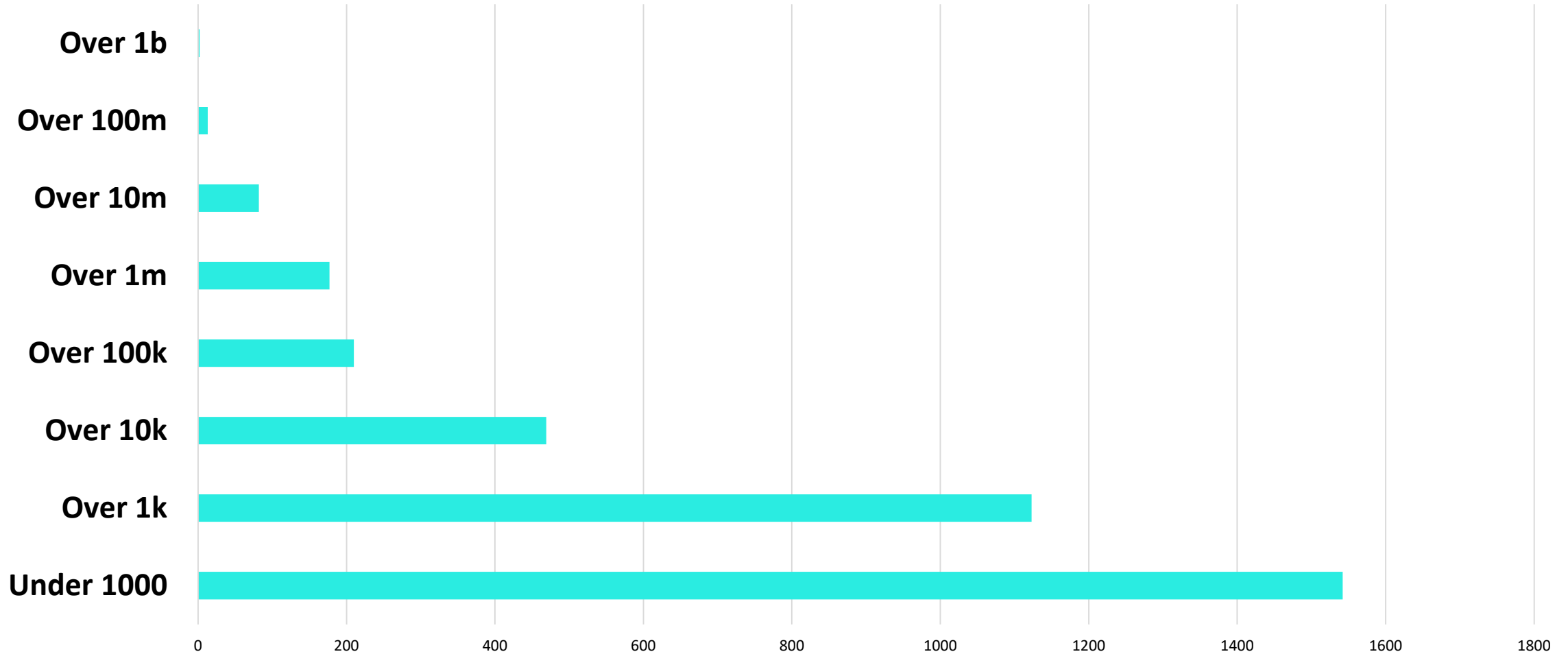
Data source:
VERIS Community Database Project

US incidents

Known # of Records

Publicly disclosed breach Reports

Indicators of Impact

Frequency of Indicators

IOI Frequency (100 and higher)

Indicator	Frequency
Media Coverage	3465
Government Reporting Required	2437
Under 1,000 Records	1091
Over 1,000 Records	989
Single Domestic Jurisdiction	708
Over 10,000 Records	379
Over 100,000 Records	162
Multiple Domestic Jurisdiction	152
Extended Media Coverage	152
Individual Lawsuit	137
Over 1 Million Records	101

verizon✓

RSAConference2019

Distribution of Record Loss

Record Loss Size Distribution

verizon✓

RSA®Conference2019

Case Study #1

Distribution of Impact Scores
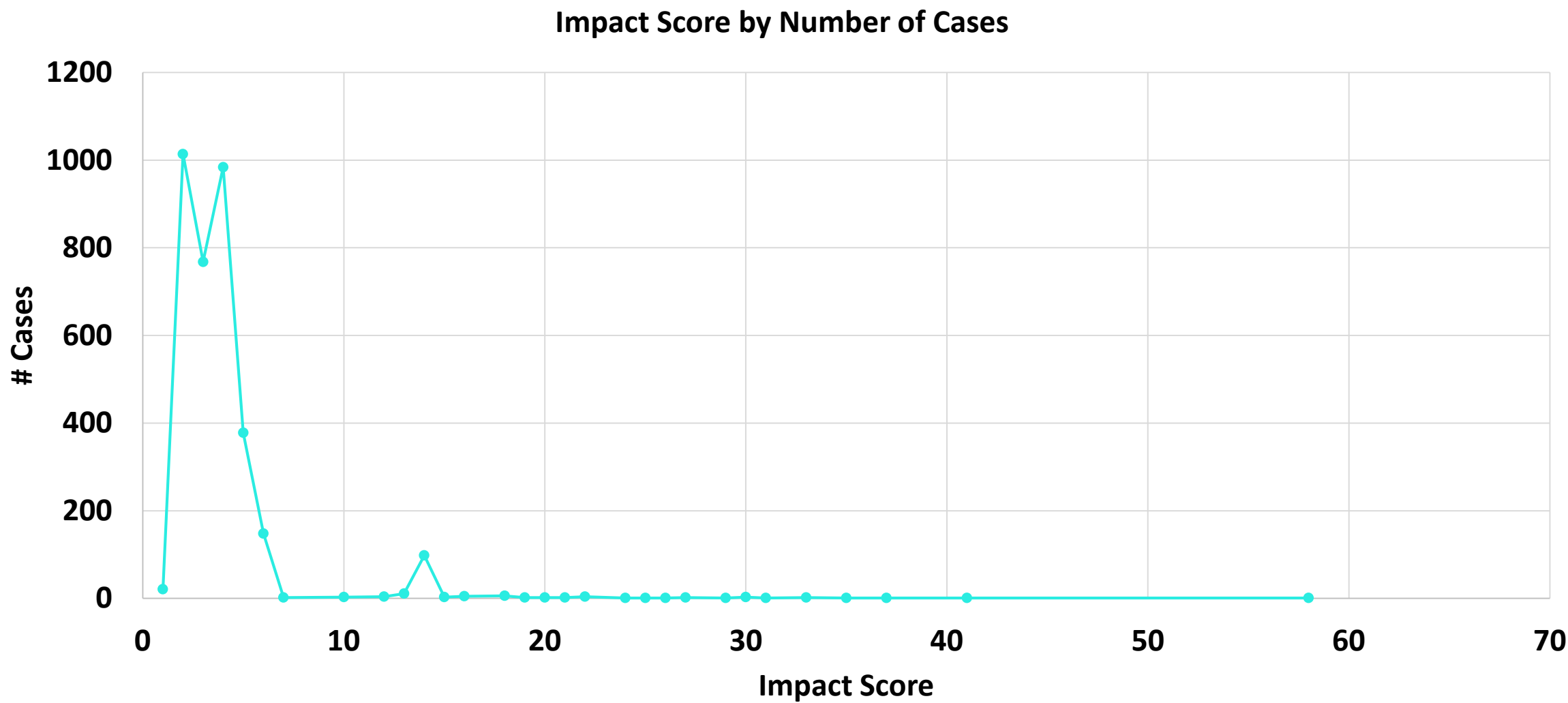
Impact Score by Number of Cases

The Breach Impact Scale

Breach Impact Scale (1/3)

Scale Level	Score Range	Impact Description	Potential Characteristics
0	0-2	Light Impact	Minimal media attention; low number of data victims; data involved not highly valued.
1	2-5	Moderate Impact	Minimal media attention; over 1,000 data victims; data involved minimally monetizable.
2	5-7	Considerable Impact	Single jurisdiction for litigation; potential for legal settlements or regulatory fines; data involved lucrative for financial crimes; number of data victims under 1 million.

verizon✓   RSAConference2019

Breach Impact Scale (2/3)

Scale Level	Score Range	Impact Description	Potential Characteristics
3	7-10	Severe Impact	Class action litigation in single jurisdiction; multiple domestic jurisdictions for individual litigation; enhanced media coverage; regulatory fines and legal settlements; number of data victims under 1 million; data disclosed may have been highly sensitive
4	11-15	Devastating Impact	Organization or partner extinction event for small organizations; bankruptcy protection may be sought for small orgs; class action litigation in multiple jurisdictions; international scope of breach; over 1,000,000 data victims.

verizon✓

RSA Conference2019

Breach Impact Scale (3/3)

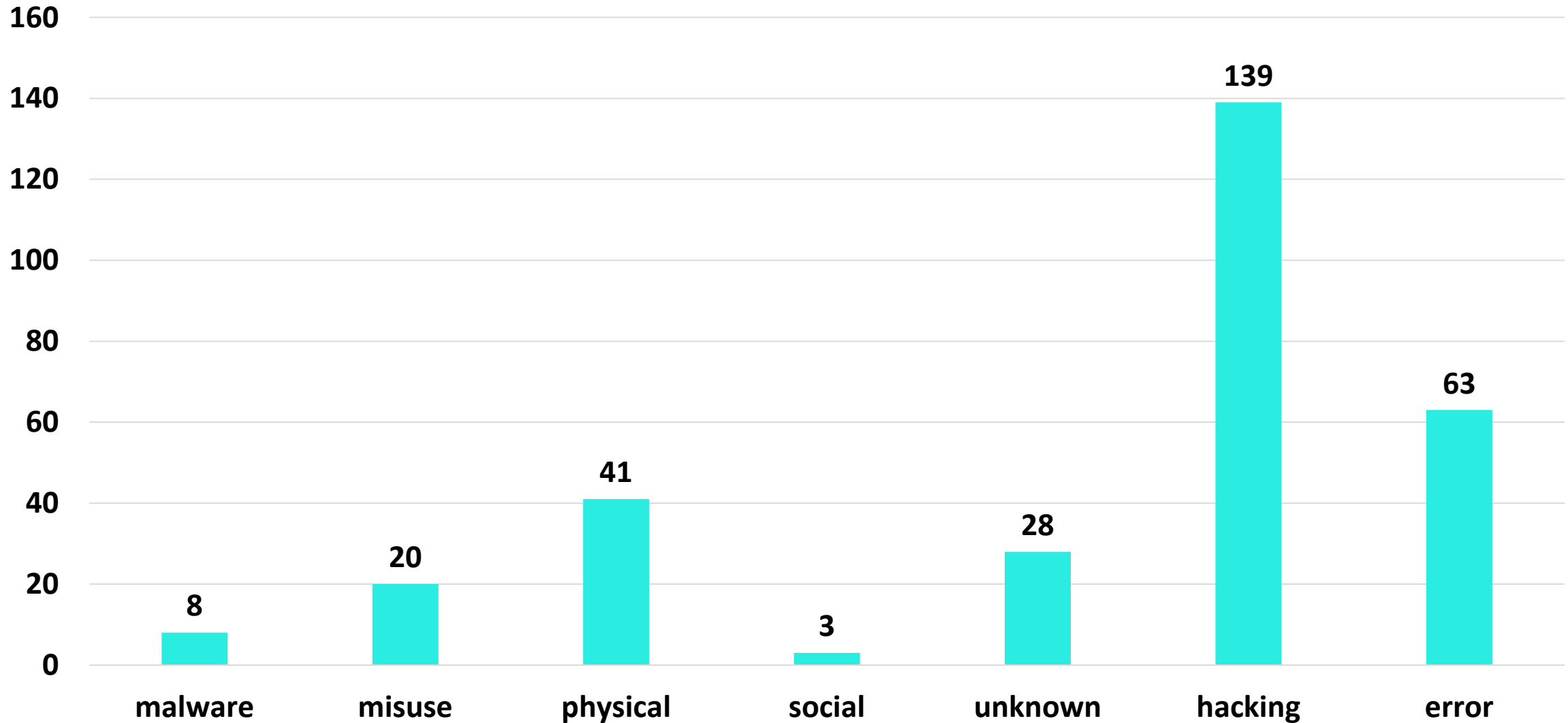| Scale Level	Score Range	Impact Description	Potential Characteristics
5	16-30	Incredible Impact	Potential organization extinction event for medium sized organization; potential partner extinction event; significant resources for litigation; potential for new laws created affecting organization's industry.
6	31+	Inconceivable Impact	Potential organization extinction or near extinction event for large enterprise; significant disruption to normal operations; potential for new laws created affecting multiple industries.

verizon✓

RSA Conference2019

Case Study #2

MARRIOTT DATA BREACH

Findings

High Impact Scores: Actions

	160
140	139
120	
100	
80	
60	63
40	41
20	20 28
0	8 3

malware   misuse   physical   social   unknown   hacking   error

RSAConference2019

High Impact Scores: Hacking Distribution

Frequency of Hacking Varities

verizon

RSAConference2019
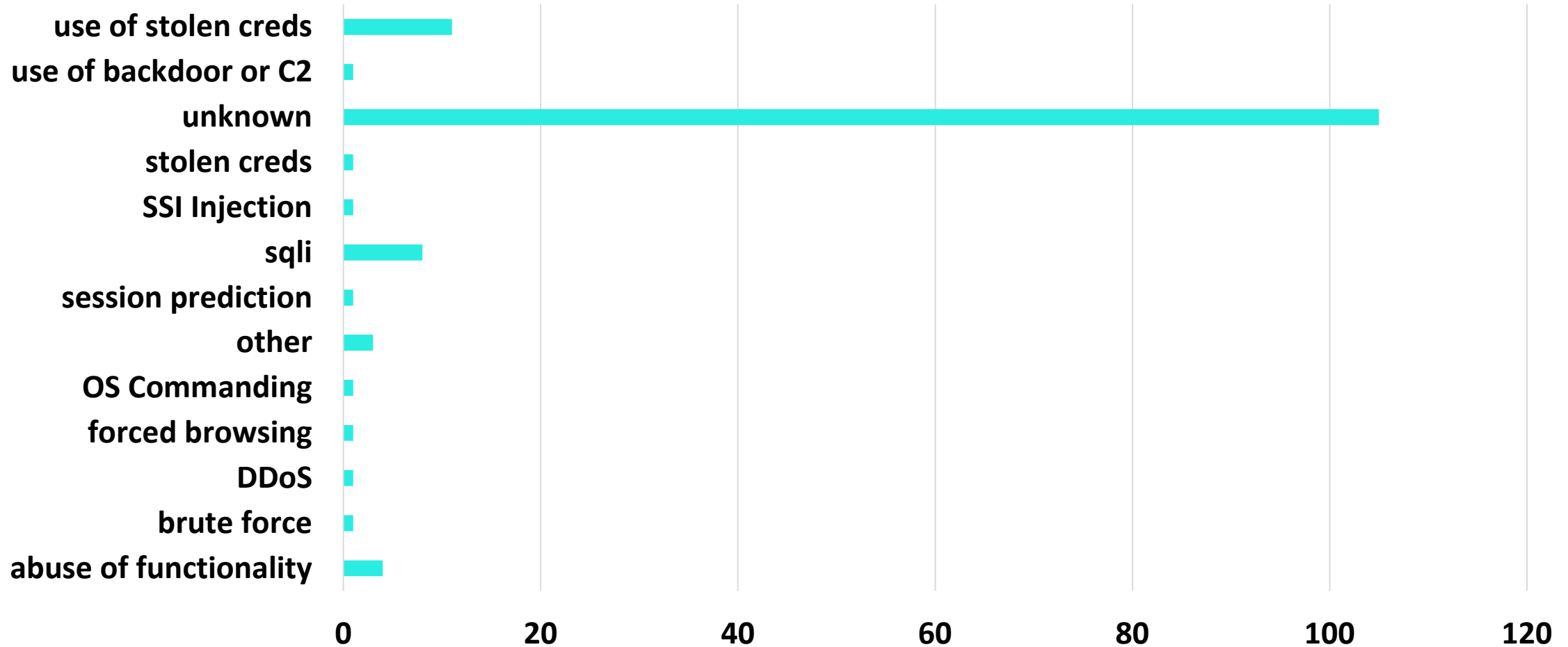
Case Study #3

YAHOO!

abc NEWS

1 BILLION USER ACCOUNTS MAY HAVE BEEN COMPROMISED

verizon

18

RSA Conference 2019

High Impact Scores: Discovery Methods
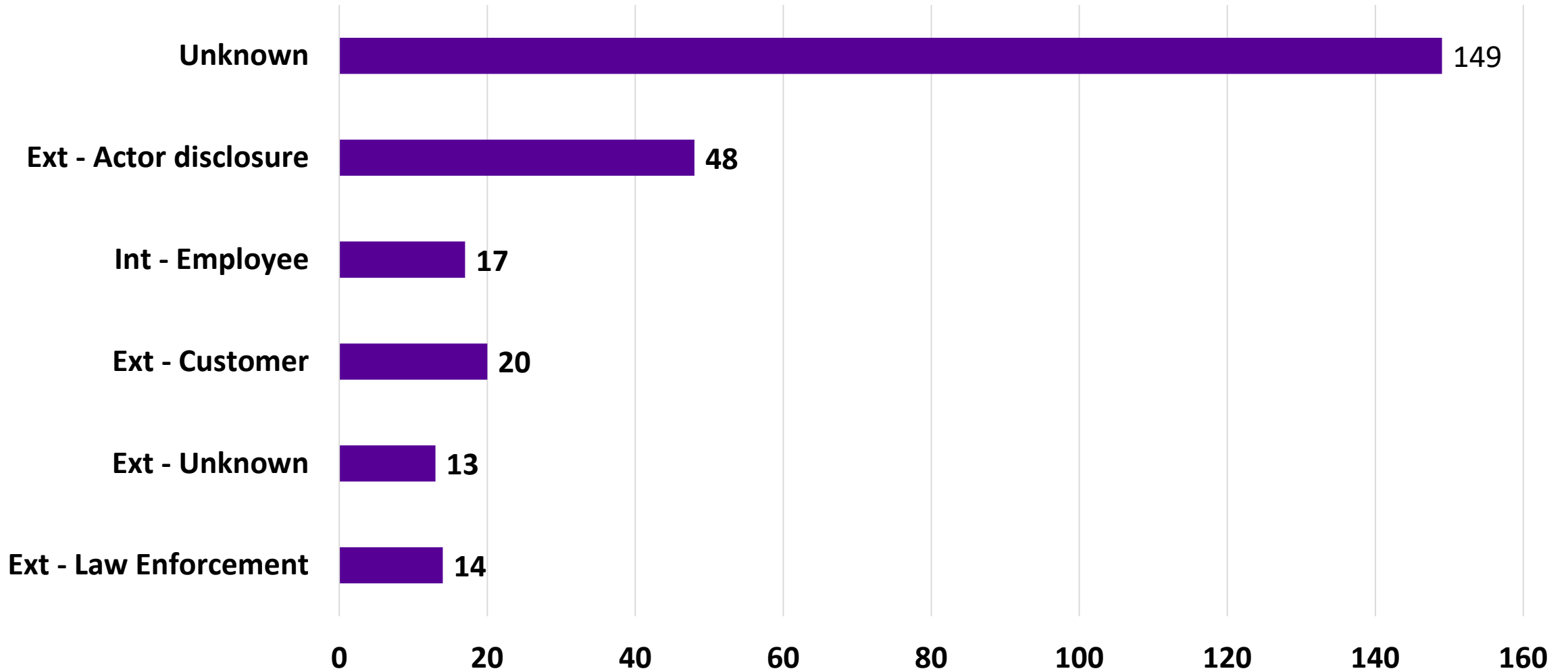
High Impact Scores: Error Distribution
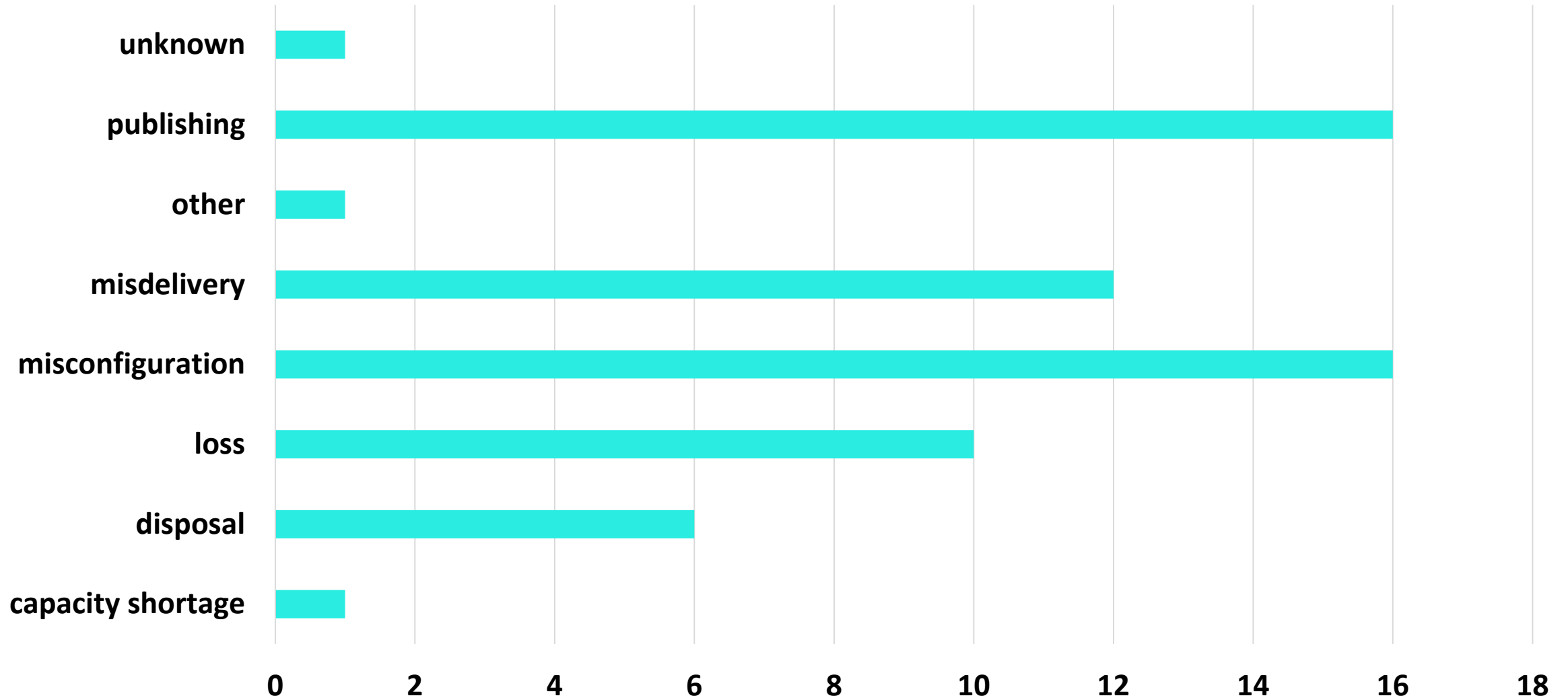
High Impact Scores: Industries

Top Scored Industries

verizon✓

RSA Conference2019
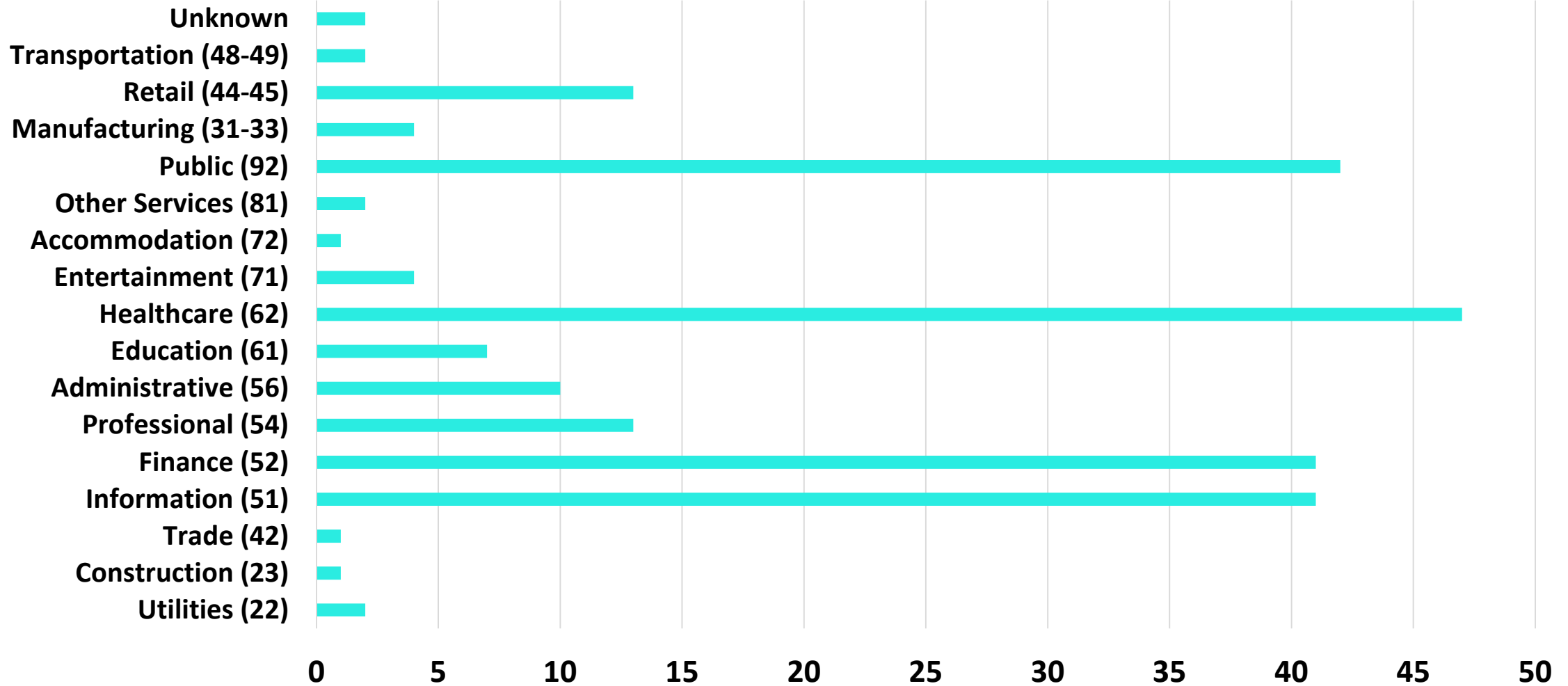
Case Study #4
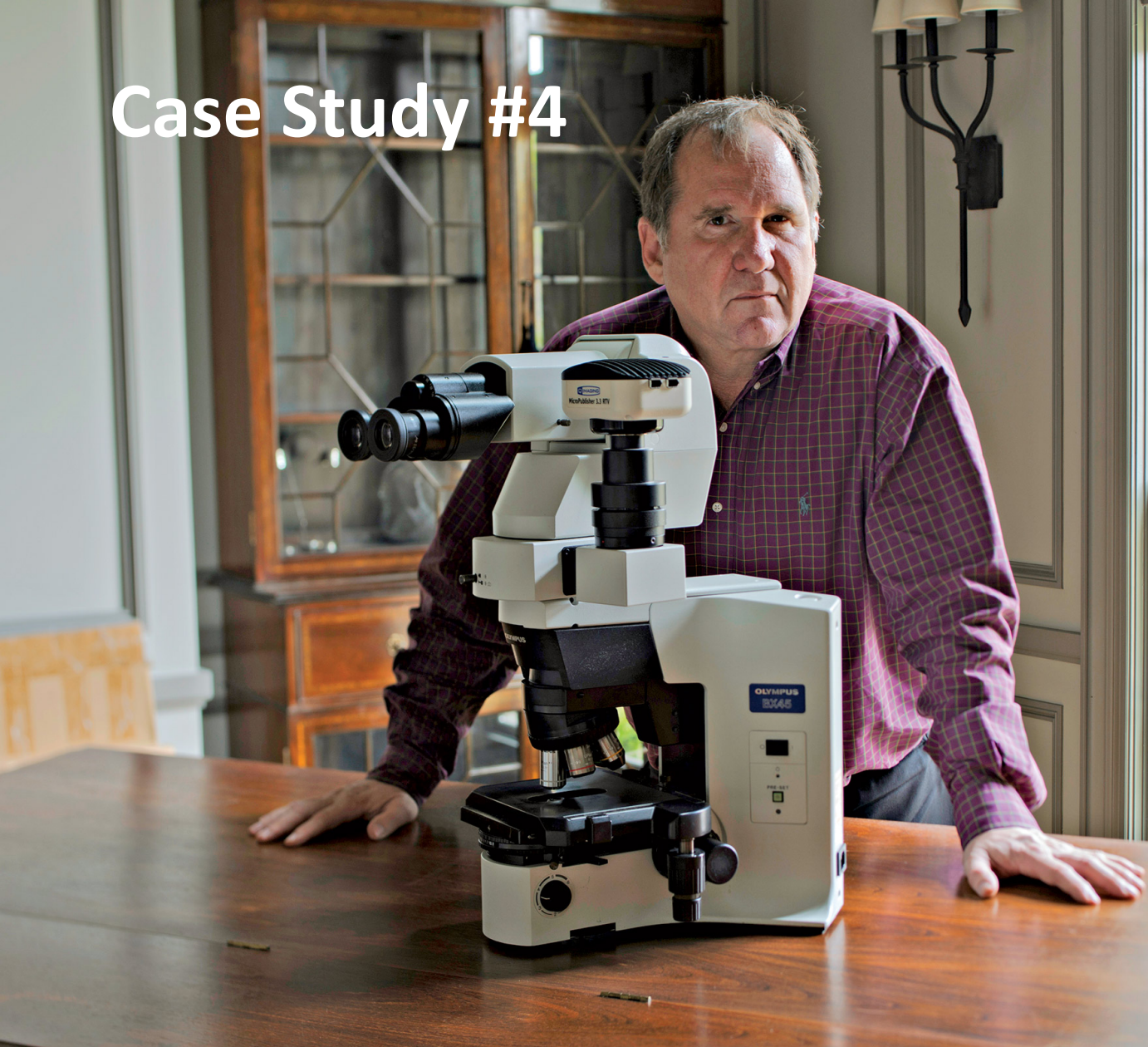
Apply What You Have Learned Today

- **How can you use this?**
  - How do you measure impact of breach risk in your organization?
  - How are these measurements communicated to management?

- **In the first three months following this presentation you should:**
  - Understand how your organization measures risk of breach
  - Determine which of these indicators apply to your situation
  - Include your findings in your management communications and evaluate how they can be used to better your security posture.

verizon✓

RSA Conference2019

Apply What You Have Learned Today

- **Within six months you should:**
  - Incorporate risk indicators into your IR planning
  - Determine if these indicators change your risk calculations
  - Expand your incident response planning to account for relevant new risks
  - Incorporate feedback from management about the communications you are providing and enhance as needed

verizon✓

RSA®Conference2019

Considerations

- These cases take a long time for some of these indicators to surface.

- Some settlements are not publicized.

- This dataset is continuing to evolve.

verizon✓

RSA Conference2019

Future Research

- How to handle unknown number of records

- Look at international incidents (different legal framework)

- Refine/bring more rigor to weighting

- Can we use this to make a predictive model?

verizon√

RSAConference2019

Resources for More Information

- VERIS Community Database Project: https://github.com/vz-risk/VCDB

- Impact Scale Research Dataset: https://github.com/swidup/Breach-Impact-Scale

- Case Study json:
  - Equifax: 957d1a6c-de24-41d0-8d09-d72157da4848.json
  - Yahoo: 7DA7CEC9-4052-4878-8EFA-44673719DAC6.json
  - Marriott: 160bd508-2d5d-435b-9e12-c58dd028ba6e.json
  - LabMD: 1F7FBF08-8CE3-4C08-A274-E62C7A07ED80.json

verizon✓

RSA Conference2019

Questions?

- Contact info:
  - Twitter: @SuzanneWidup
  - Email: suzanne.widup@verizon.com

verizon✓

RSA®Conference2019