RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: RC-R09

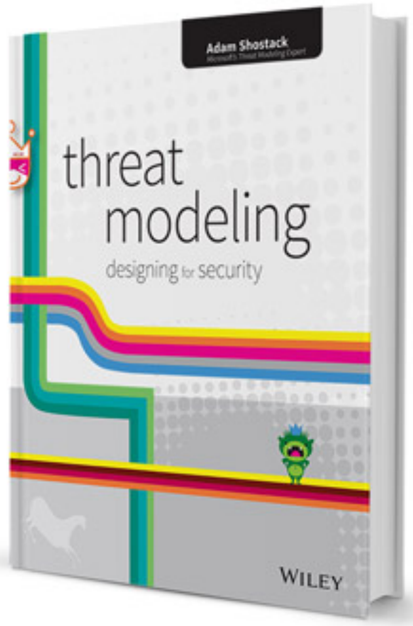
How to Measure Ecosystem Impacts

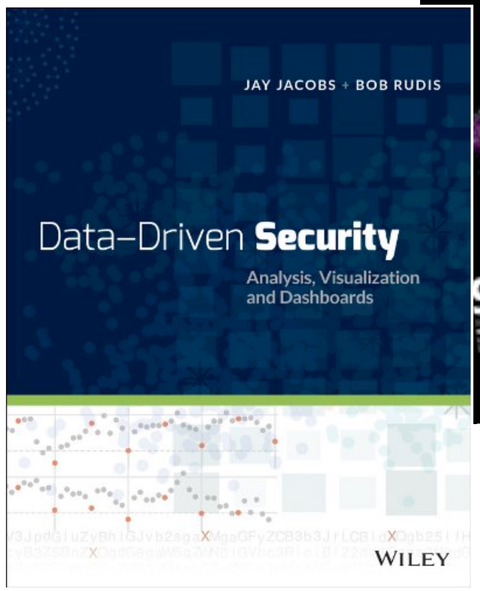
Adam Shostack
President
Shostack & Associates
@adamshostack

Jay Jacobs
Data Scientist
Cyentia Institute
@jayjacobs

Adam Shostack and Jay Jacobs

Adam





CYENTIA INSTITUTE

Jay

Agenda

- Our DMARC mission
- Measuring intangibles
- Simulation under high uncertainty
- The impact of DMARC

Intro to DMARC

- DMARC
  - Email security standard
  - “Domain-based Message Authentication, Reporting & Conformance”
  - Implemented via DNS records
- Global Cyber Alliance (GCA) has a project to drive deployment
- Asked Adam, Jay and Wade for help measuring that project’s ROI

Challenges

- GCA wanted a dollar figure for return on investment
- Hmmmm…

If only we had a holocaust cloak…

Why Didn't You List That Amongst Our Assets?

GCA Has

- A tool that shows you the status of your DMARC records.
- A list of domains whose DMARC policies have changed since they were entered in the tool
- Active partners

Does Not Have

- Reliable cost of a breach #
- Root causes of breaches
- List of breaches DMARC could have stopped

¯_(ツ)_/¯

GCA DMARC Tool

If you would like to share the results just click on the Share button, a link will be copied to clipboard.

Selecting a protocol will also show the current record if available.

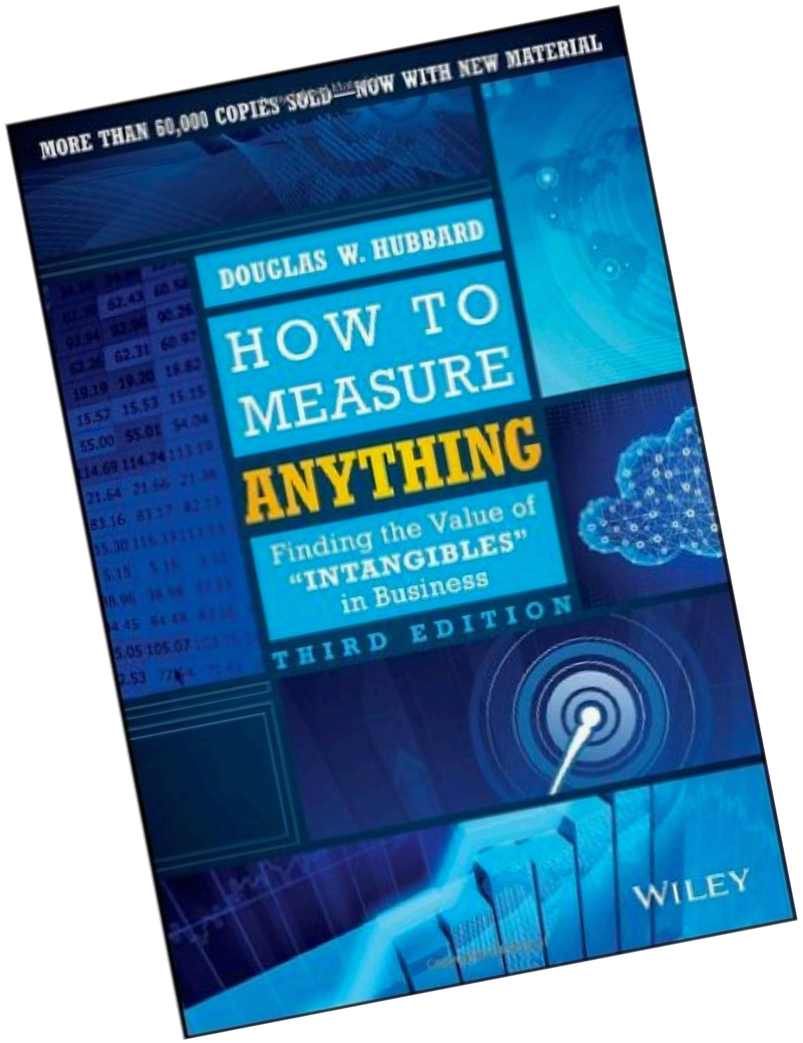
SPF		✔
DKIM		✖
DMARC	DMARC has not been implemented on this email's domain. Please press the 'Next' button below to start the DMARC Setup Guide.	✖

We couldn't find a DKIM record associated with your domain given a list of default selectors: default, google*, google2048, google1024, mail, selector1, selector2, smtpapi, s1024, s2048

RSA Conference 2019

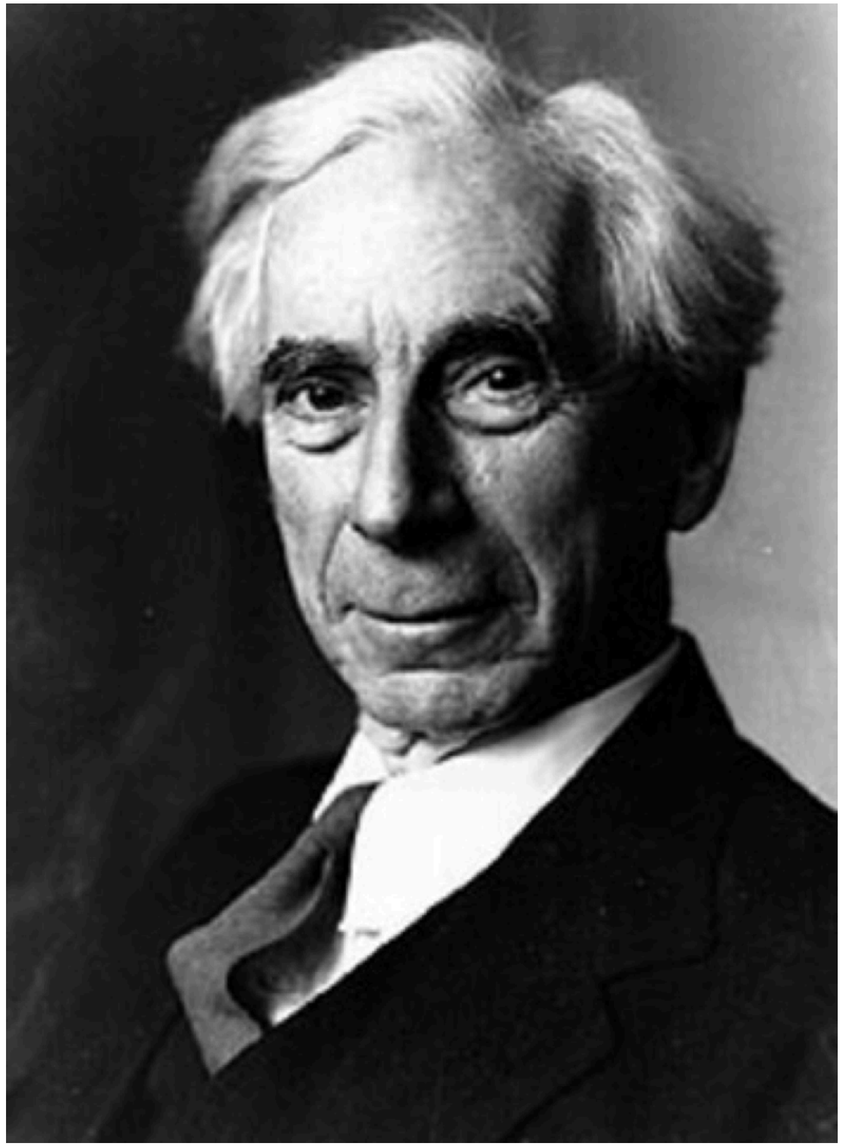
Inconcievable?

Measuring an Intangible



- Concept of Measurement
- Object of Measurement
- Method of Measurement

The Concept of Measurement



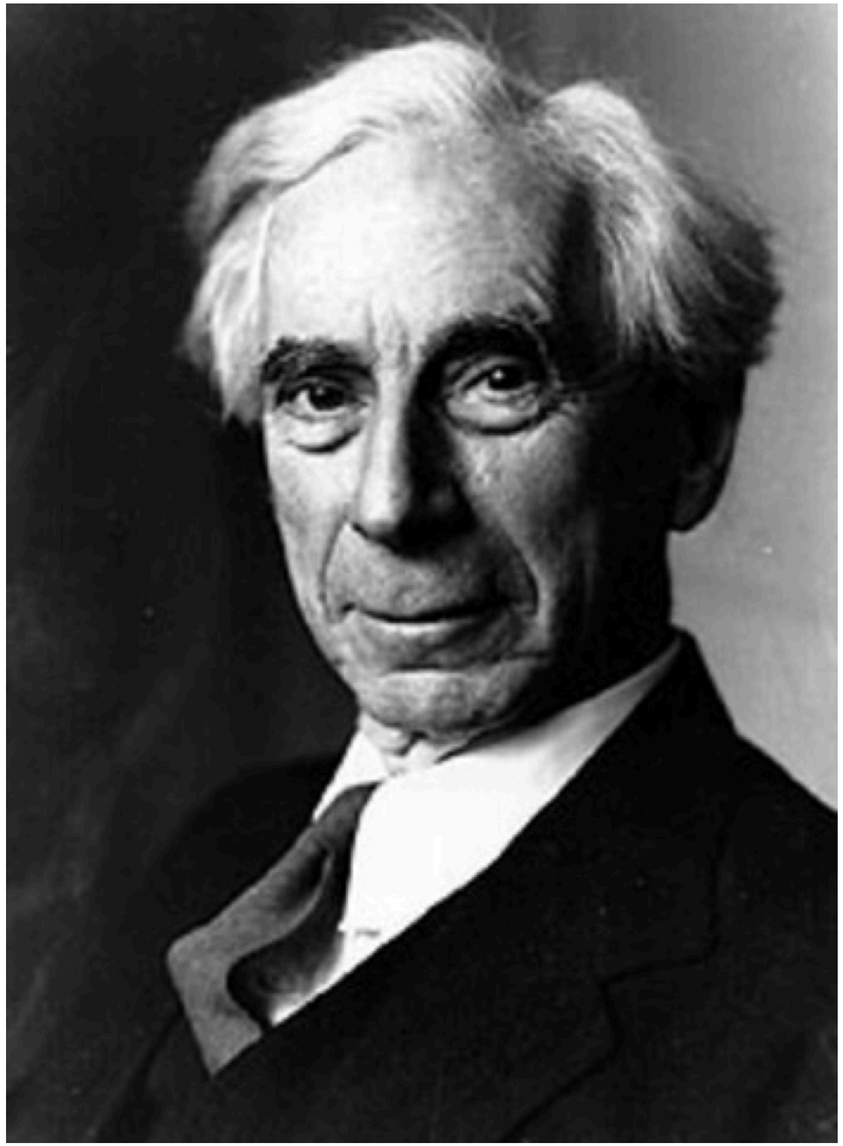
"Although this may seem a paradox, all exact science is based on the idea of approximation. If a person tells you they know a thing exactly, then you can be safe in inferring that you are speaking to an inexact person."

Bertrand Russell

Philosopher, Mathematician, Nobel Laureate

The Concept of Measurement

Measurement:
A set of observations that reduce uncertainty where the result is expressed as a quantity



"Although this may seem a paradox, all exact science is based on the idea of approximation. If a person tells you they know a thing exactly, then you can be safe in inferring that you are speaking to an inexact person."

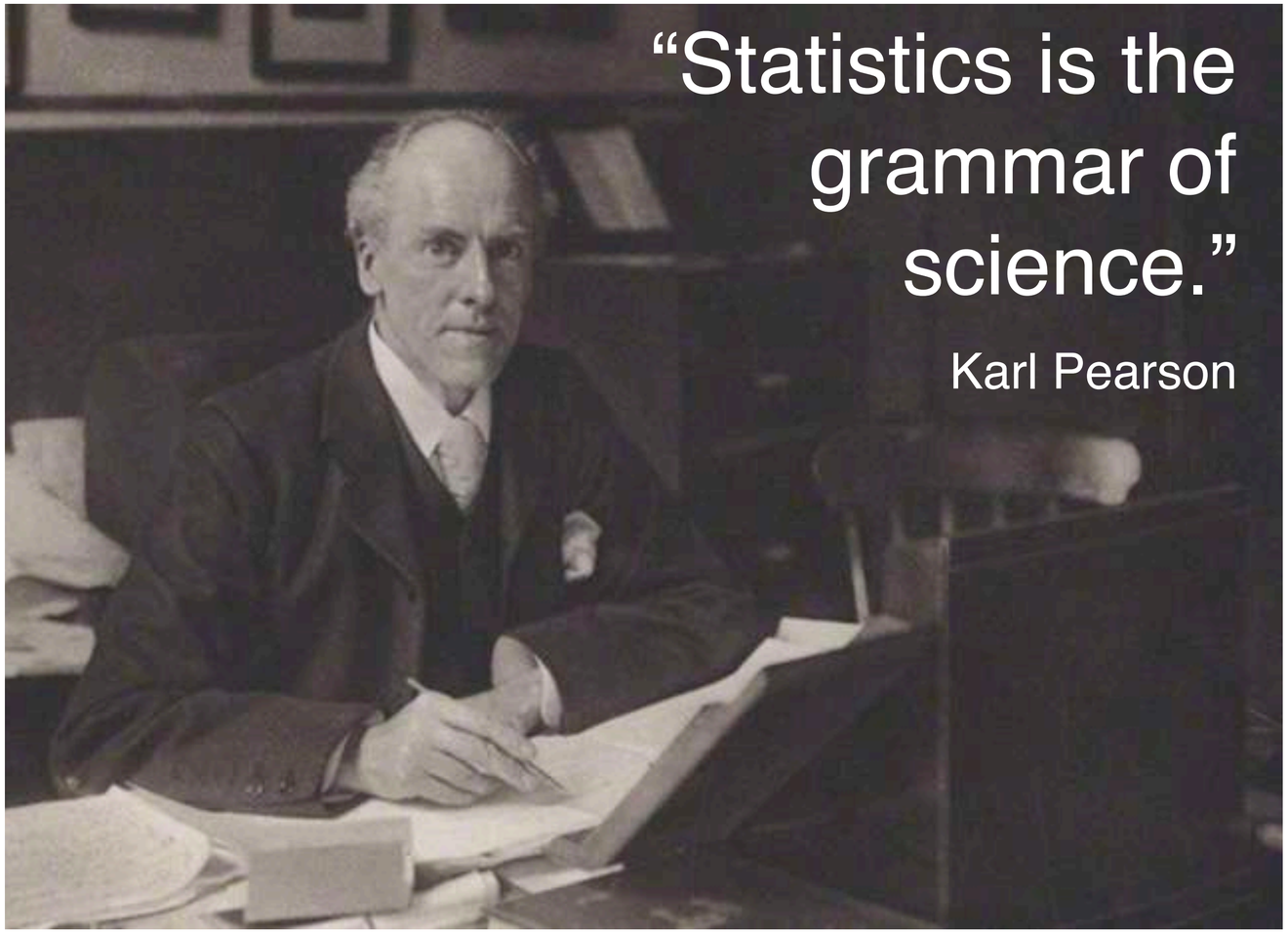
Bertrand Russell
Philosopher, Mathematician, Nobel Laureate

The Object of Measurement

"There is no greater impediment to the advancement of knowledge than the ambiguity of words."

Thomas Reid
Scottish Philosopher

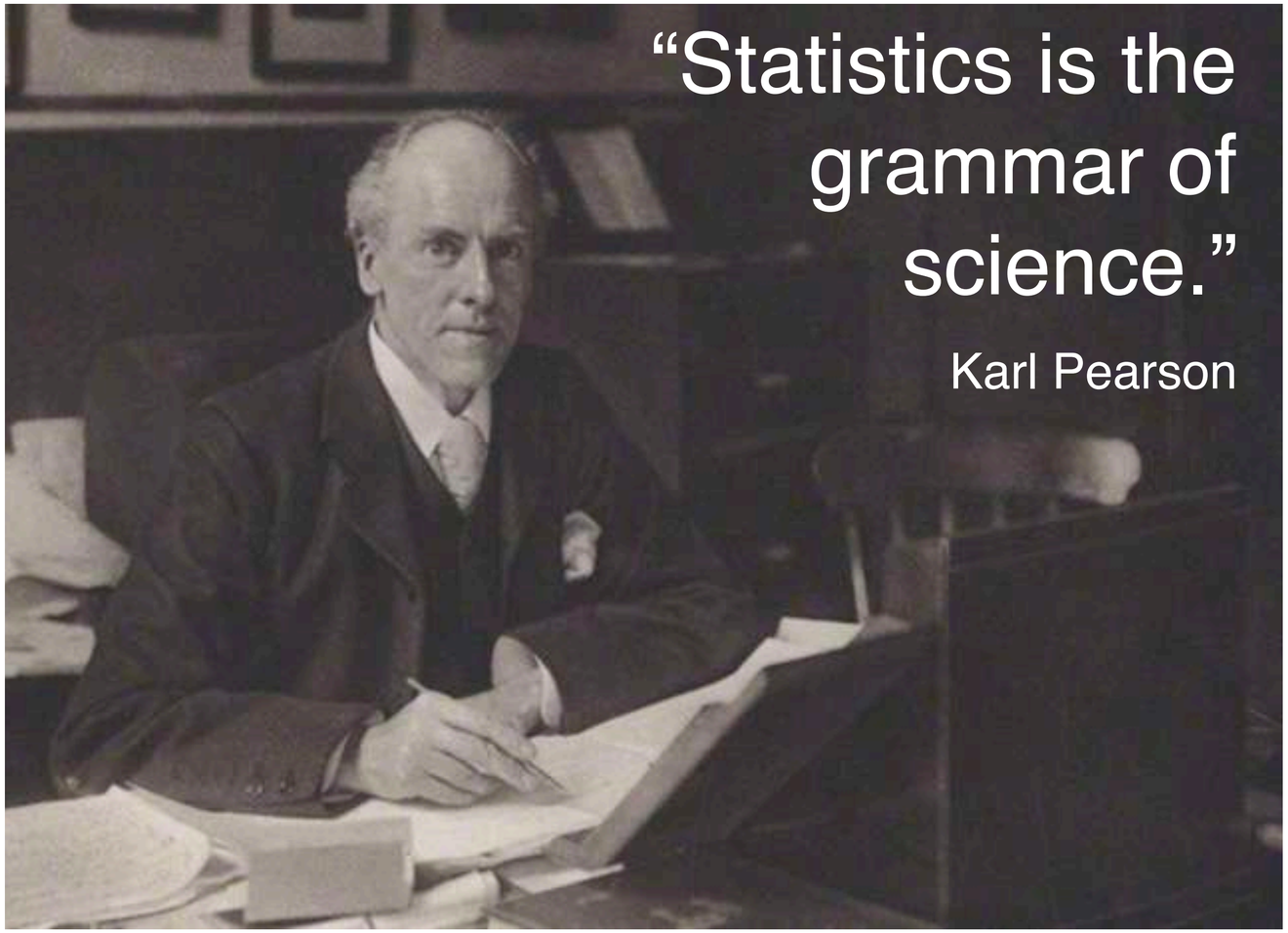
Method of Measurement



“It’s easy to lie with statistics. It’s hard to tell the truth without statistics.”

Andrejs Dunkels

Method of Measurement



“It’s easy to lie with statistics. It’s hard to tell the truth without statistics.”

Andrejs Dunkels

How do we know if research is worthy of our trust?

Worthy of Trust

- Context
- Quality of evidence
  - Design of experiments
  - Source/collection of data
  - Sample size
- Strength of recommendation
  - Inference
  - Data visualization

- “Perfect is the enemy of good”
  - We are not physics
  - Can’t wait for clinical trials

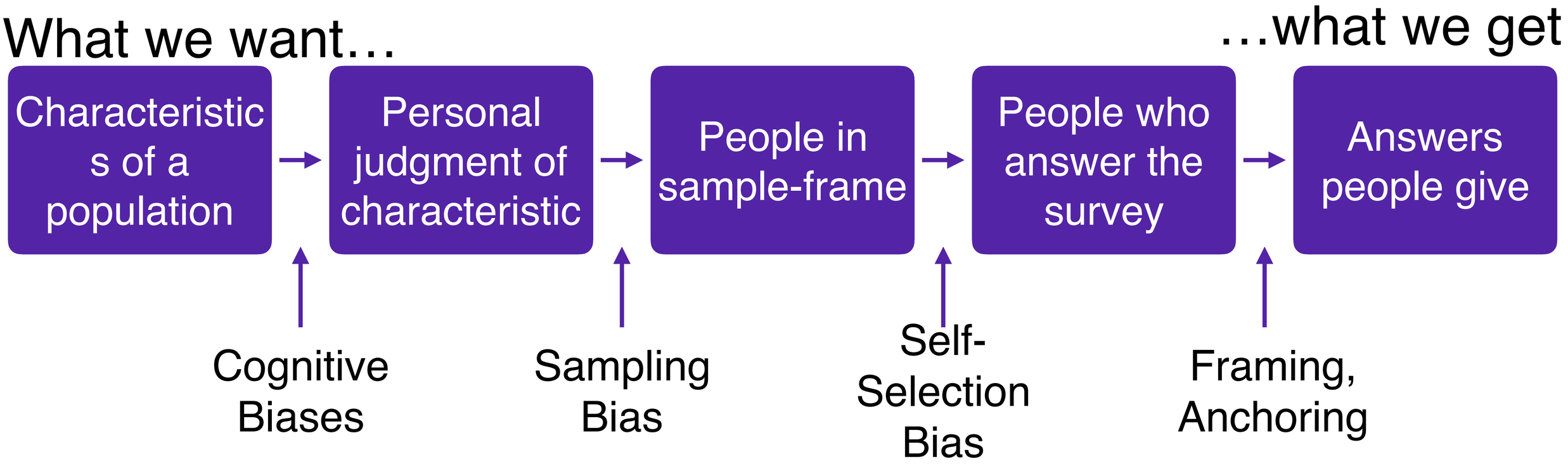
http://www.gradeworkinggroup.org/

Surveys are, um… Tricky

What we want…

…what we get

Surveys are, um… Tricky



DMARC-ish Research

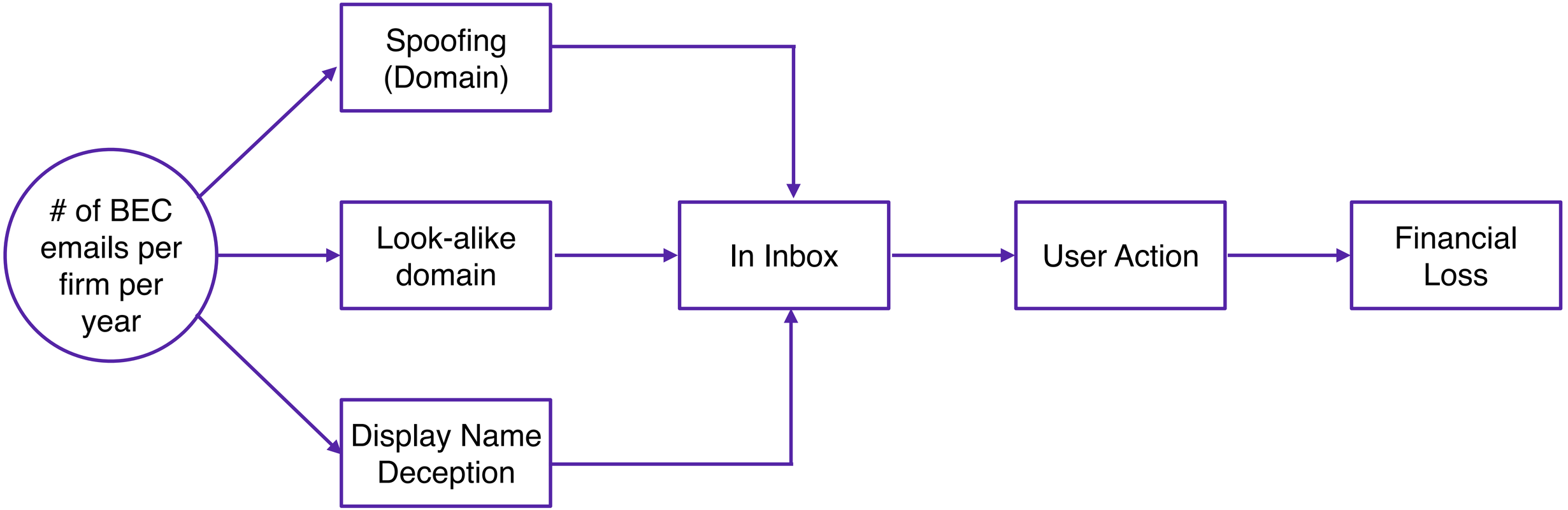
- American Bankers Association: Corporate Account Takeover/ Business Email Compromise, last visited June 23, 2018
- Agari: Threat Taxonomy: A Working Framework to Describe Cyber Attacks, Agari, July 24, 2017
- Agari: Business Email Compromise (BEC) Attack Trends Report
- FBI: Business E-Mail Compromise, Federal Bureau of Investigation, February 27, 2017
- FBI: 2017 Internet Crime Report
- FBI: Business E-mail Compromise: The 12 Billion Dollar Scam, Alert # I-071218-PSA, July 12, 2018
- GreatHorn: Spear Phishing Report, 2017
- NetDiligence: 2017, 2016 Cyber Claims Study, NetDiligence
- Proofpoint: Email Fraud Threat Report, Year in Review
- Symantec: ISTR Email Threats 2017
- TrendLabs 2016 Security Roundup:A Record Year for Enterprise Threats
- Verizon DBIR
- Wombat State of the Phish Report 2018
- Amaroso: Fundamentals of computer security technology, Edward G. Amaroso (Prentice Hall, 1994)
- "Measuring the cost of cybercrime," Anderson et al. The economics of information security and privacy, pp. 265-300. 2013.
- 2015 SUSB Annual Data Tables by Establishment Industry, United States Census Bureau, 2015
- USA Business List, Employee Size Profile, Direct Marketing Databases
- Understanding the costs of cyber crime: A report of key findings from the Costs of Cyber Crime Working Group, Research Report 96, [UK] Home Office Science Advisory Council, January 2018
- Examining the costs and causes of cyber incidents, Sasha Romanosky, Journal of Cybersecurity, Volume 2, Issue 2, 1 December 2016
- "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries (working paper)" Riek et al., Workshop on the Economics of Information Security (WEIS). 2016.
- Gordon Snow, "Cyber Security: Threats To The Financial Sector", Congressional Testimony

Key Decision: Focus on Business Email Compromise (BEC)

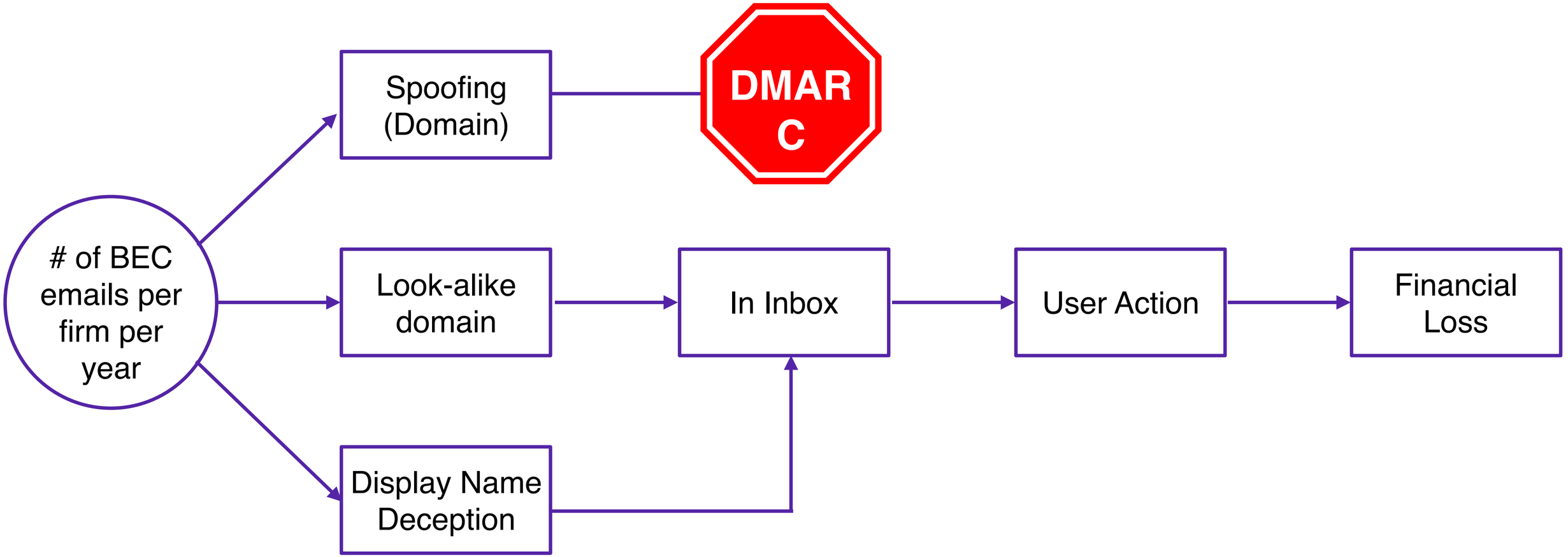
- There is a morass between phishing email and breach
- Path between email and financial loss is relatively clear
- From the [incomplete] data, BEC losses dwarfed all other email losses

This concept of measurement made other decisions fall into place.

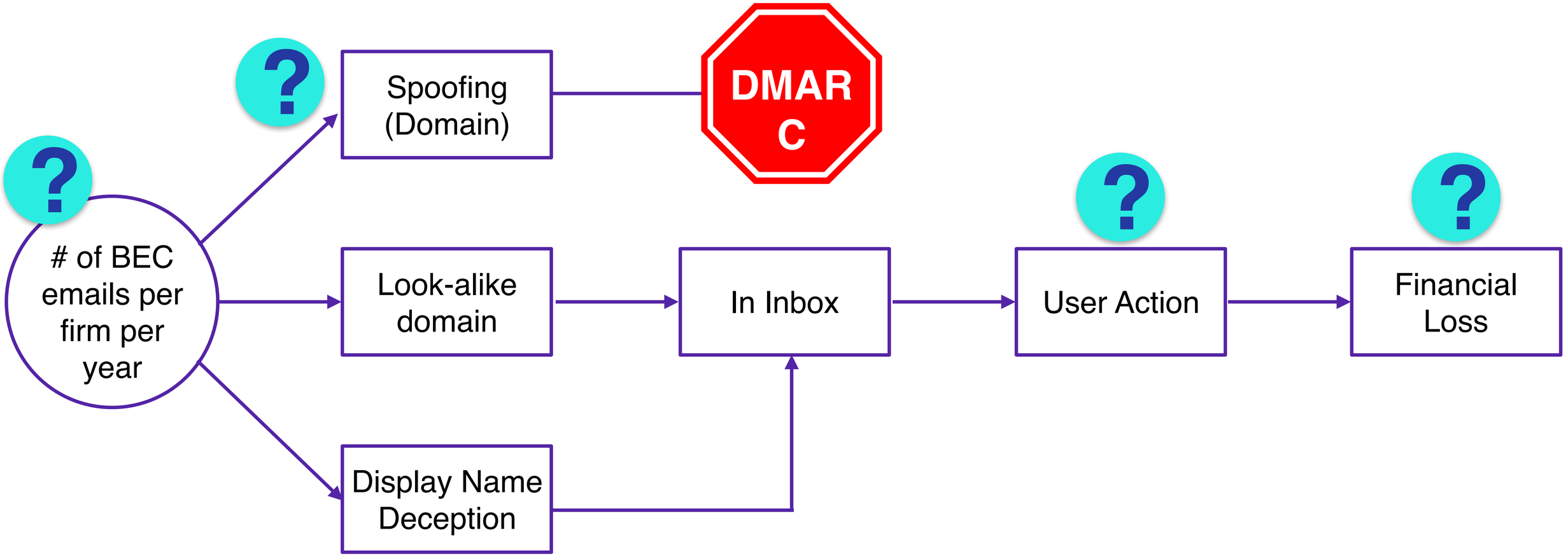
BEC-Specific Threat Model



BEC-Specific Threat Model: With DMARC



Things we know we don't know

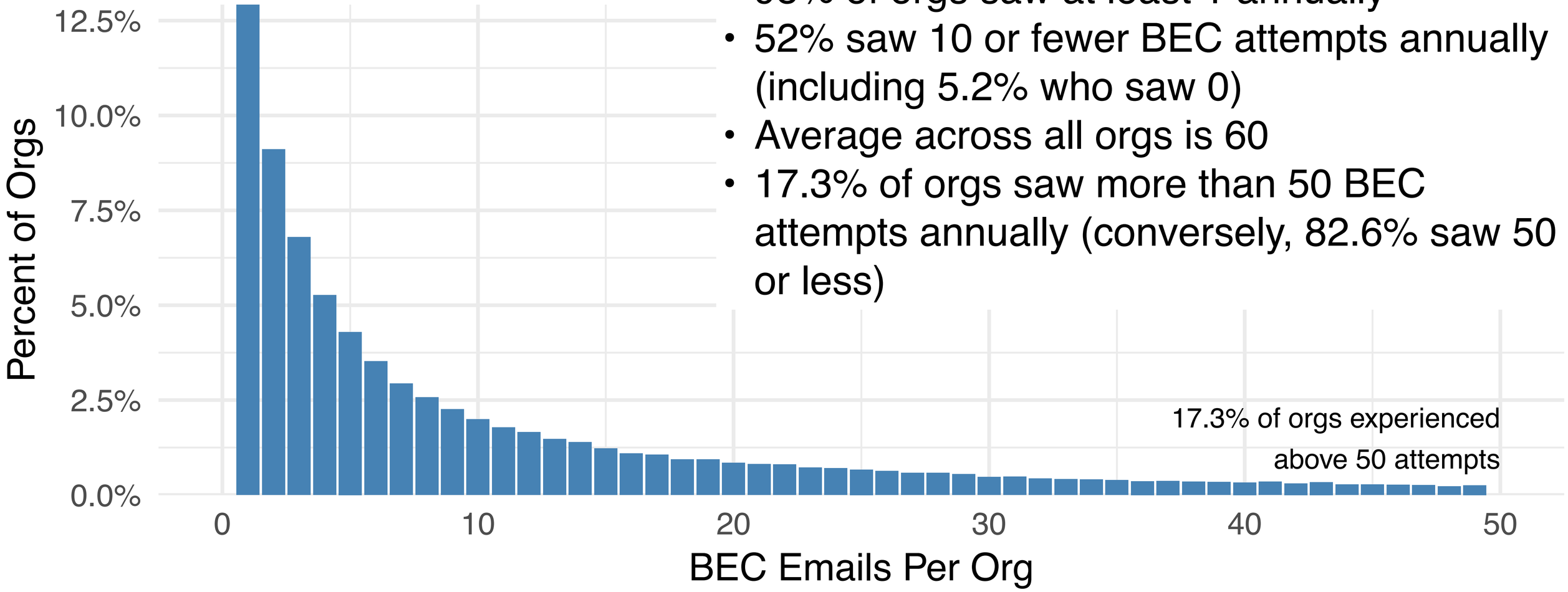


BECs per firm per year

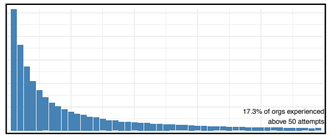
- “On average a targeted organization has 5.2 BEC emails sent to them each month.” - Symantec
  - Note: At 5.2 per month, the annual average is about 62 BEC emails.
- “On average, companies were targeted by 18.5 fraudulent emails per quarter.” - Proofpoint
  - Note: at 18.5 per quarter, the annual average is about 74.
- “In the second half of 2017, BEC attacks continued to accelerate with 96% of organizations analyzed by Agari being attacked at least one time, and with the average business experiencing 45 BEC attacks from June through December 2017.” - Agari
- “In the first three months of this year (2017), nearly 85% of organizations were targeted by at least one BEC message.” - Proofpoint

BECs per firm per year

- 95% of orgs saw at least 1 annually
- 52% saw 10 or fewer BEC attempts annually (including 5.2% who saw 0)
- Average across all orgs is 60
- 17.3% of orgs saw more than 50 BEC attempts annually (conversely, 82.6% saw 50 or less)



Things we know we don't know



# of BEC emails per firm per year

?

Spoofing (Domain)

DMARC

Look-alike domain

Display Name Deception

In Inbox

?

User Action

?

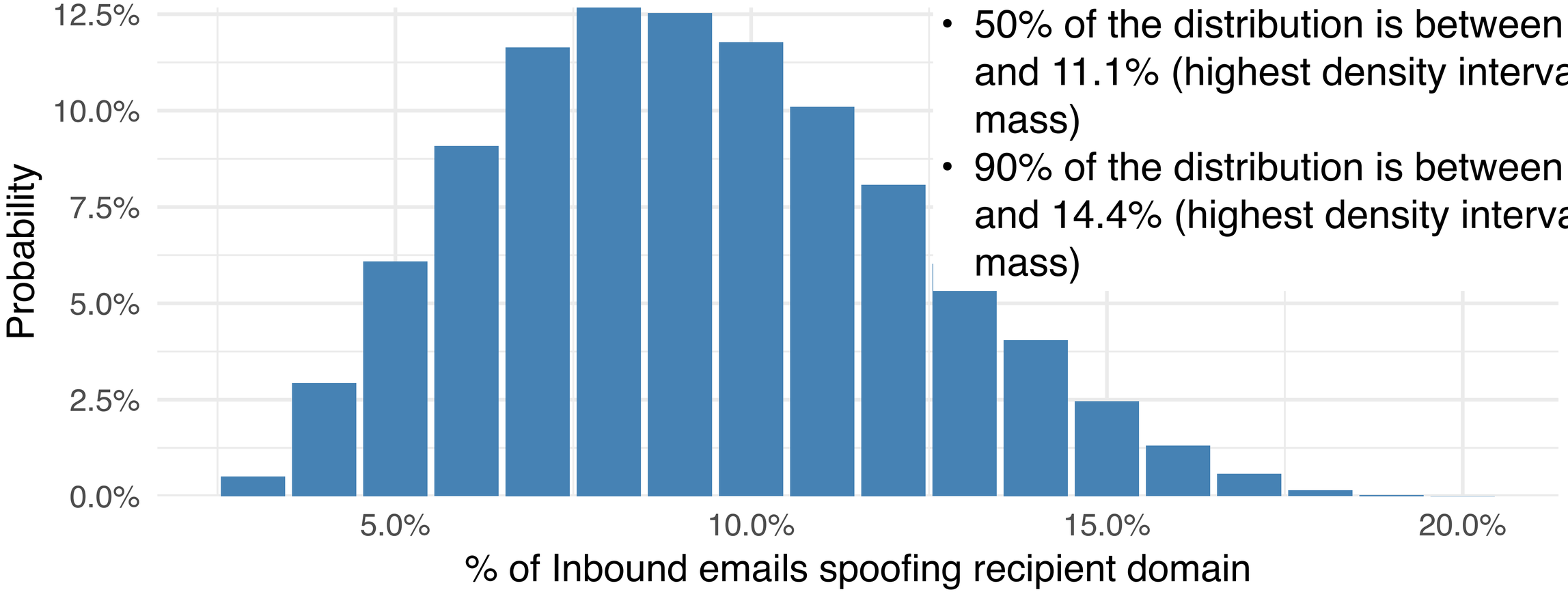
Financial Loss

Proportion of BEC using Domain Spoofing

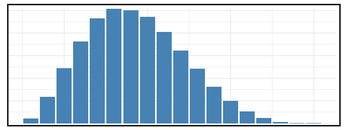
- GreatHorn reports out of 537,617 spear-phishing threats, 44,726 were “direct spoofs”, which is about 8% of the fraudulent emails they studied.
- Agari covers this statistic quite thoroughly:
  - “...Agari’s research shows that 12% of BEC attacks use spoofing; 7% a combination of look alike domains and display name deception; and 81% pure display name deception.”
  - “For organizations that use Proofpoint, 95% of attacks that went undetected used display name deception and 5% domain spoofing.”
  - “For organizations that used Microsoft EOP with no third party SEG, 90% of attacks were display name deception, 7% domain spoofs and 3% look alike domain based BEC”
  - “For organizations that use Google G Suite with no third party SEG, 93% of the attacks that were not blocked used display name deception and 7% domain spoofing.”
  - “For small businesses, 90% of BEC attacks observed used display name deception, 6% used domain spoofing and 4% used look alike domains.
  - “For medium businesses, 95% of BEC attacks used display name deception, 3% used domain spoofing and 2% used look alike Domains.
  - “For large businesses, 75% of BEC attacks used display name deception, 16% domain spoofing and 9% look alike domains.”

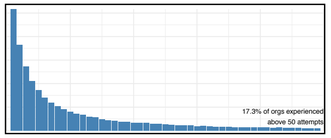
Probability of BEC using Domain Spoofing

- Average is 9.7% (arithmetic mean), minimum of 3%, maximum of 19.8%
- 50% of the distribution is between 7% and 11.1% (highest density interval, 50% mass)
- 90% of the distribution is between 4.9% and 14.4% (highest density interval, 90% mass)



Things we know we don't know





# of BEC emails per firm per year

Spoofing (Domain)

DMARC

Look-alike domain

Display Name Deception

In Inbox

?

User Action

?

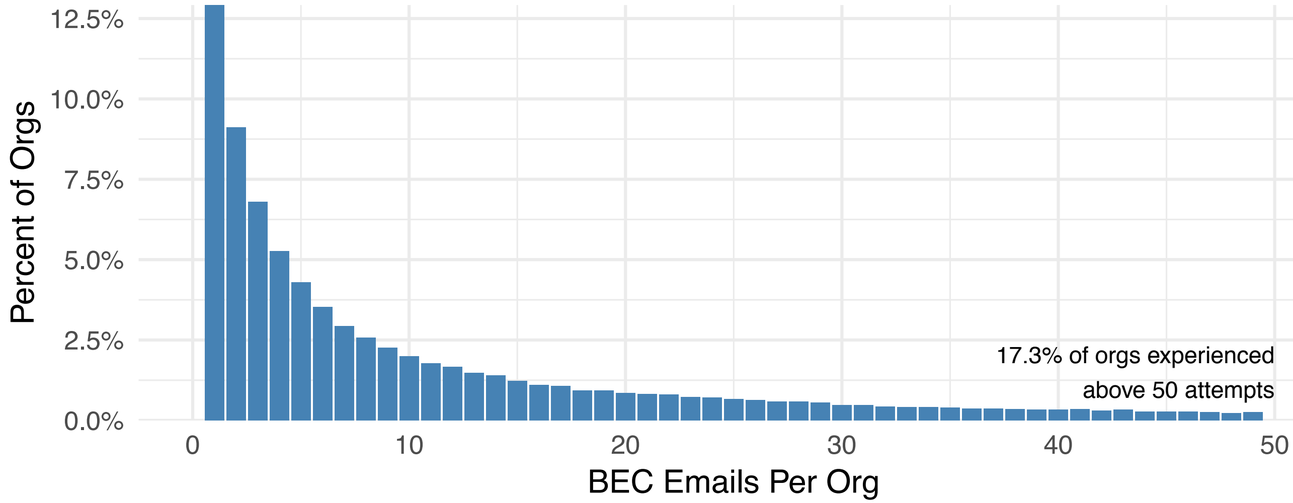
Financial Loss

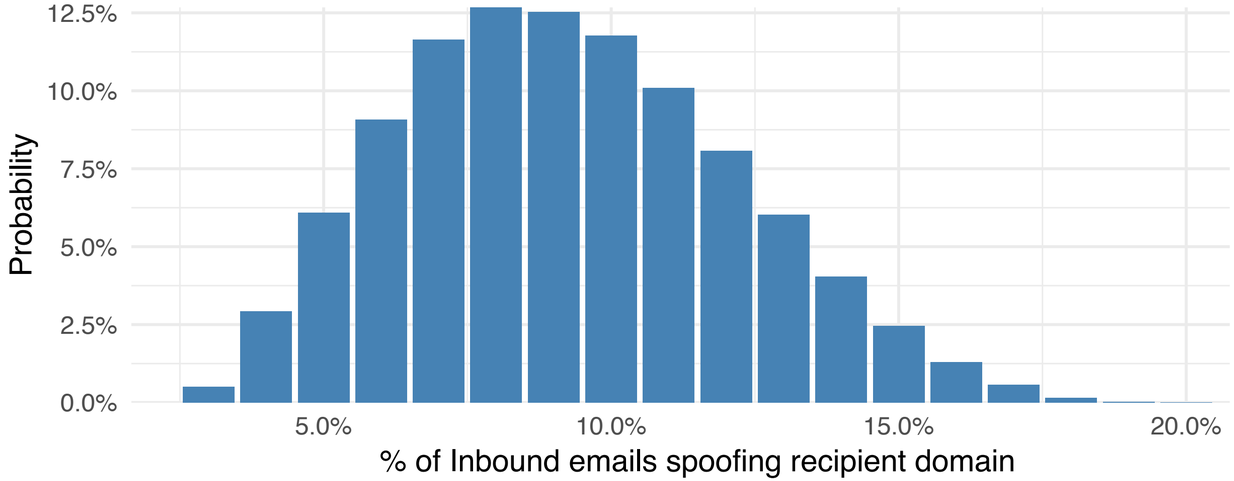
RSAConference2019

Simulating with Monte Carlo

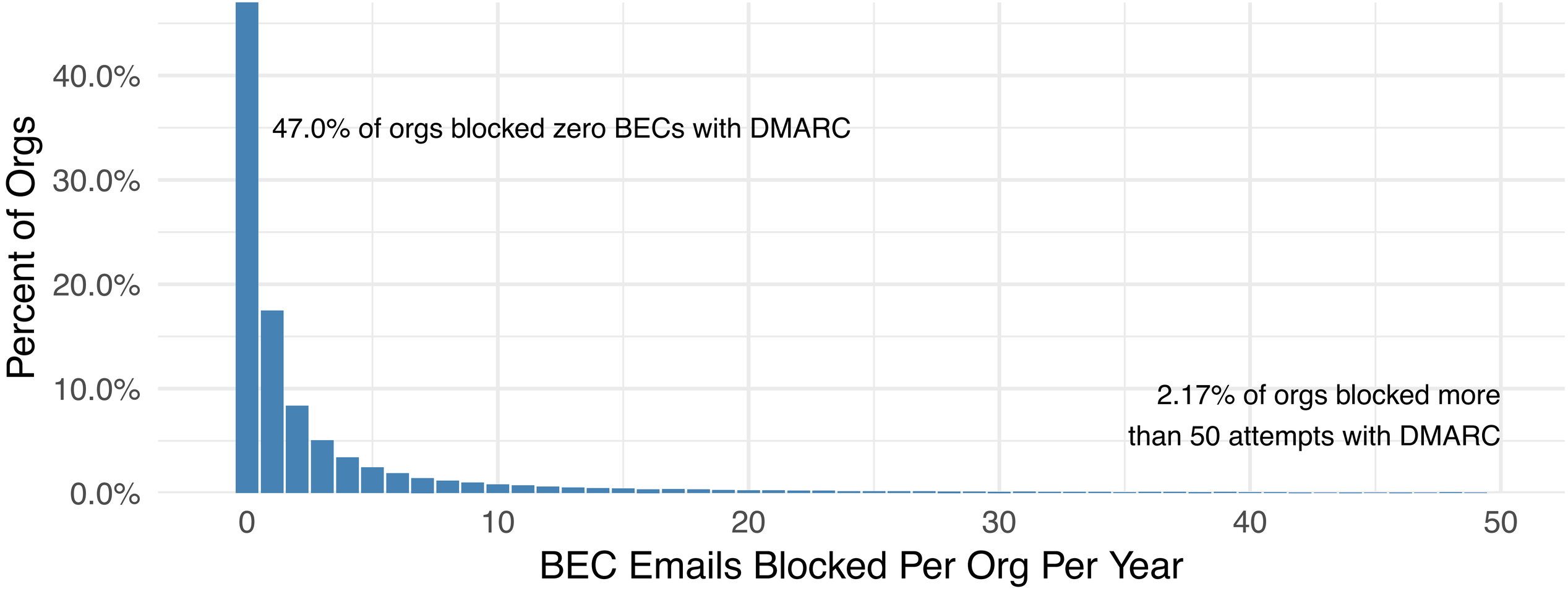
BECs blocked by DMARC

$$\#\text{ of BECs per Org} \times \frac{\text{domain spoofing}}{\text{BECs blocked by DMARC per Org}}$$

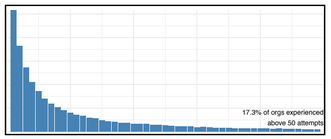




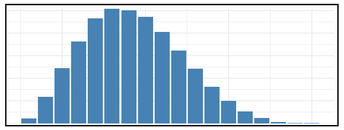
BECs blocked by DMARC



Things we know we don't know

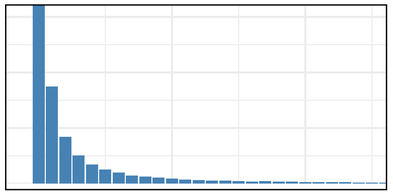


# of BEC emails per firm per year



Spoofing (Domain)

DMARC



We didn't even know we didn't know this

Look-alike domain

Display Name Deception

In Inbox

?

User Action

?

Financial Loss

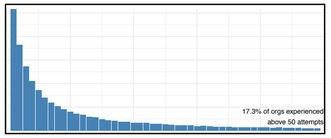
How Many Clicks Does a BEC Get?

- Phishing success rates are “well studied”
  - Commercial training companies compete on click through rates
  - 5% to 100% success rates reported
- BEC ≠ phishing
  - Response to a message is not the same as funds transferred
  - We found no reported BEC success rate
- Large opportunity to reduce uncertainty here

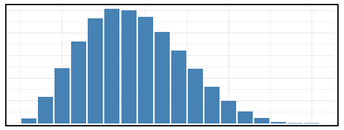
"Everything is Obvious…with hindsight"

- We wrote decent justifications that span the possibility space
- "BEC uses social norms and gets less attention than phishing, so the rate of success could be higher"
  - Victims are giving it 110%?
- "BEC requires more steps, so there's more to go wrong?"
  - Could reasonably be 1-5%
- This is a key uncertainty — we use a very conservative estimate

Things we know we don't know

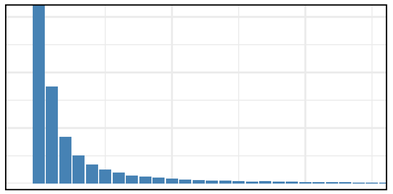


# of BEC emails per firm per year



Spoofing (Domain)

DMARC



We didn't even know we didn't know this

Look-alike domain

Display Name Deception

In Inbox

?

User Action

1-25% User Action Rate

?

Financial Loss

Financial Loss

Statistics:

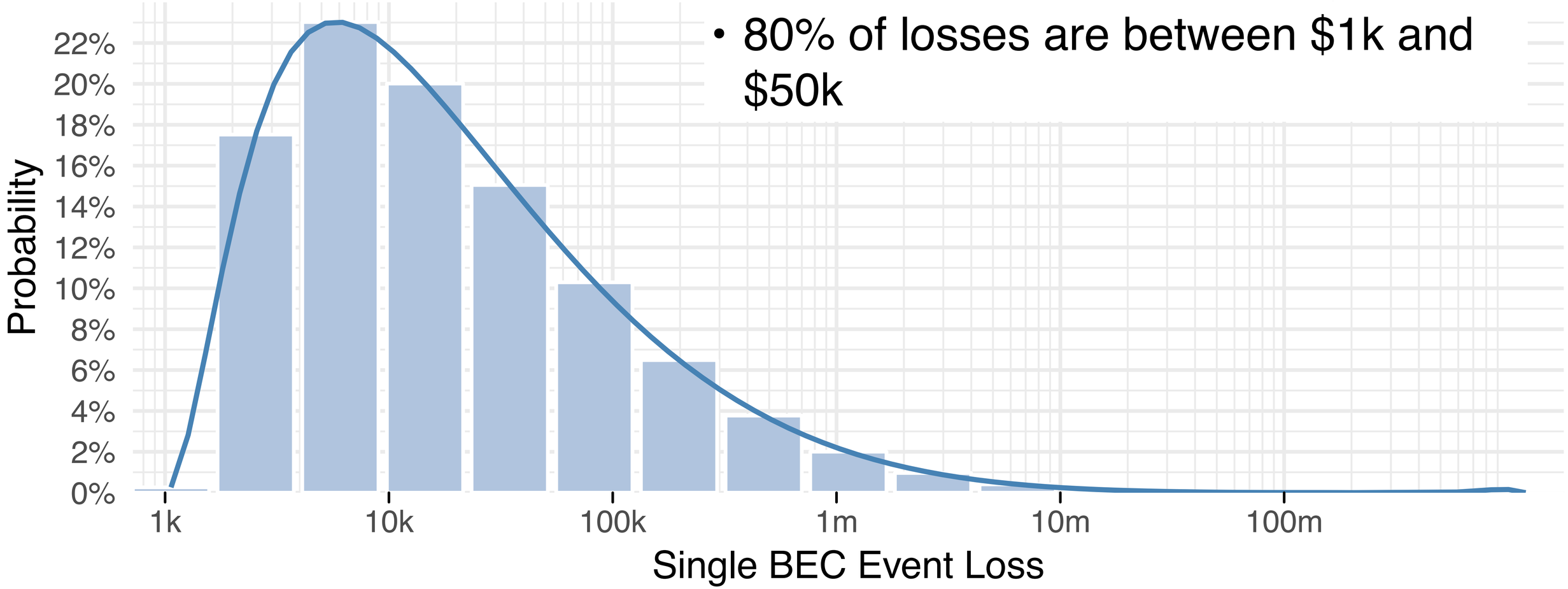
- “In 2017, the IC3 received 15,690 BEC/EAC complaints with adjusted losses of over $675 million.” (FBI/IC3). - Note average is $43k
- $131K in average loss for U.S. victims, and a $71K worldwide average loss. (FBI)
- over $12 billion in losses over 78,617 domestic and international incidents, which averages out to about $160,000 per organization (FBI 2018)

Headlines:

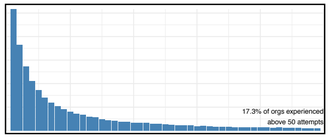
- “Leoni AG… became a victim of a BEC attack when its Chief Financial Officer (CFO) was tricked into transferring about US $44.6 million” (TrendMicro)
- “Xoom was probably the year’s first victim of a Business Email Compromise (BEC) to the tune of $31 million.” (Verizon)
- “...Belgian bank Crelan announced they were the victim of a €78 million BEC fraud.” (about $91 million USD). (Verizon)

Financial Losses from BEC

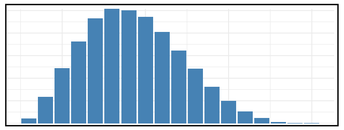
- Arithmetic mean is $108k
- 88% of losses are less than $100k
- 80% of losses are between $1k and $50k



Things we know we don't know

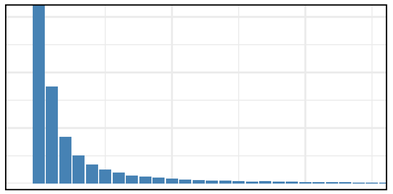


# of BEC emails per firm per year



Spoofing (Domain)

DMARC



Look-alike domain

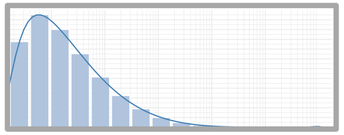
Display Name Deception

In Inbox

?

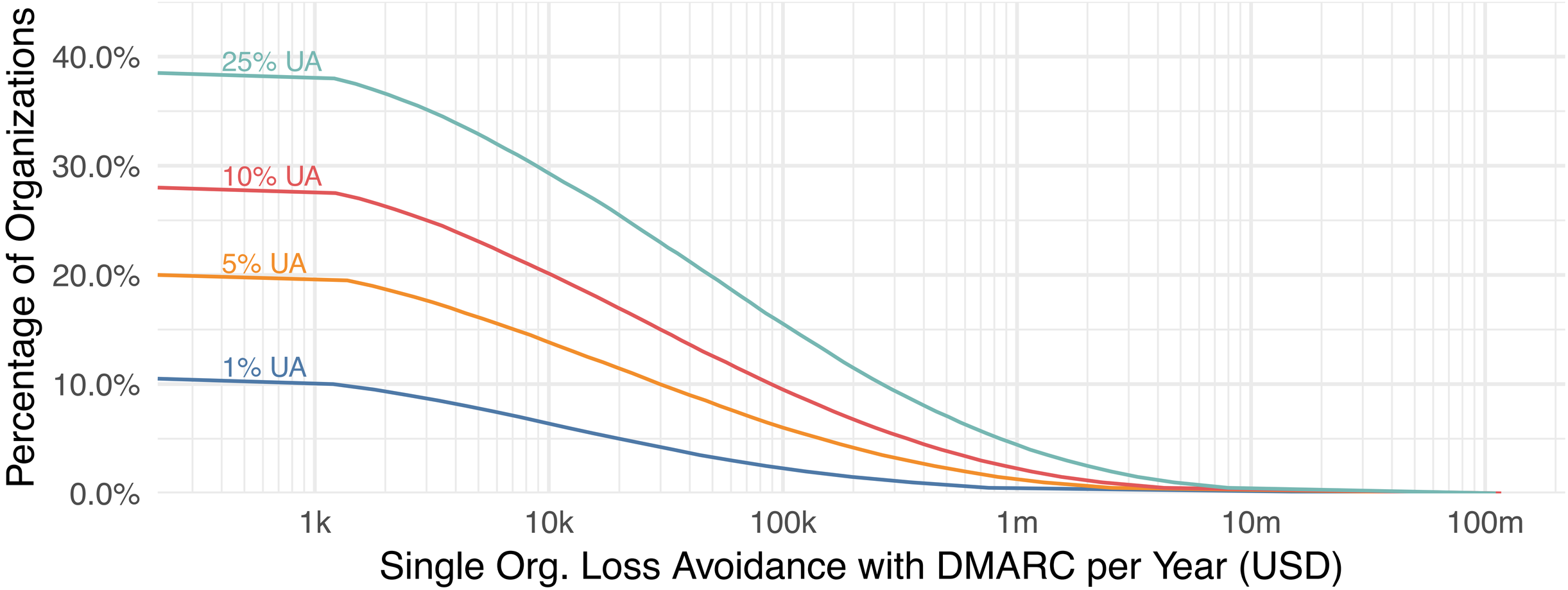
User Action

1-25% User Action Rate

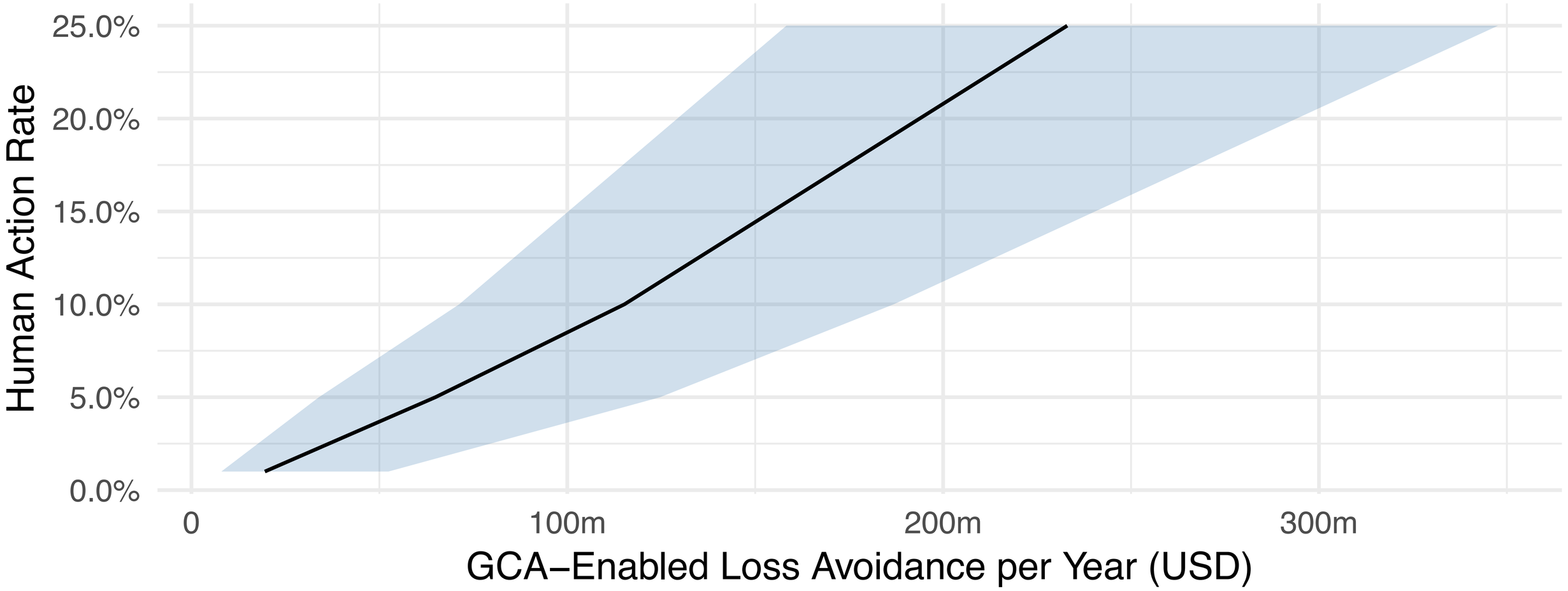


Financial Loss

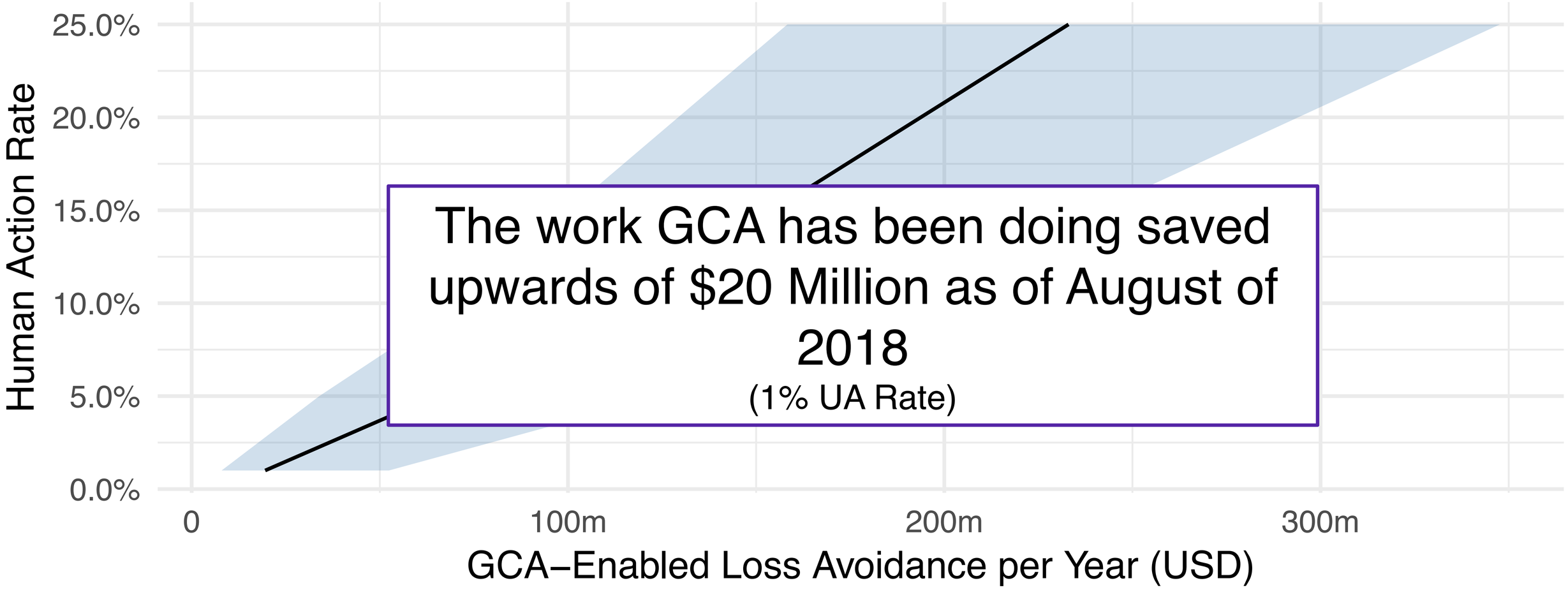
Financial Loss given Human Action Rate



GCA Helped 1,046 Domains implement DMARC



GCA Helped 1,046 Domains implement DMARC



Apply What You Have Learned Today

- Next week you should:
  - Check your domain with https://dmarcguide.globalcyberalliance.org
  - Distribute our “how to evaluate a vendor report” cheat sheet
- In the next month:
  - Set up a DMARC p of “none” if you don’t have at least that. (None generates reports, doesn’t change mail delivery.)
- Within six months you should:
  - Have a stronger DMARC policy
  - If you release reports, make sure they pass the criteria we’ve shared

RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: RC-R09

How to Measure Ecosystem Impacts

Adam Shostack
President
Shostack & Associates
@adamshostack

Jay Jacobs
Data Scientist
Cyentia Institute
@jayjacobs