RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-T09R

We’re Not in Kansas Anymore: Measuring the Impact of a Data Breach (Repeat)

Suzanne Widup

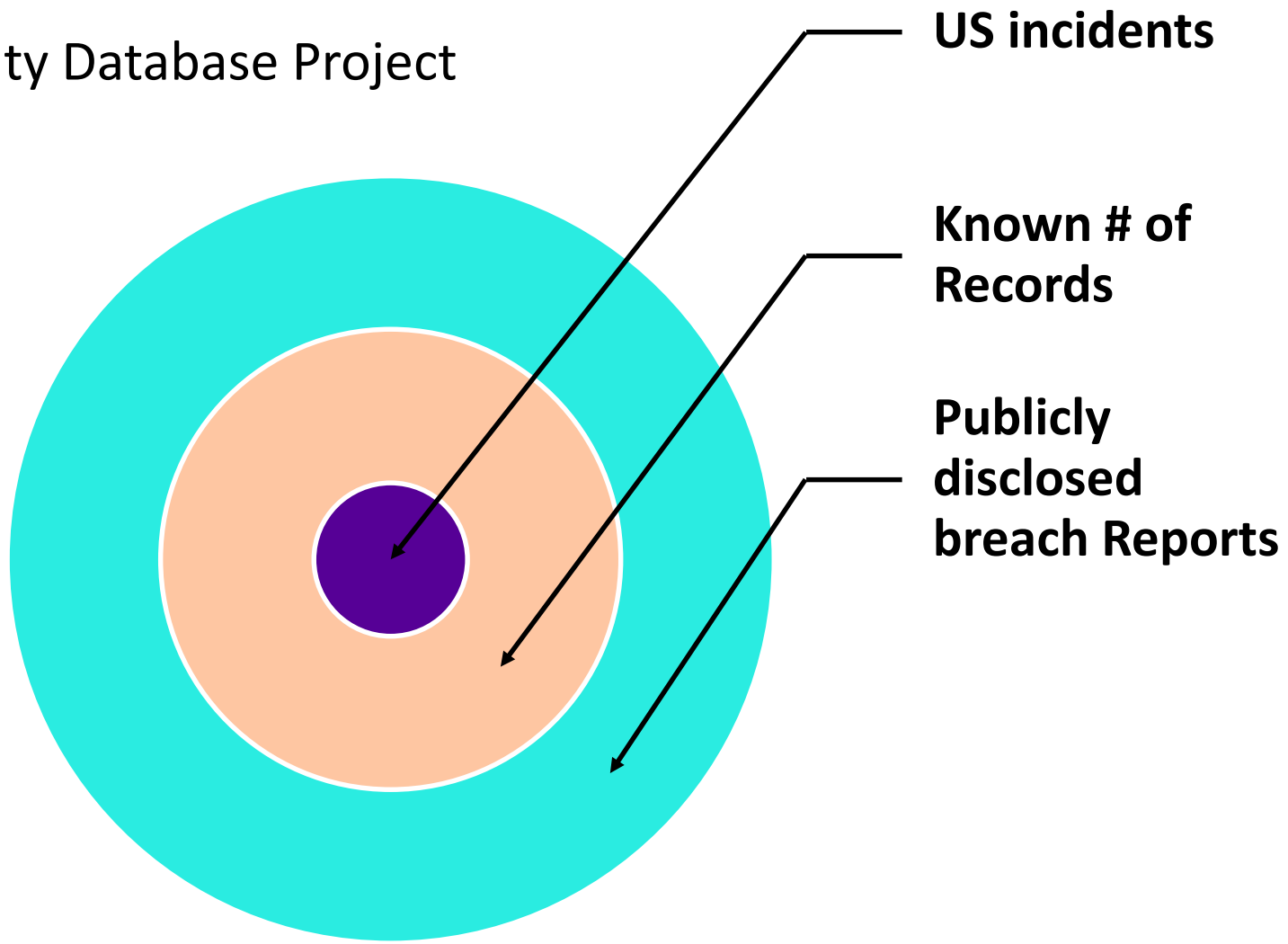
Senior Analyst, DBIR Co-Author
Verizon Enterprise Solutions
@SuzanneWidup

How Breach Impact Has Been Measured in the Past

How This Study Measures Impact

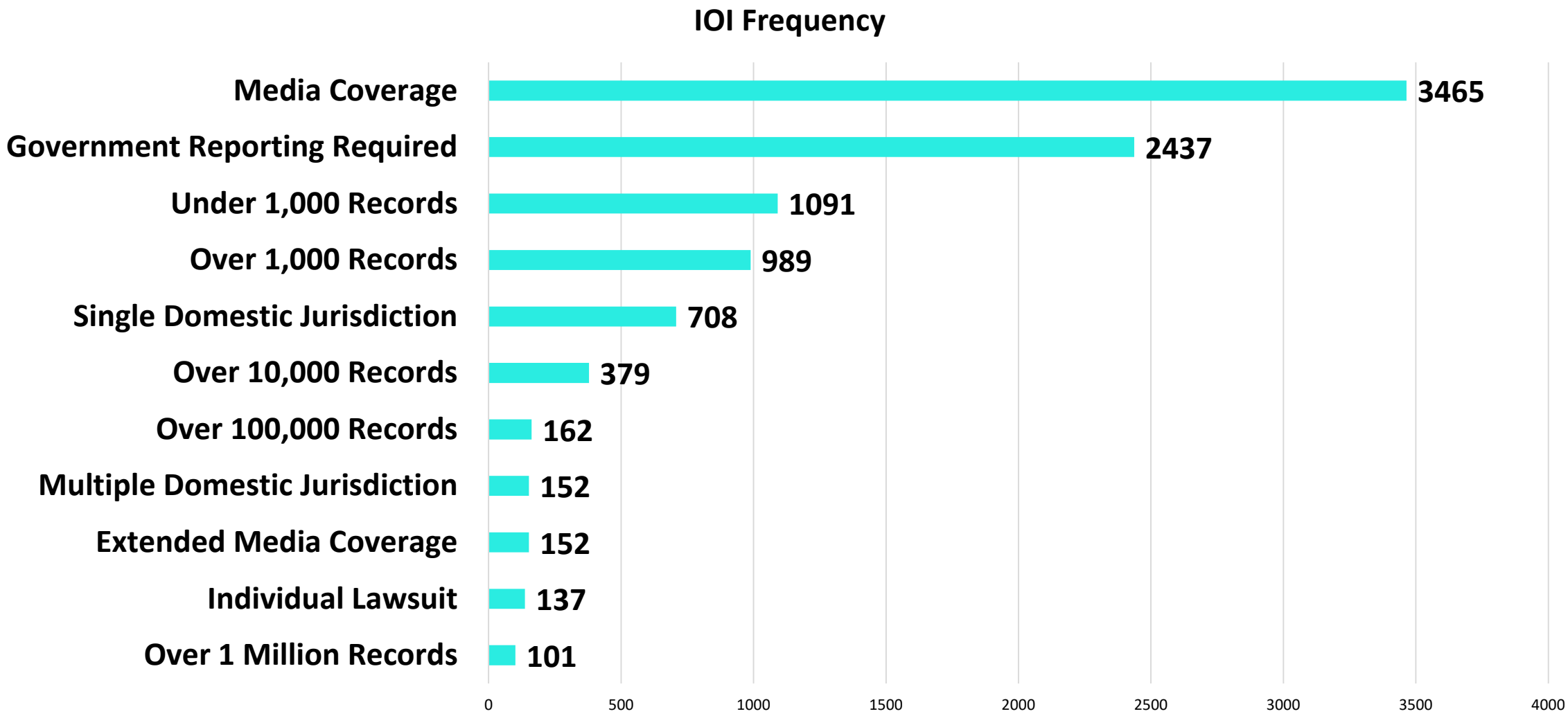
Methodology

Data source:
VERIS Community Database Project

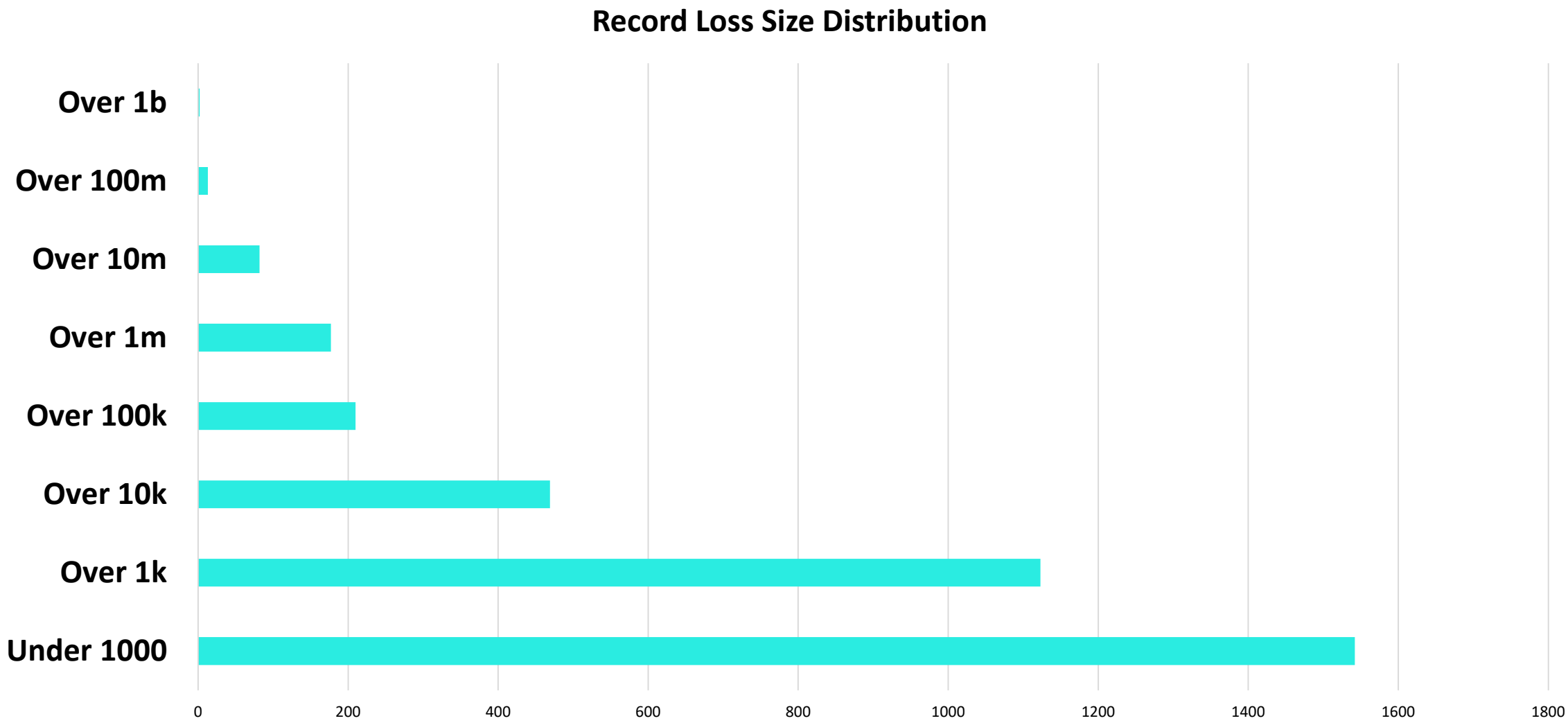


Indicators of Impact

Frequency of Indicators

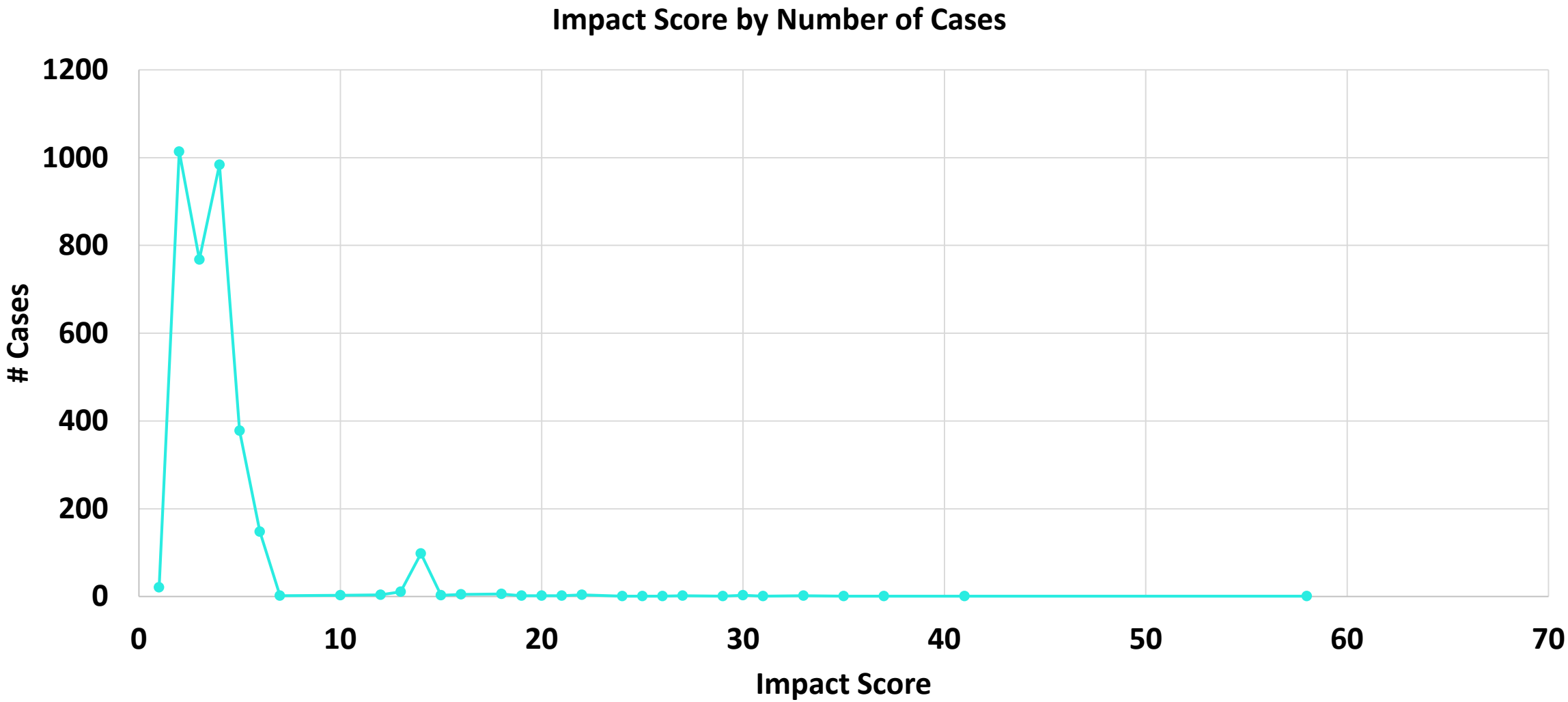


Distribution of Record Loss

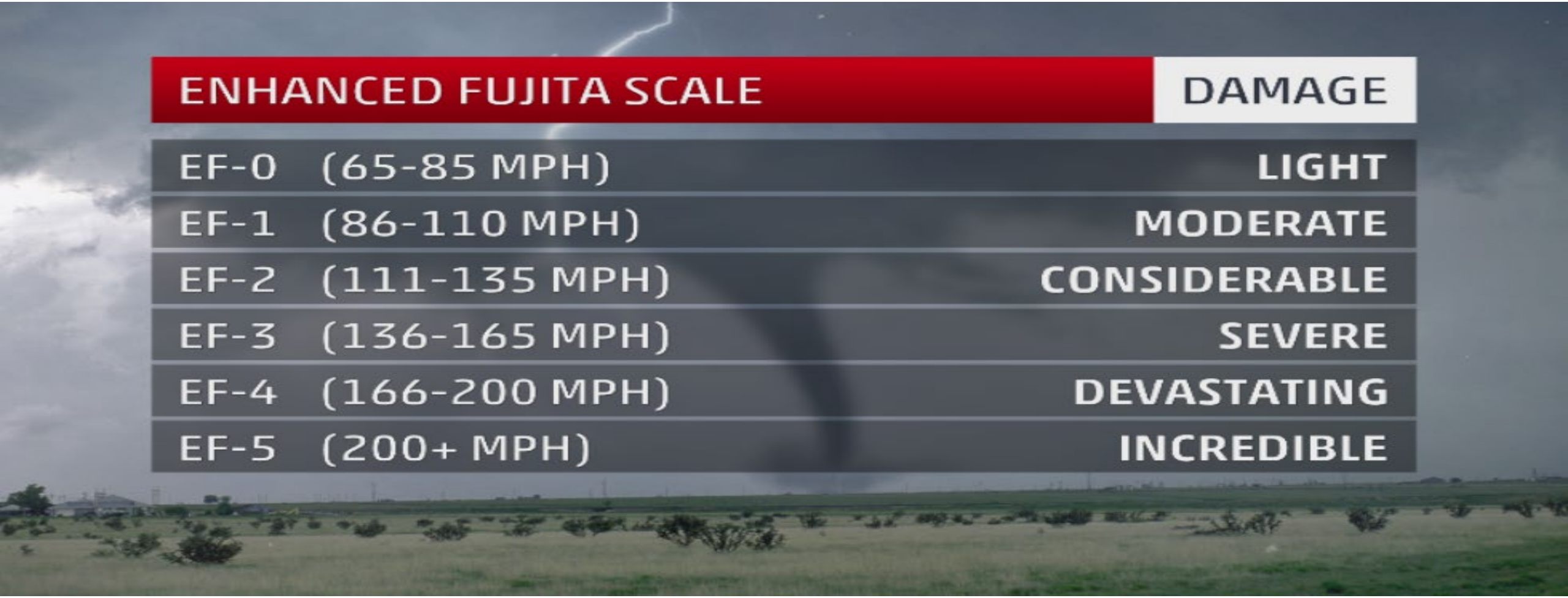


Case Study #1

Distribution of Impact Scores



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.

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.

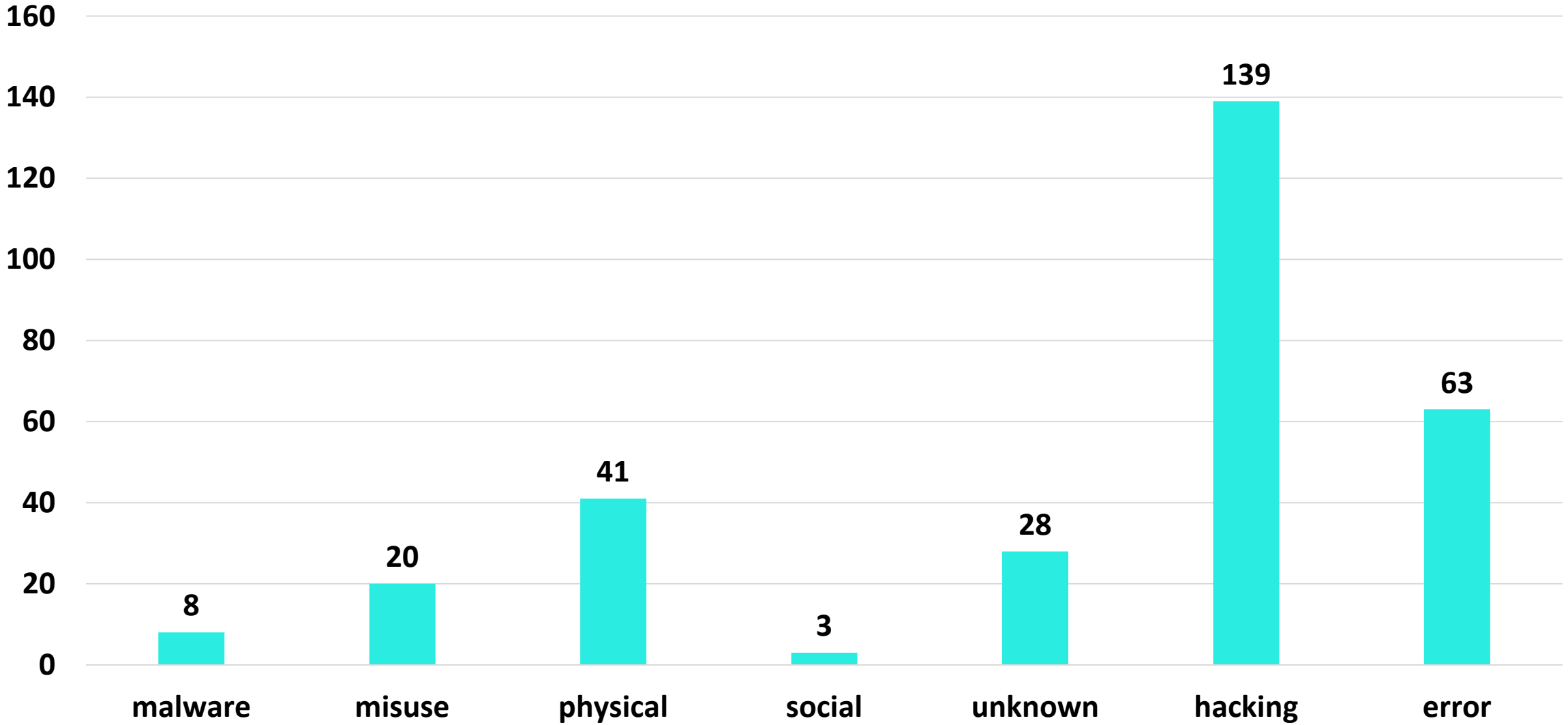
Breach Impact Scale (3/3)

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.

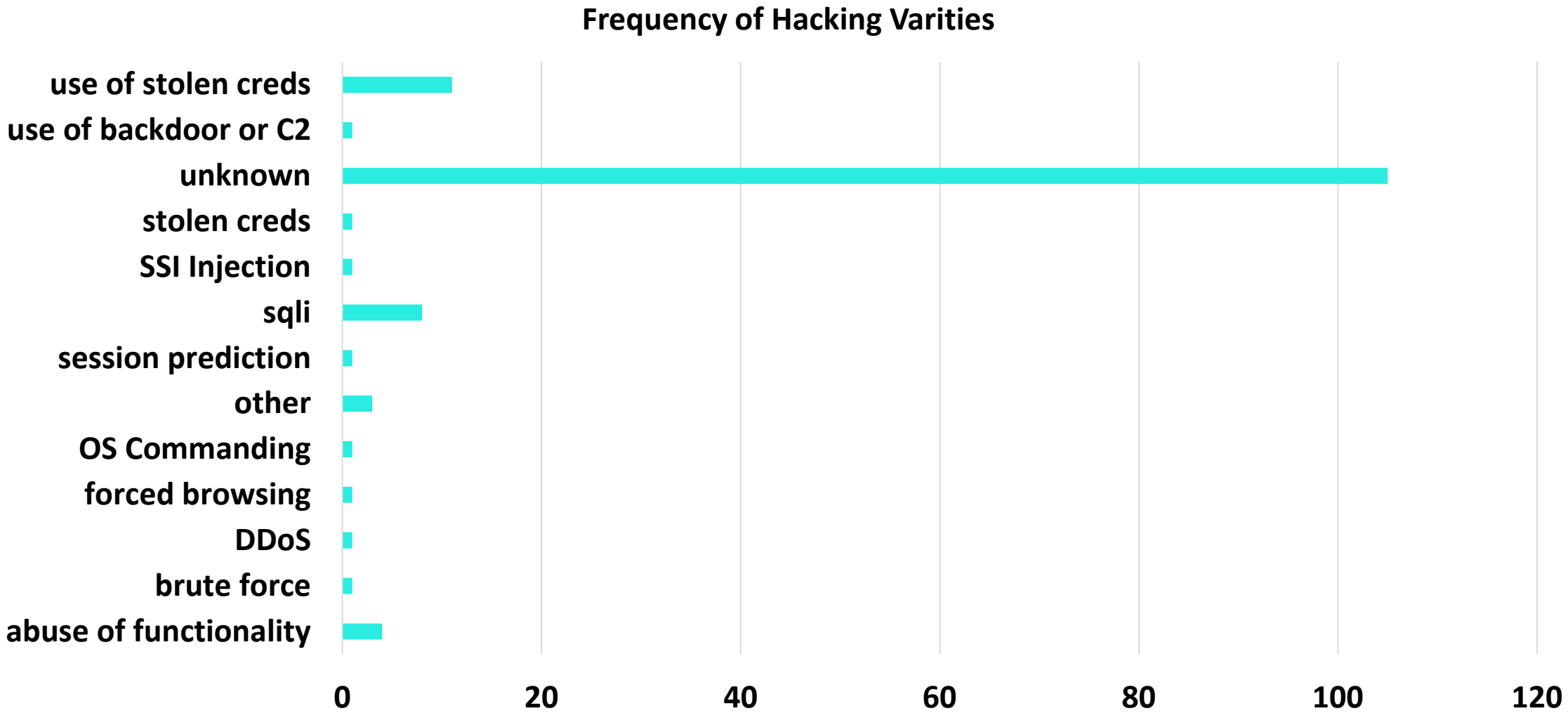
Case Study #2

Findings

High Impact Scores: Actions



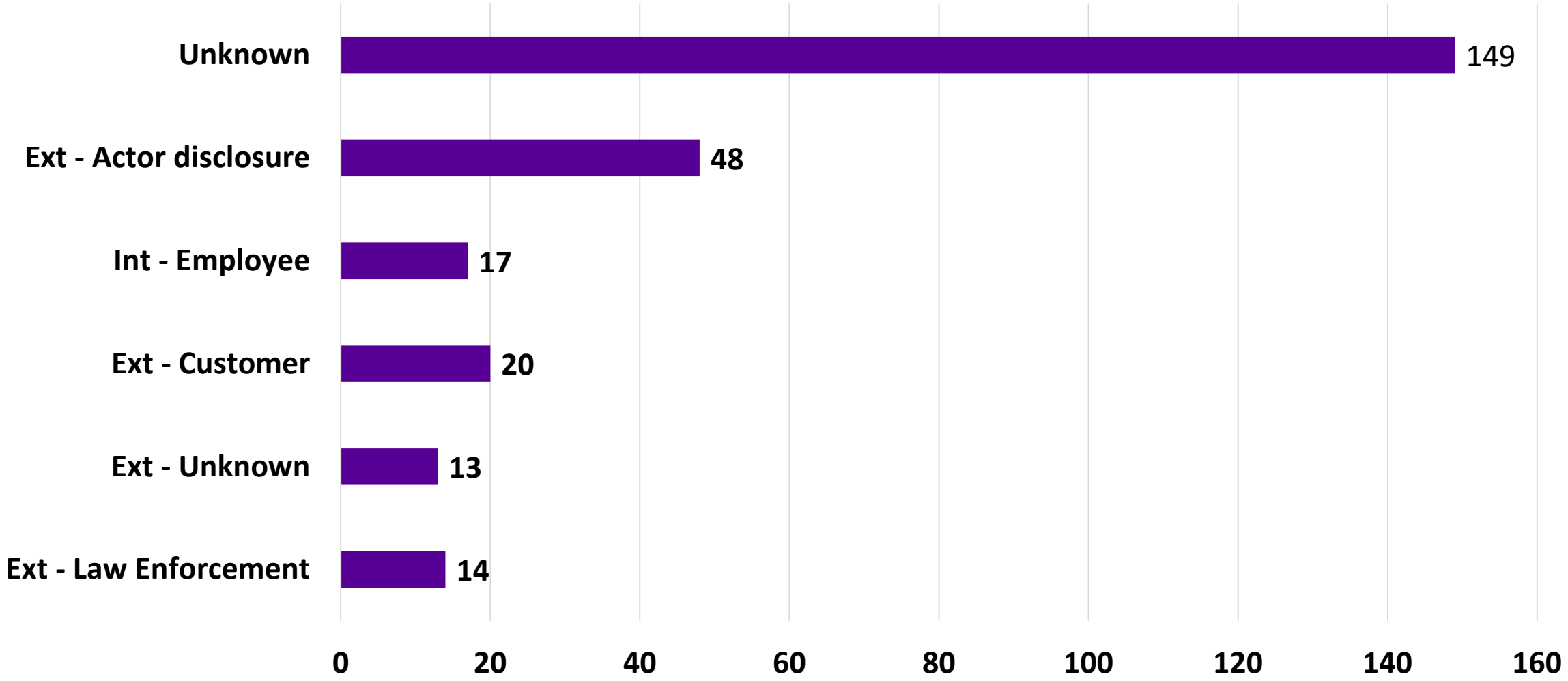
High Impact Scores: Hacking Distribution



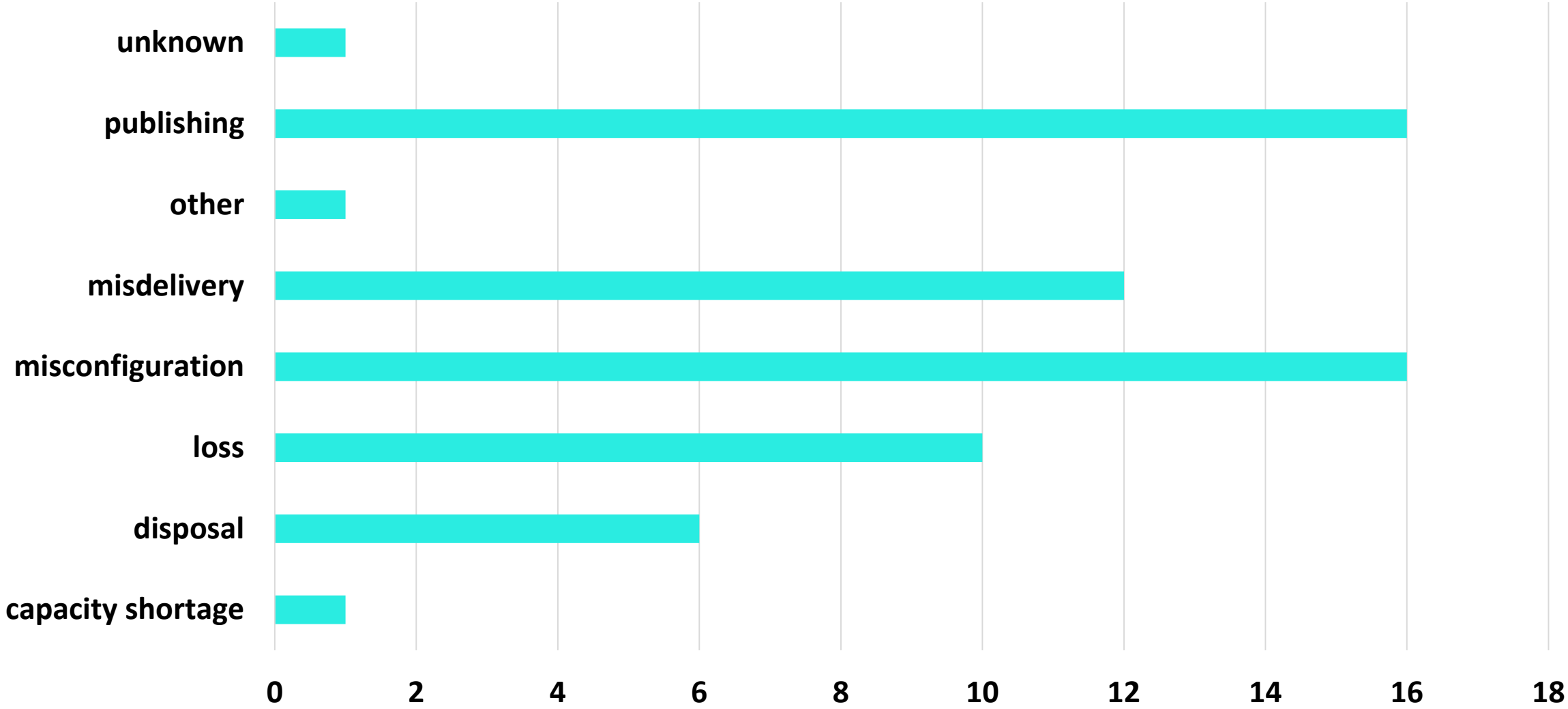
Case Study #3


YAHOO!
abc NEWS
1 BILLION
USER ACCOUNTS
MAY HAVE BEEN
COMPROMISED

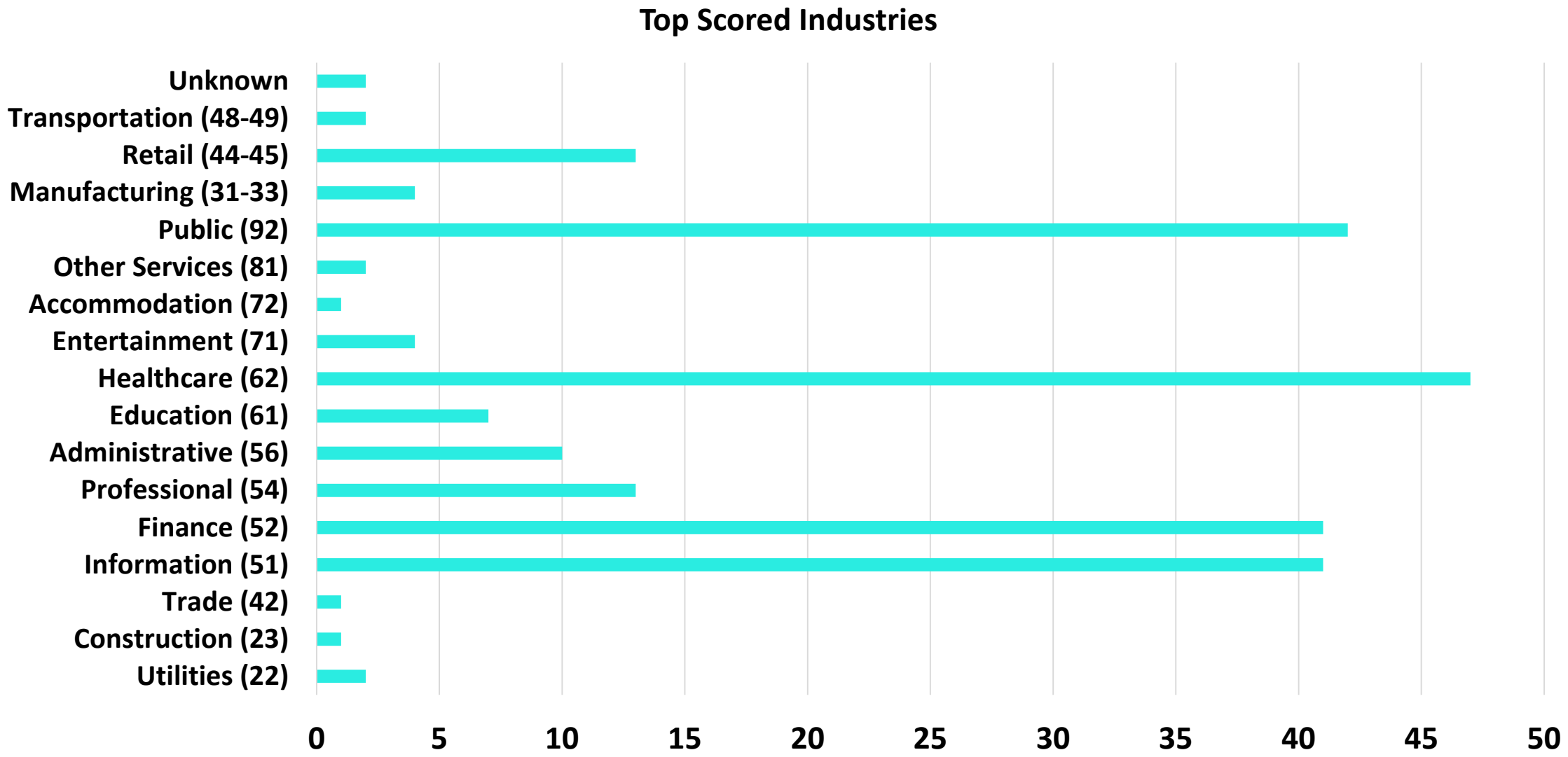
High Impact Scores: Discovery Methods



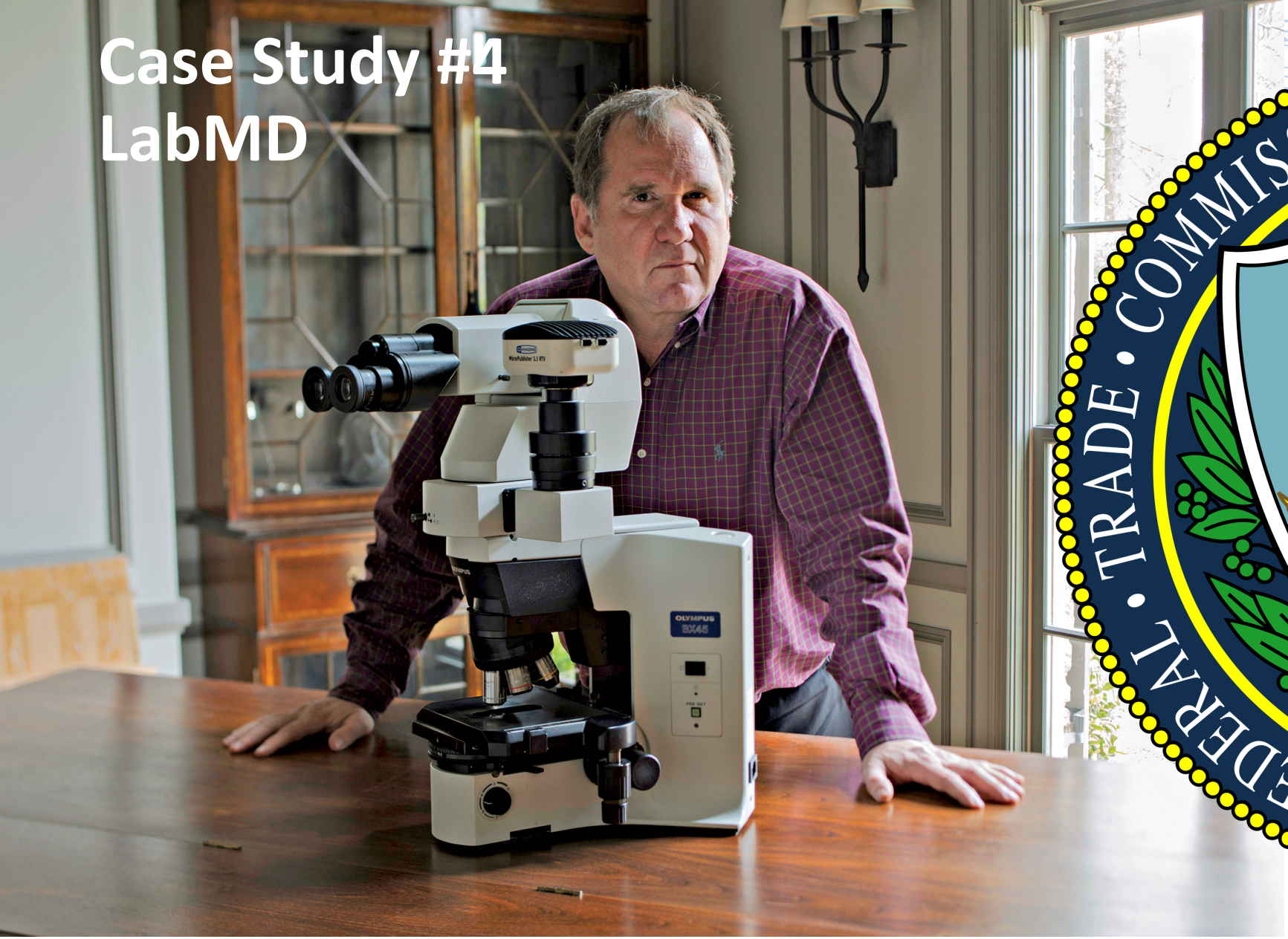
High Impact Scores: Error Distribution



High Impact Scores: Industries



Case Study #4
LabMD



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.

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

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.

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?

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

Questions?

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

  - Twitter: @VERISDB for running data breach feed as I find them