RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PDSC-M05**

# What the Headlines Don’t Tell You About Supply Lines

**David Severski**
Senior Risk Data Scientist
Cyentia
@dseverski

**Jonathan Ehret**
SVP, Strategy and Risk
RiskRecon, A MasterCard Company

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

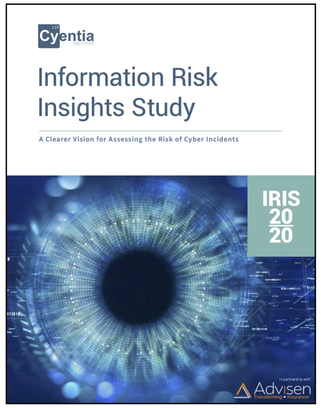
# Some of these things are not like the other..

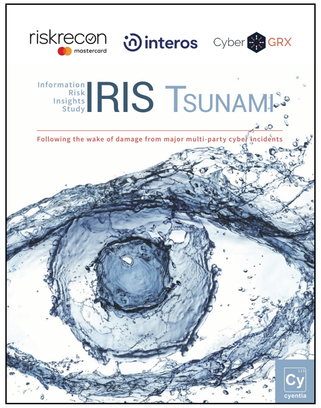


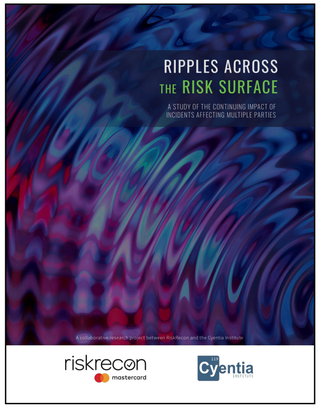
Supply chains? Vendor issues? Multiparty events?

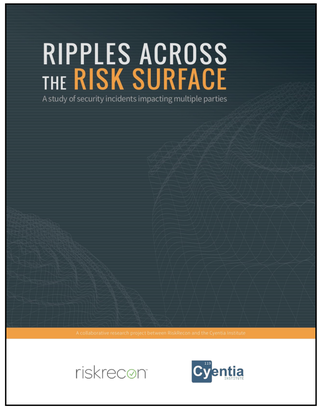
# Cyentia and RiskRecon – A research partnership

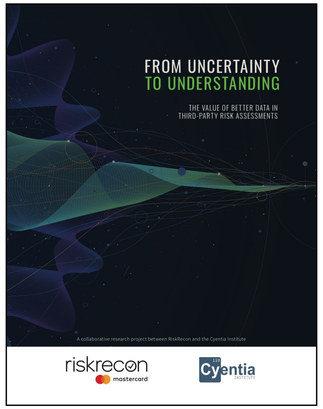
- IRIS 20/20 and IRIS Tsunami
- Ripples across the Risk Surface
  - Two editions!
- State of Third-Party Risk Management
- From Uncertainty to Understanding
- Risk Surface
  - 2022 update out next week!



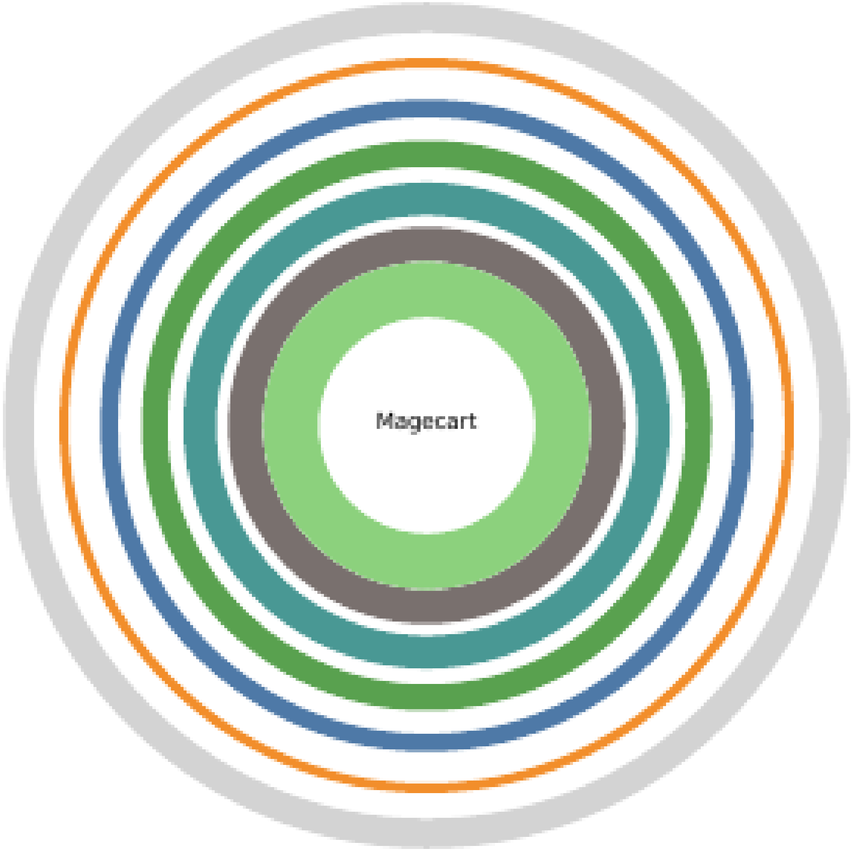



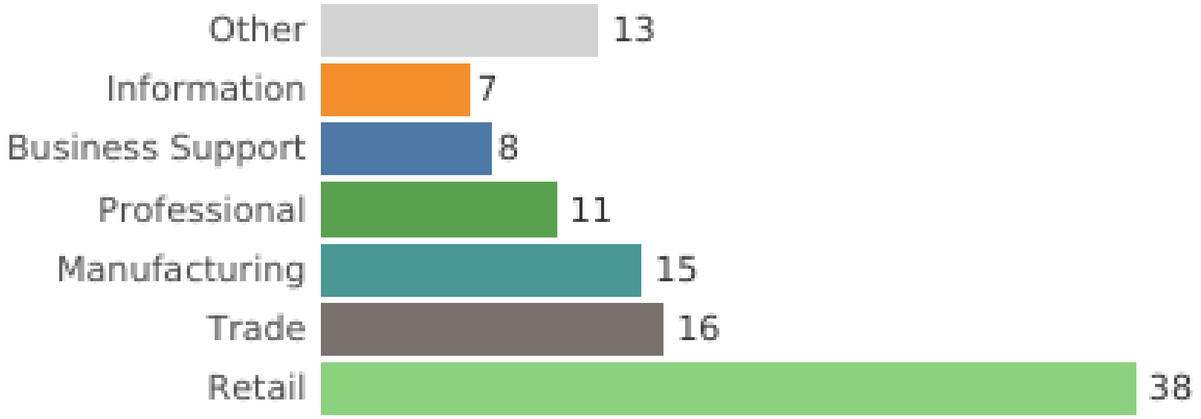




# Just what is a ripple?

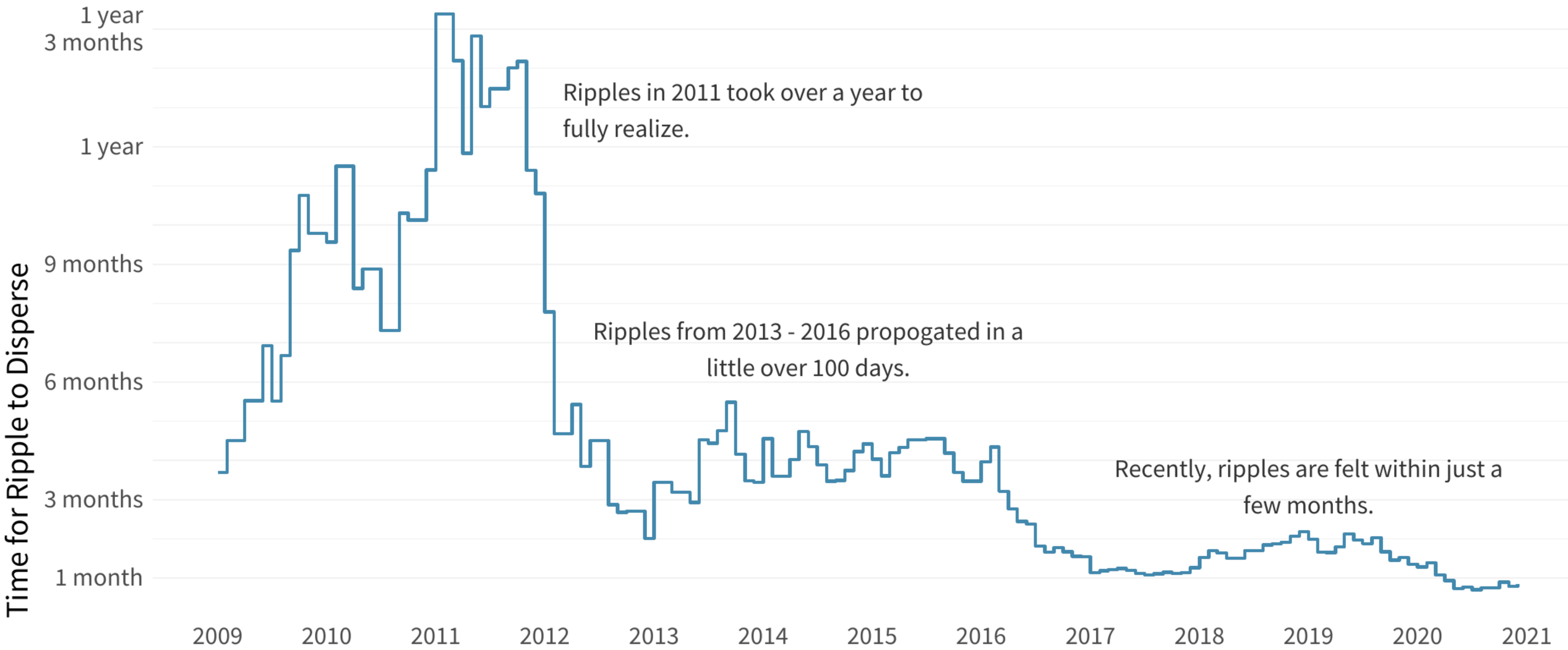


# Where are we getting this data?

A/k/a/ Why should we trust you?

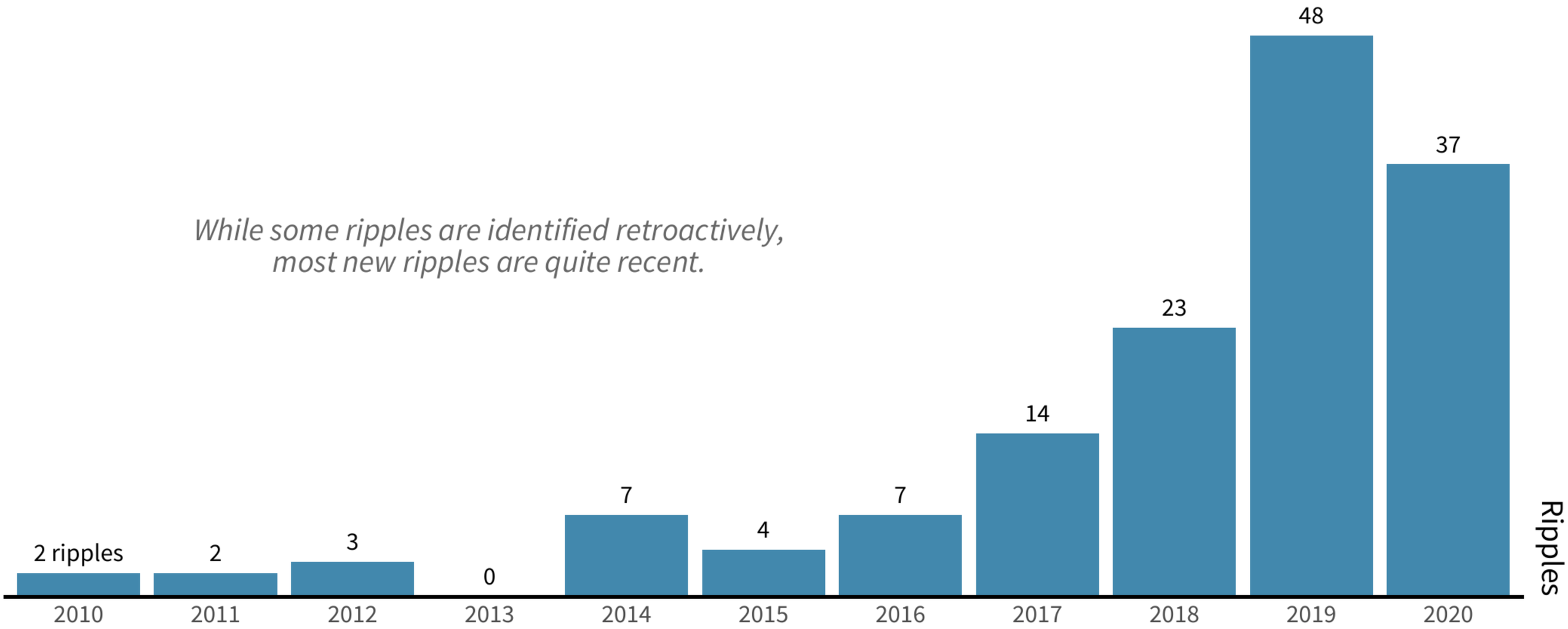

# Time to discovery



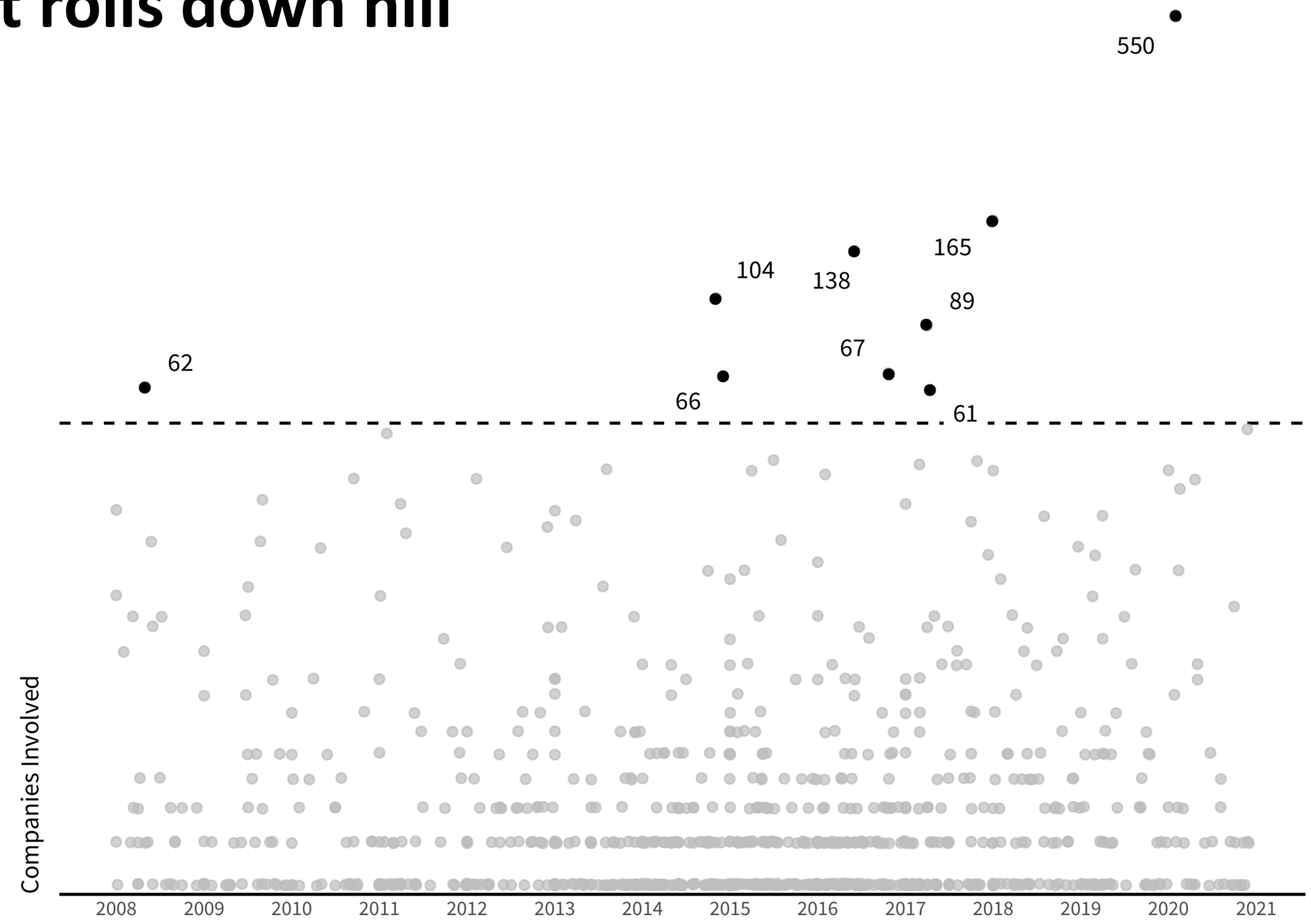
RSAConference2022

# Getting frank with frequency

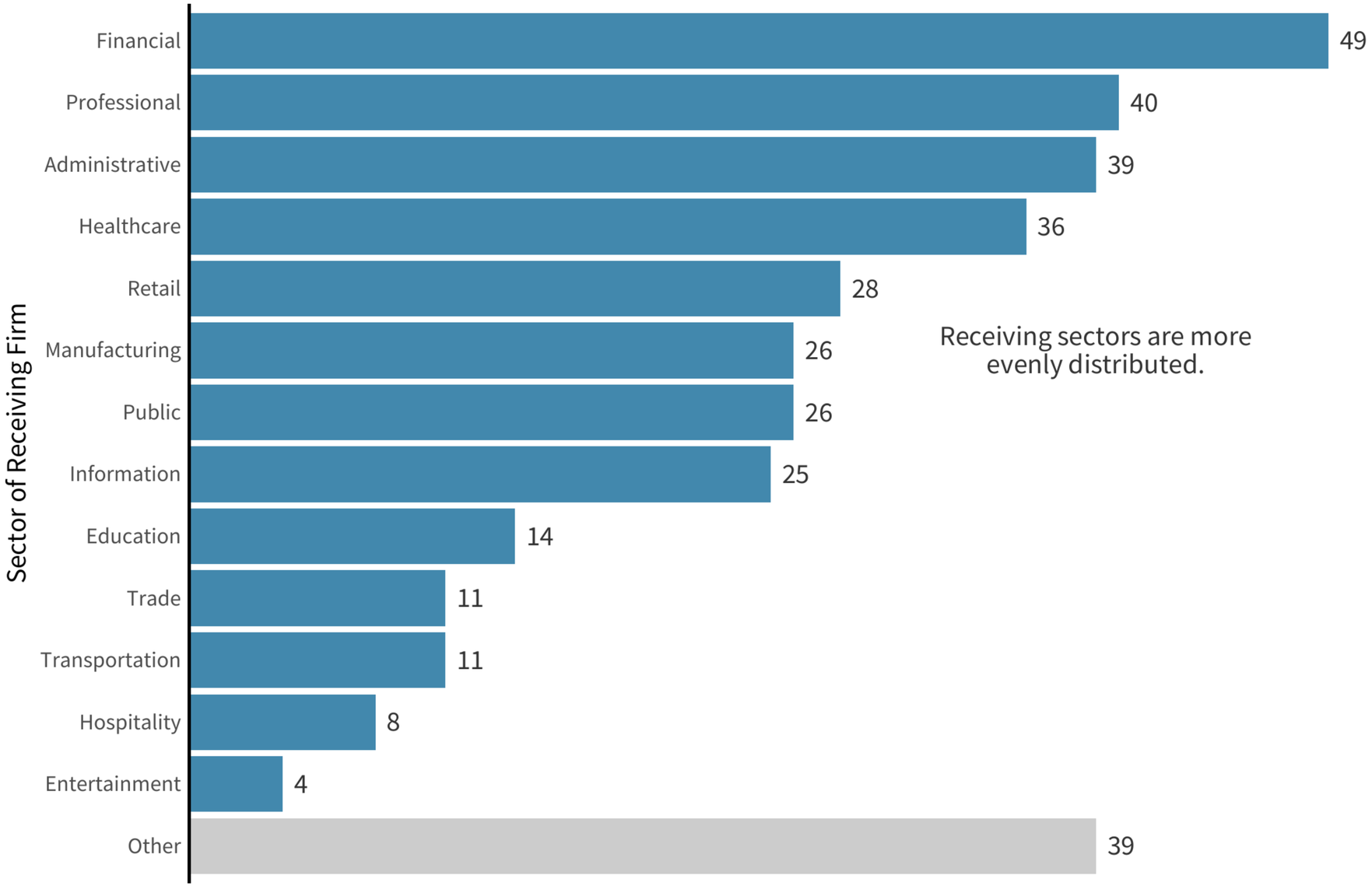
# Ripples through time



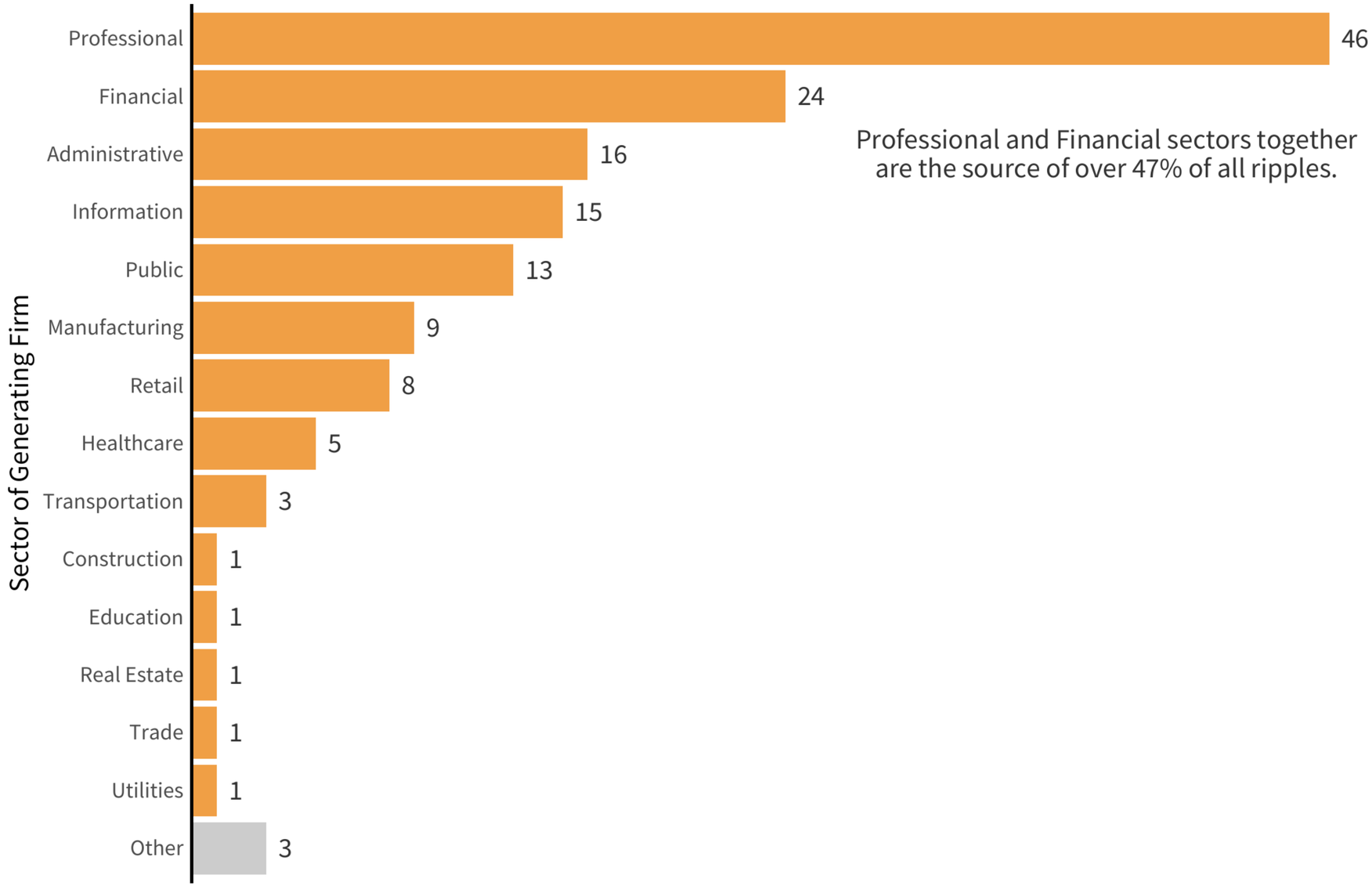
# Impact rolls down hill



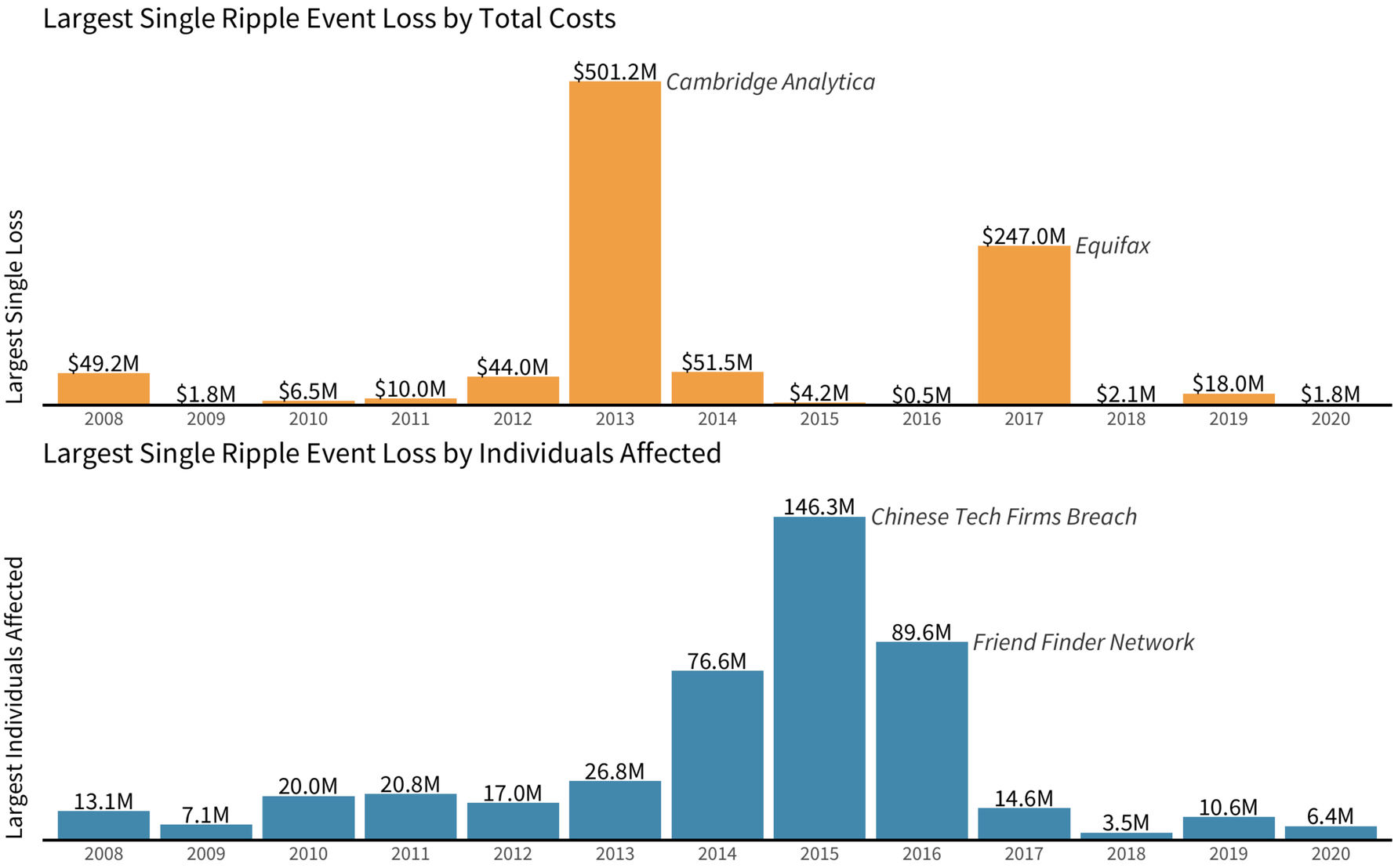
# Receivers

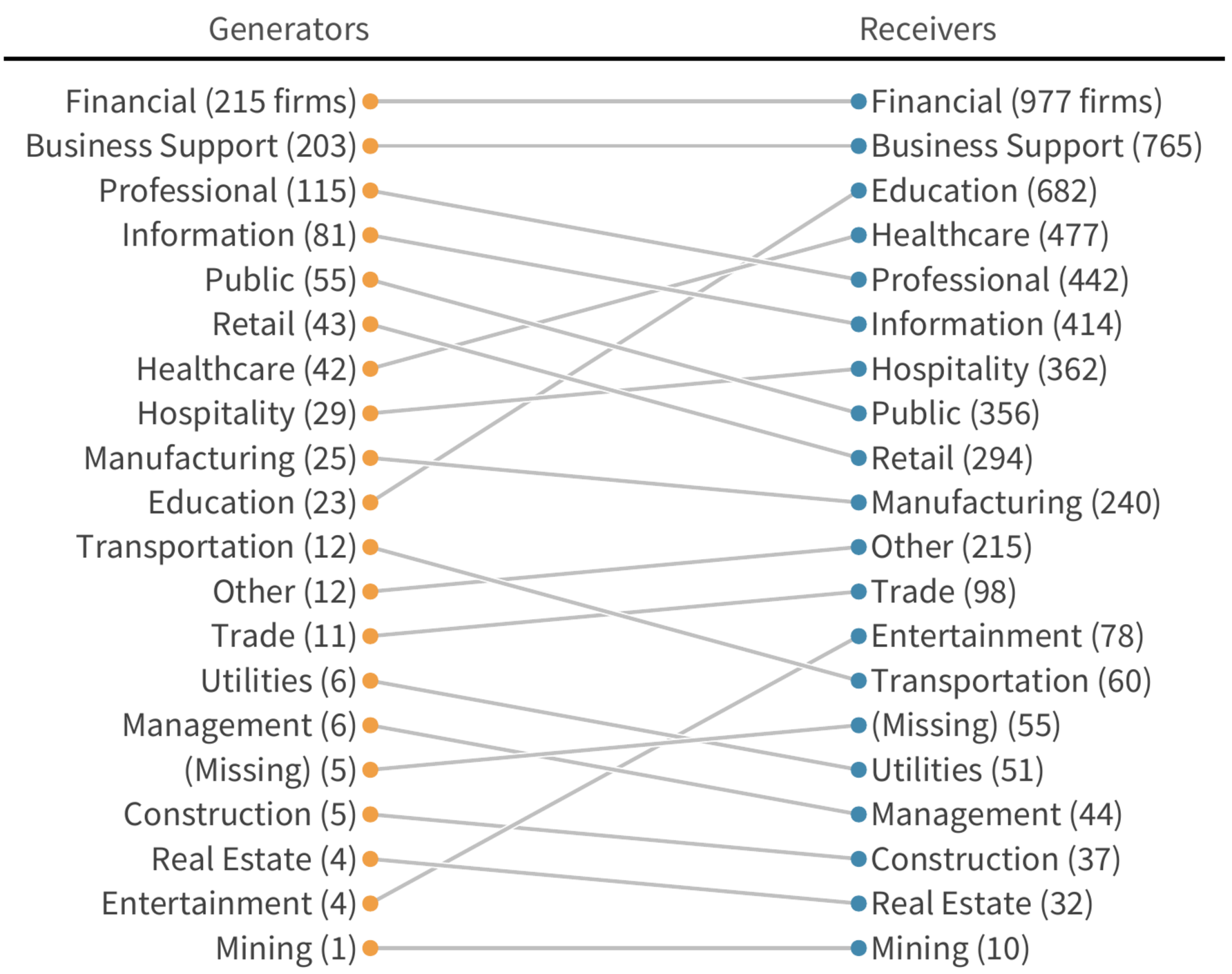

Sector of Receiving Firm
Financial
Professional
Administrative
Healthcare
Retail
Manufacturing
Public
Information
Education
Trade
Transportation
Hospitality
Entertainment
Other
49
40
39
36
28
26
26
25
14
11
11
8
4
39
Receiving sectors are more evenly distributed.

# Generators


Professional
Financial
Administrative
Information
Public
Manufacturing
Retail
Healthcare
Transportation
Construction
Education
Real Estate
Trade
Utilities
Other
Sector of Generating Firm
46
24
16
15
13
9
8
5
3
1
1
1
1
1
3
Professional and Financial sectors together are the source of over 47% of all ripples.

# Measuring ripples across multiple dimensions

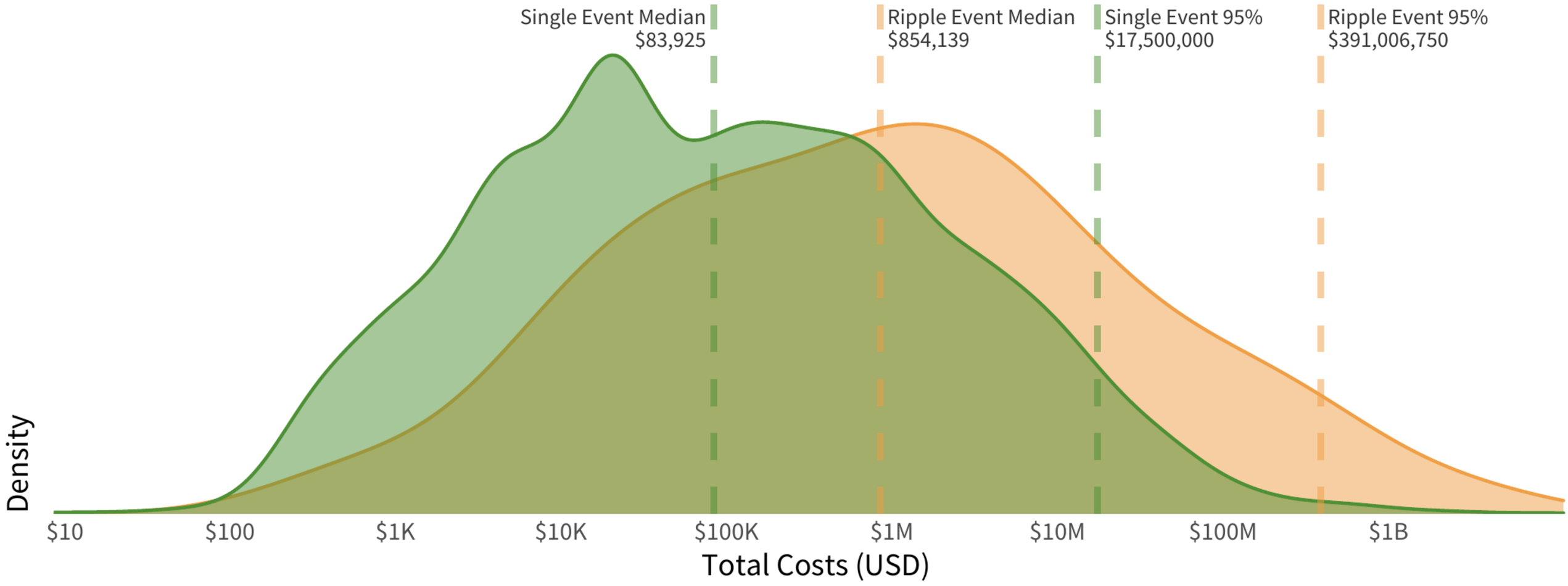



Generators
Receivers
Financial (215 firms)
Business Support (203)
Professional (115)
Information (81)
Public (55)
Retail (43)
Healthcare (42)
Hospitality (29)
Manufacturing (25)
Education (23)
Transportation (12)
Other (12)
Trade (11)
Utilities (6)
Management (6)
(Missing) (5)
Construction (5)
Real Estate (4)
Entertainment (4)
Mining (1)
Financial (977 firms)
Business Support (765)
Education (682)
Healthcare (477)
Professional (442)
Information (414)
Hospitality (362)
Public (356)
Retail (294)
Manufacturing (240)
Other (215)
Trade (98)
Entertainment (78)
Transportation (60)
(Missing) (55)
Utilities (51)
Management (44)
Construction (37)
Real Estate (32)
Mining (10)

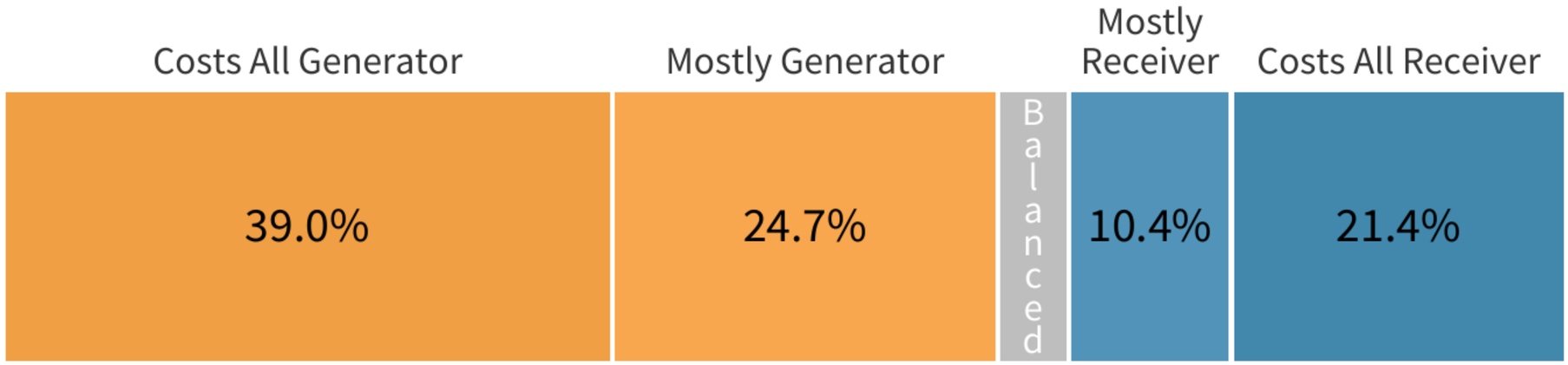
RSAConference2022

# Straight talk on losses

# How big are these, anyhow?



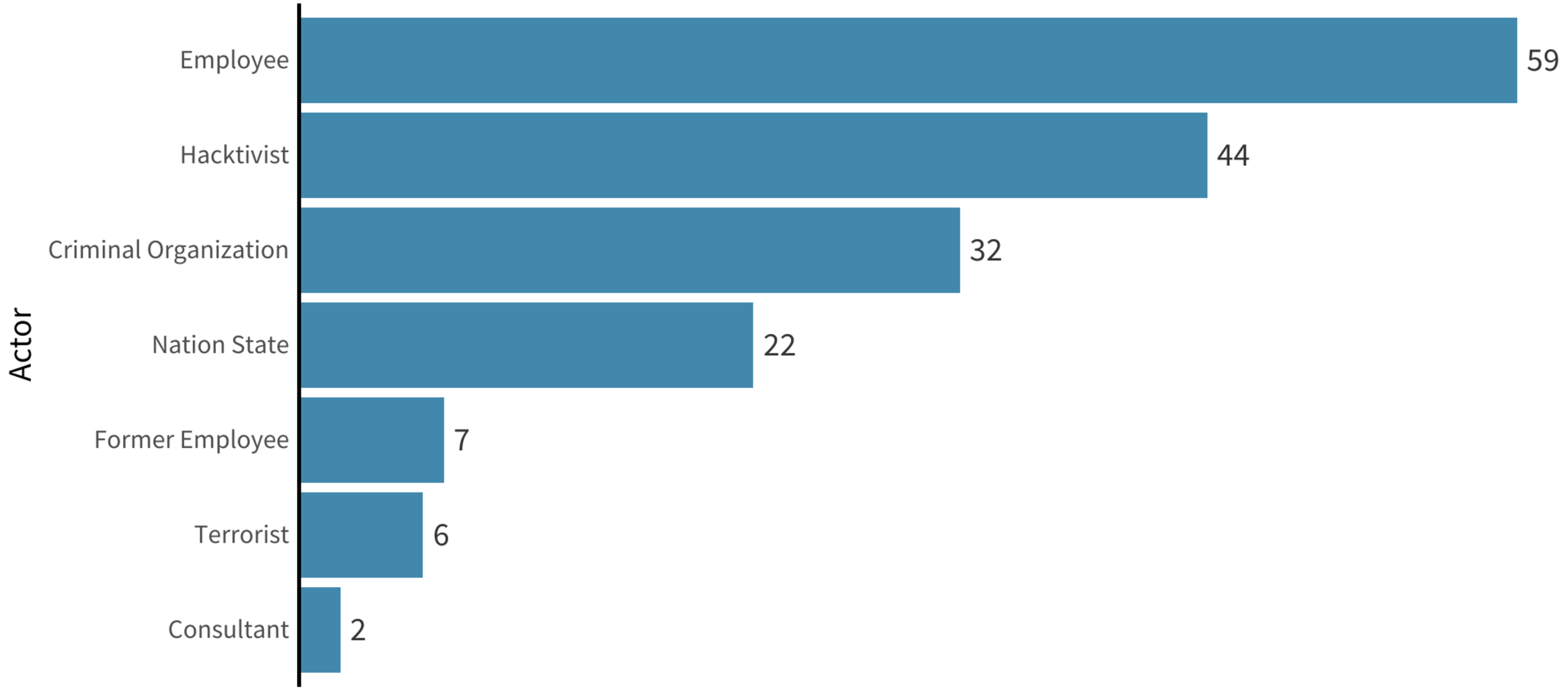
# Balance of costs



RSAConference2022

# Who and how?

# Actors at the source of ripples

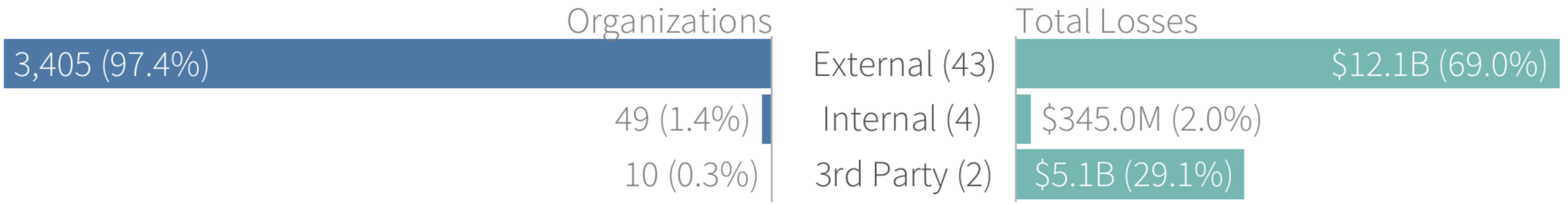


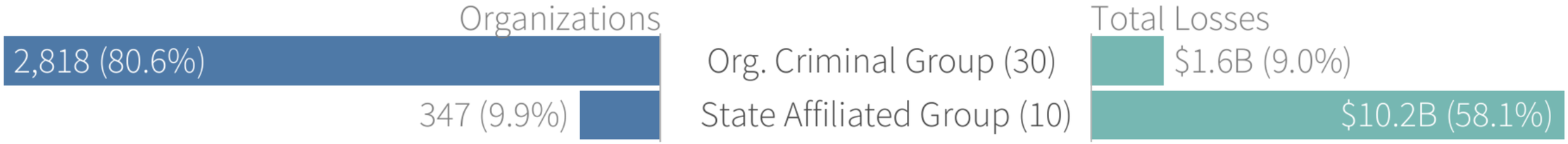
# We can apply ATT&CK

ATT&CK Supply Chain Sub-techniques

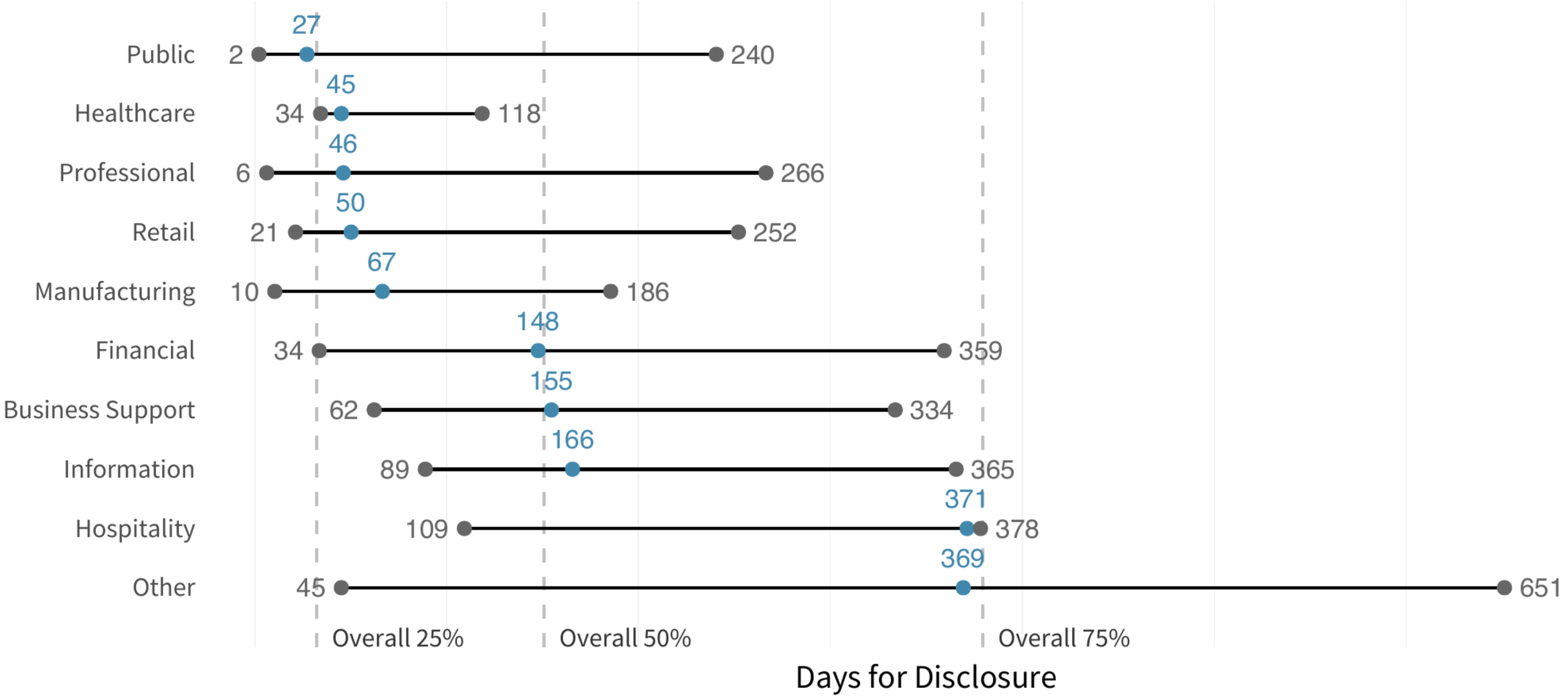
| | Incidents | Total Losses | % of Losses | % of Orgs |
|---|---|---|---|---|
| Compromise software supply chain | 5 | $7.4B | 42.1% | 27.8% |
| Compromise software dependencies & development tools | 3 | $29.4M | 0.2% | 9.8% |

# Threat actors



# Industry level time to discovery



# What does this mean for you?

- Know your customer
- Third (and fourth, and fifth…) party connections can hurt
- Not all ripples are the same