RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HUM-W08**

Security's Holy Grail: Predicting Attacks Before They Happen

Robert Fly

CEO & Co-Founder
Elevate Security
@hello_elevate

Wade Baker, PhD

Partner, Cyentia Institute
& Professor, Virginia Tech
@wadebaker

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.

RSAConference2022

Sizing Up Human Risk

Investigating the human attack surface

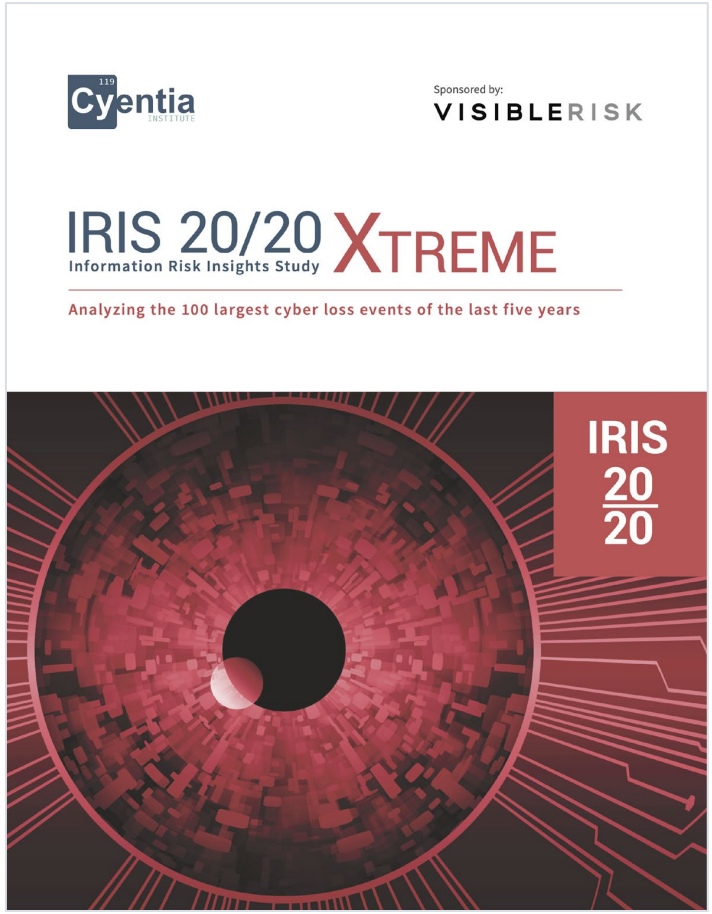
Of all data breaches examined in a recent Verizon DBIR:

- 30% of breaches involve internal threat actors
- 8% of breaches involve misuse actions
- 20% of breaches involve human error
- 22% phishing and other social engineering tactics
- 29% of breaches target humans as a compromised asset
- 40% of malware breaches employ password dumpers
- 37% of malware breaches prompted users to click email links
- 13% of malware breaches prompted users to execute attachments
- 80% of hacking involves brute force or lost/stolen credentials

Thanks to the DBIR team for providing these stats!

Investigating the human attack surface

Observable forms of human risk played a direct role in **61% of the largest cyber incidents** of the last 5 years. Even more daunting is the fact that these human risk factors racked up a price tag of $15 billion—that's **88% of the total losses**!



https://www.cyentia.com/iris

Investigating the human attack surface

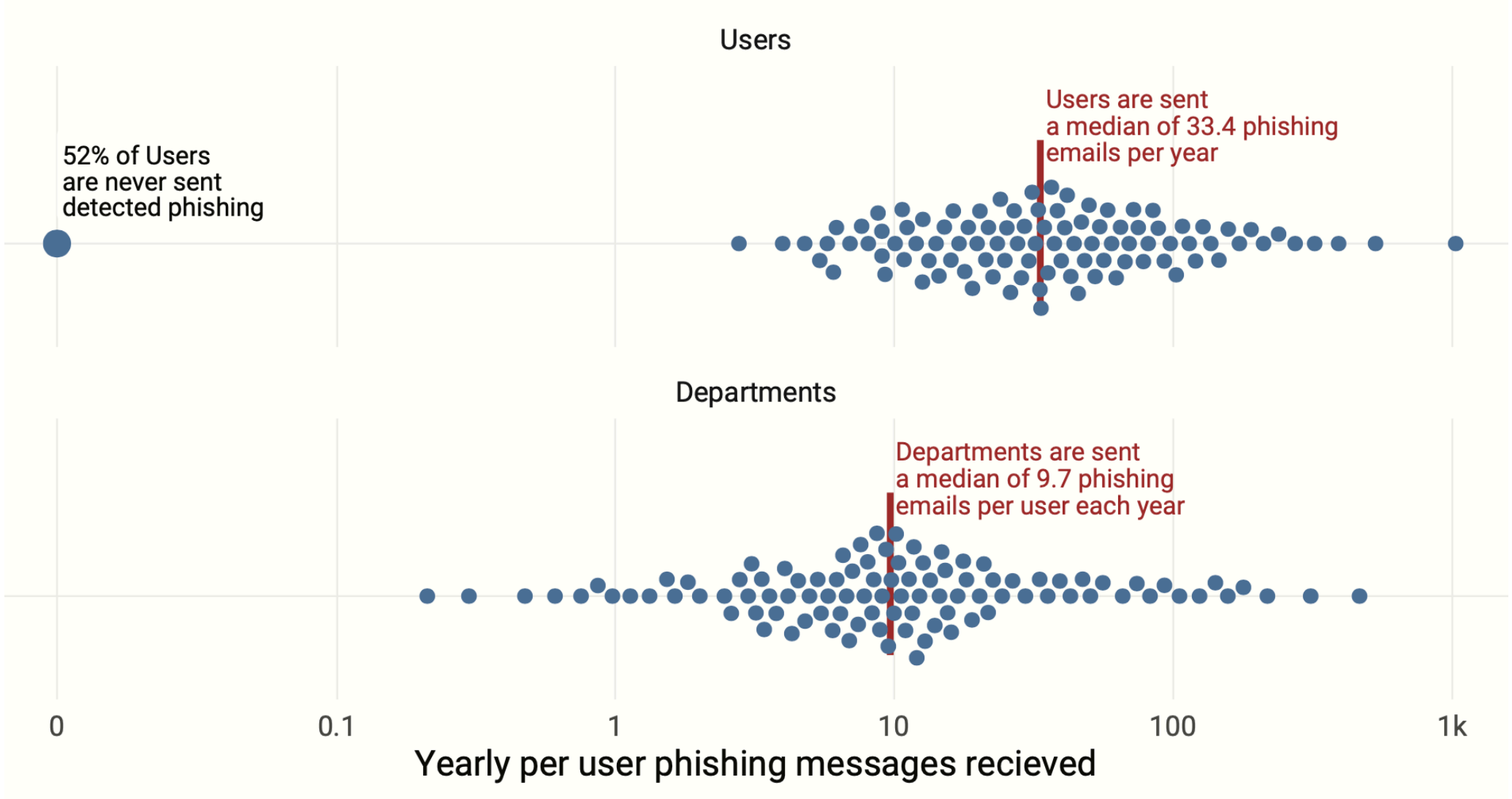
Insiders are **vectors** more often than they're **villains**.

But we need to recognize and respond to signs of both to manage the whole of human risk.

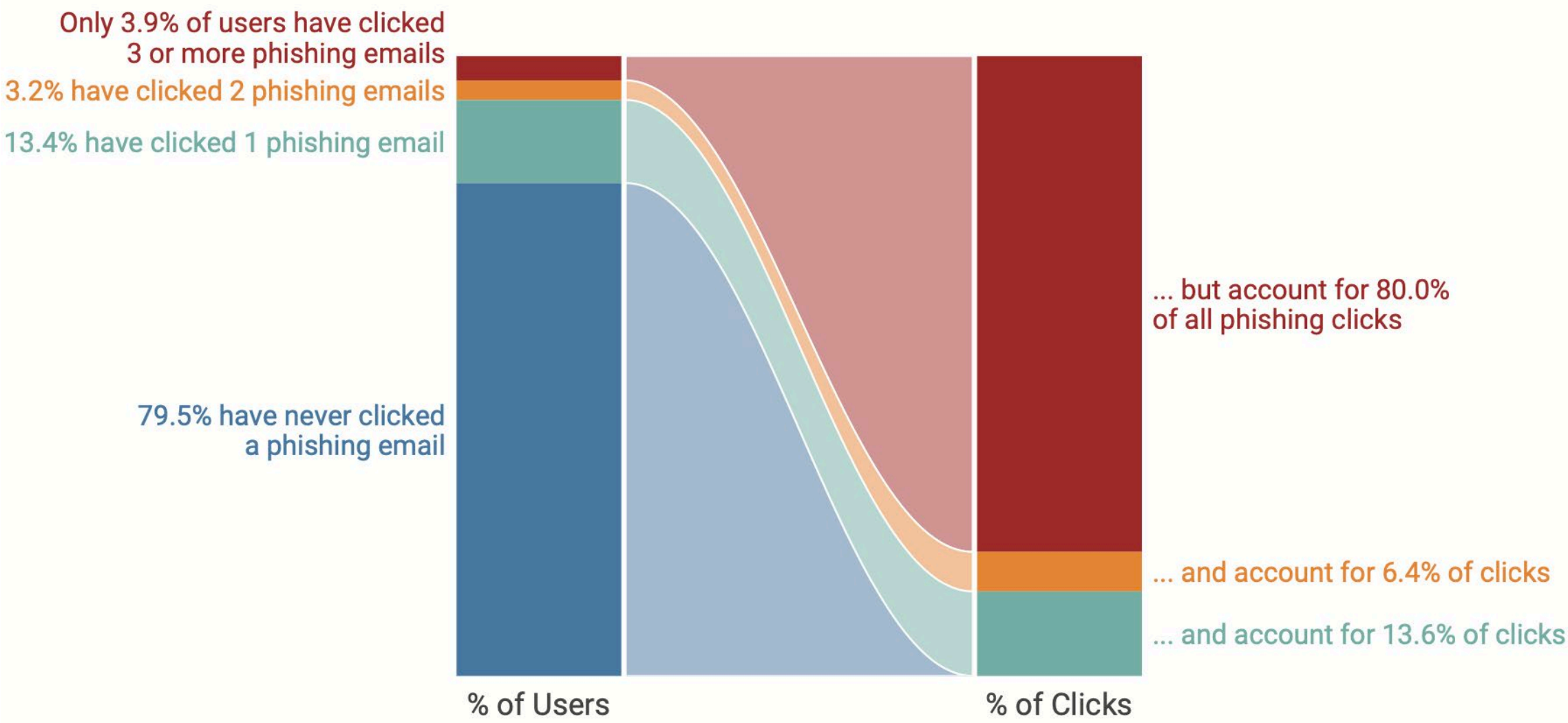
RSAConference2022

Pinpointing Human Risk

Benchmark: phishing emails RECEIVED

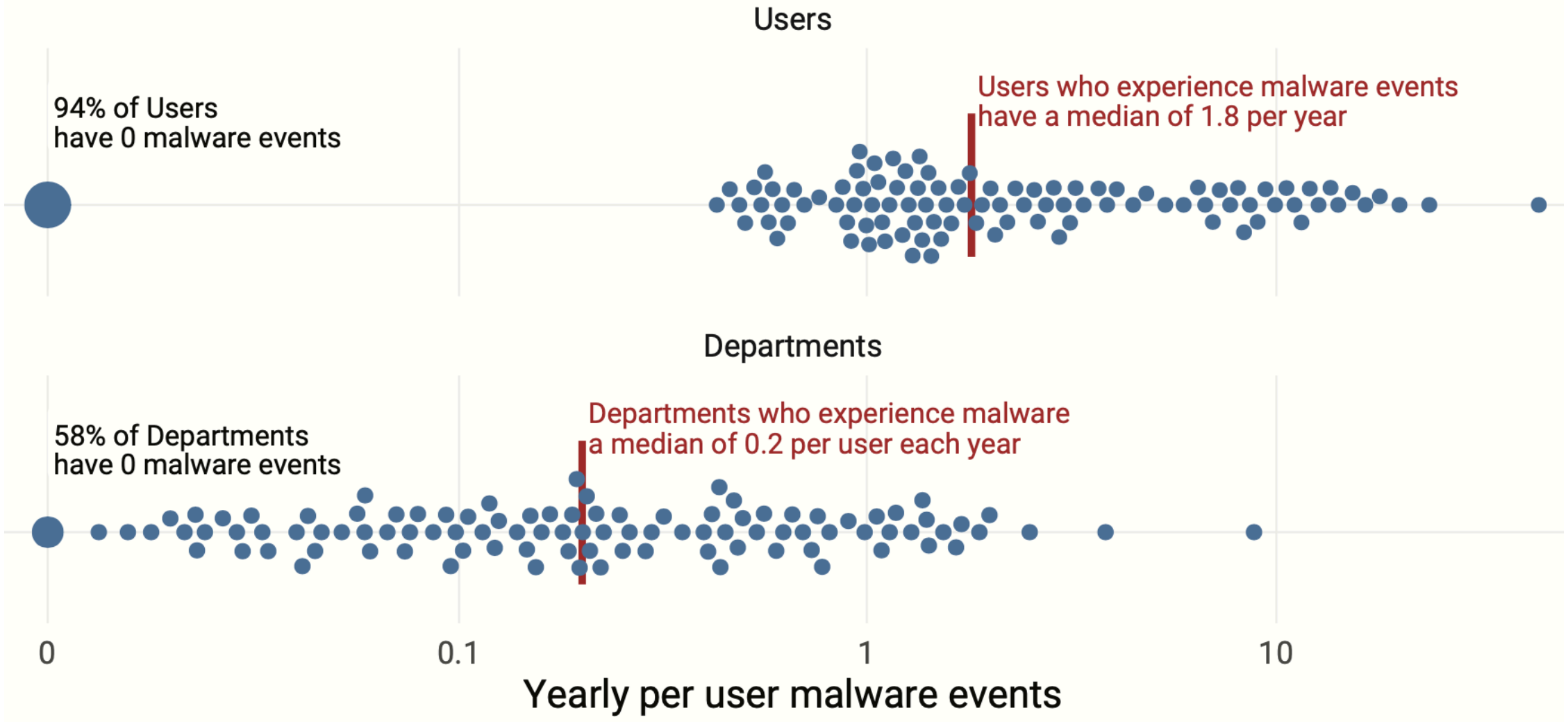


Benchmark: phishing emails CLICKED

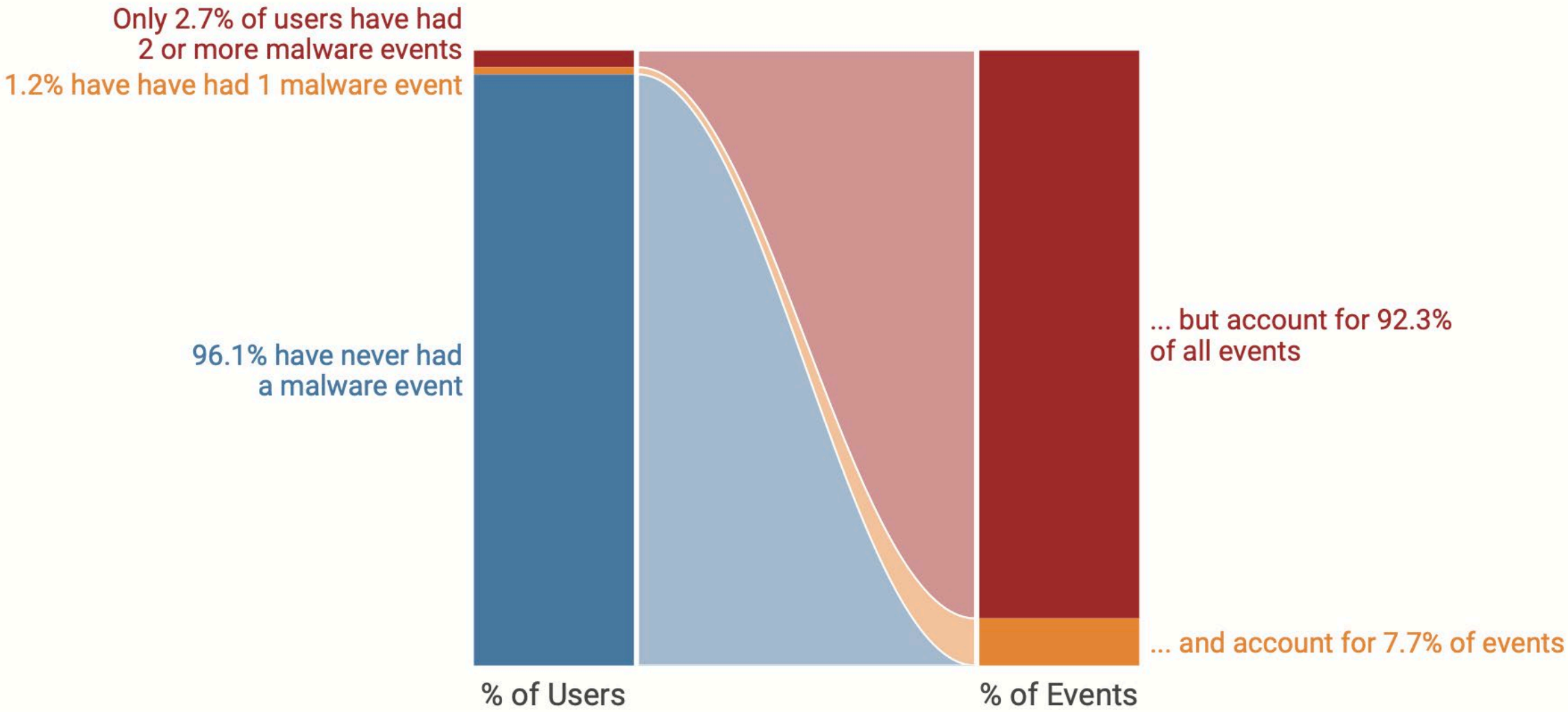


Benchmark: Number of successful phish

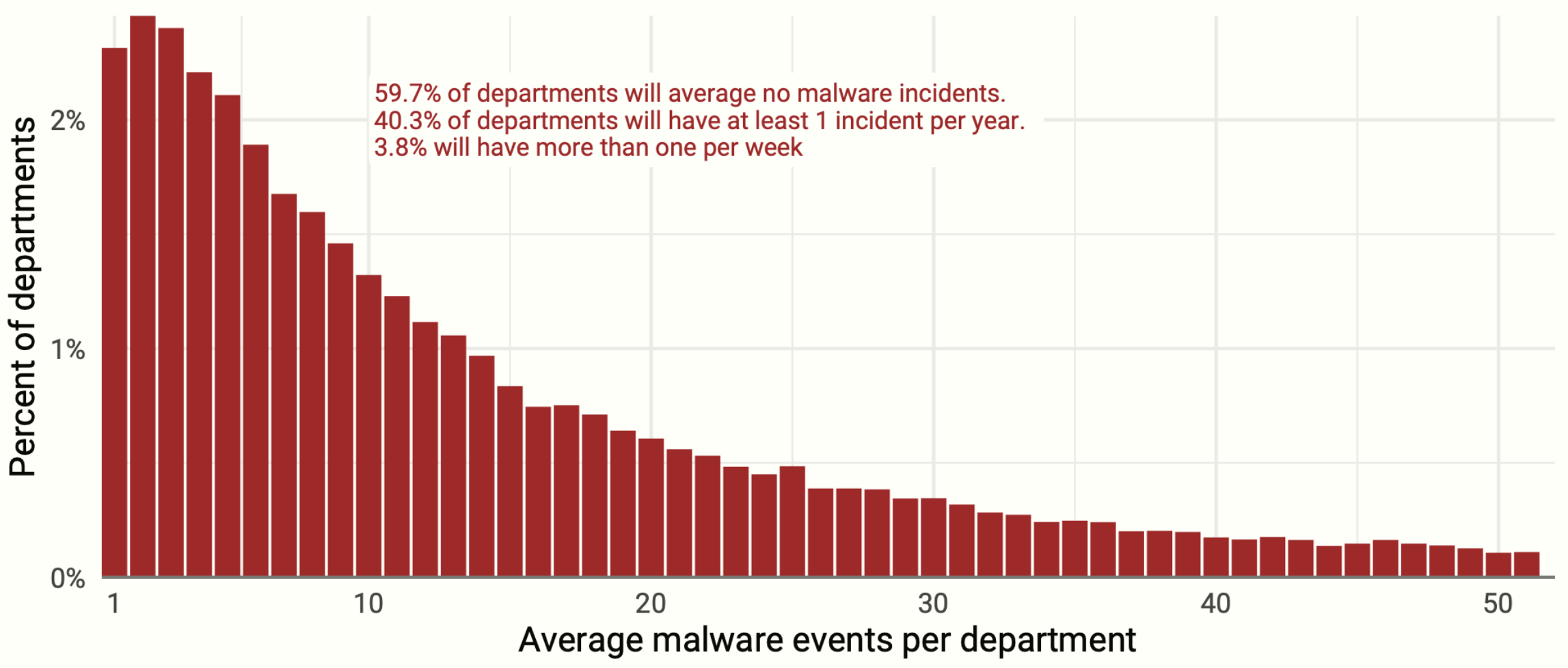
Benchmark: malware received



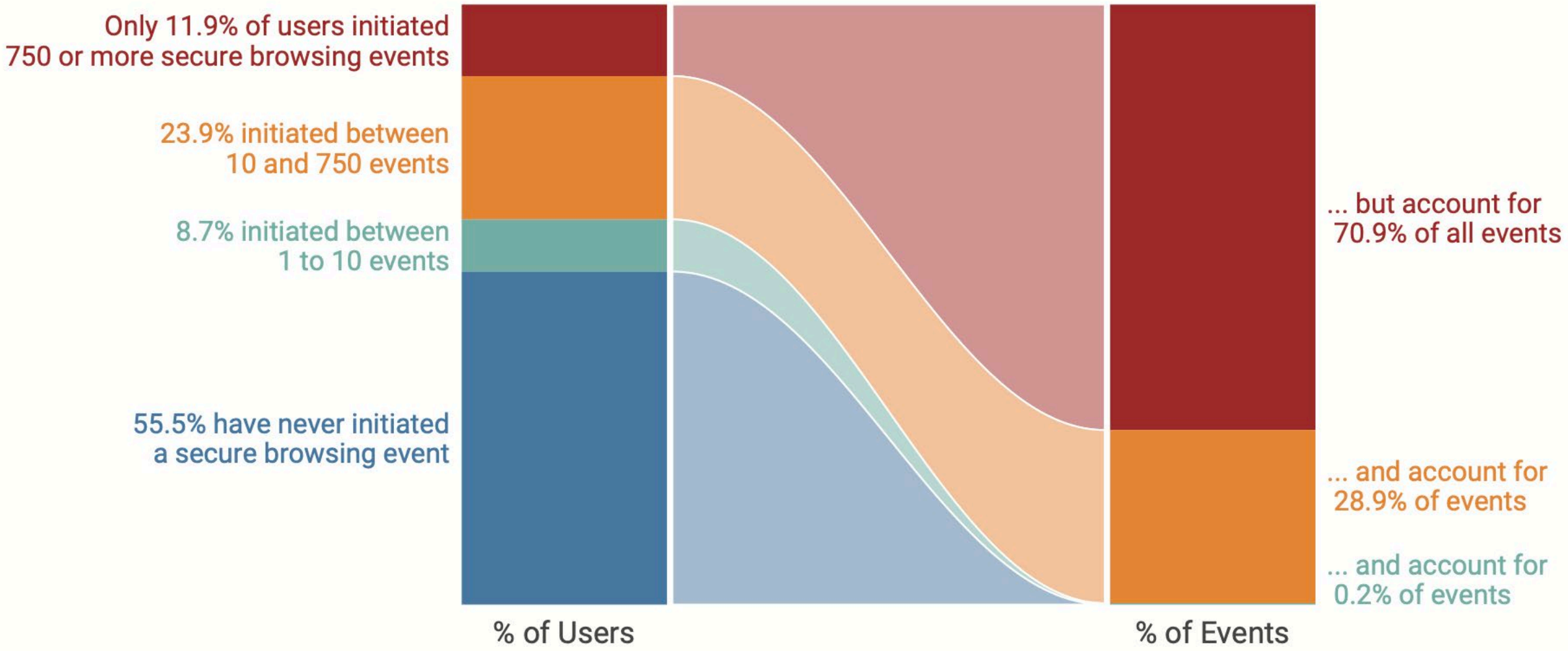
Benchmark: malware downloaded/executed



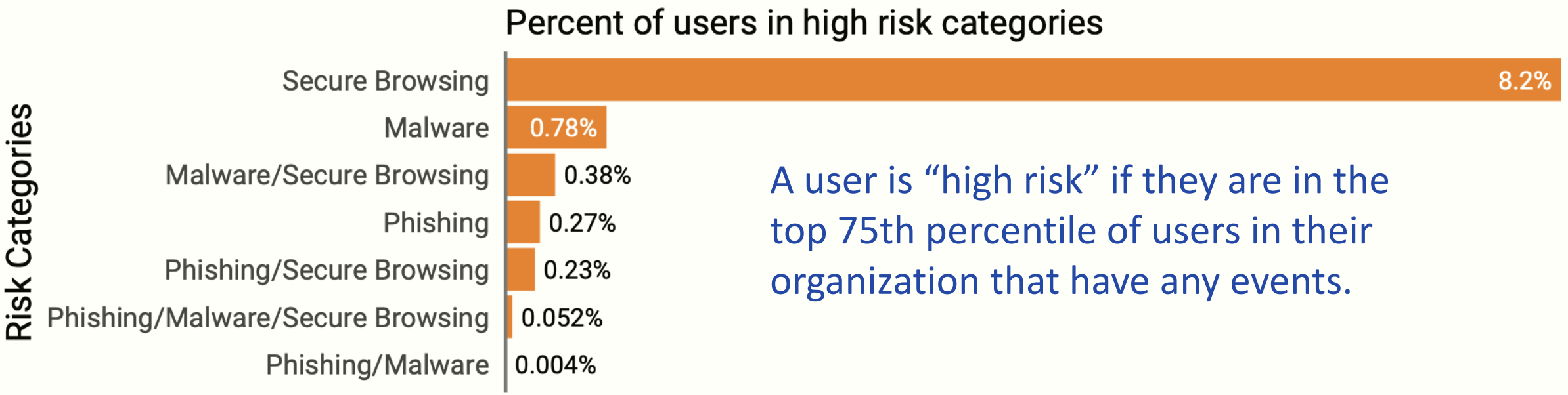
Benchmark: Number of successful malware



Benchmark: browsing policy violations



Combinations of risky behaviors



A user is “high risk” if they are in the top 75th percentile of users in their organization that have any events.

FIGURE 13: COMBINATIONS OF RISKY BEHAVIOR

Where do we focus interventions?

9% of users are high risk in one category

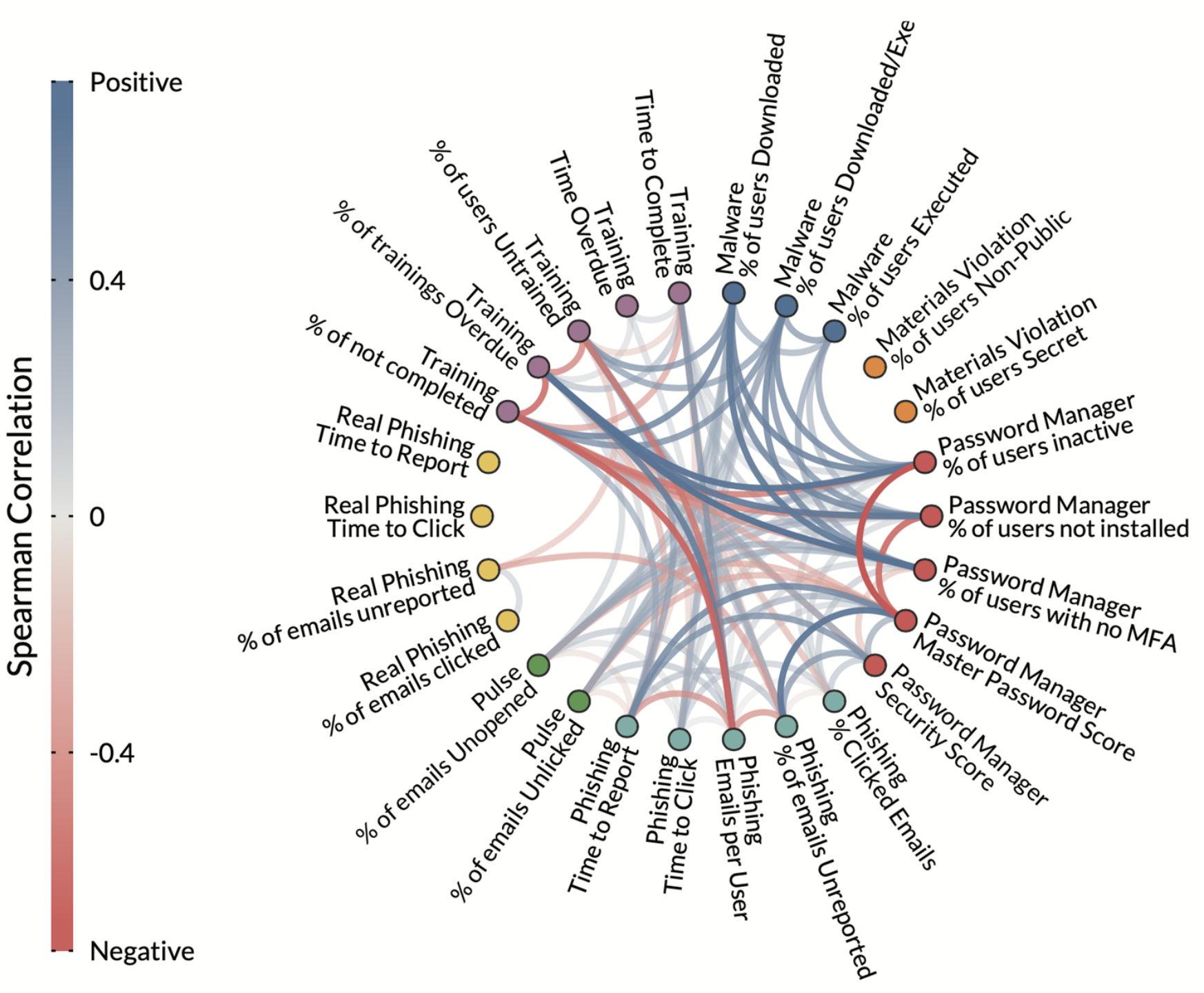
0.6% of users are high risk in two categories

0.05% of users are high risk in three categories

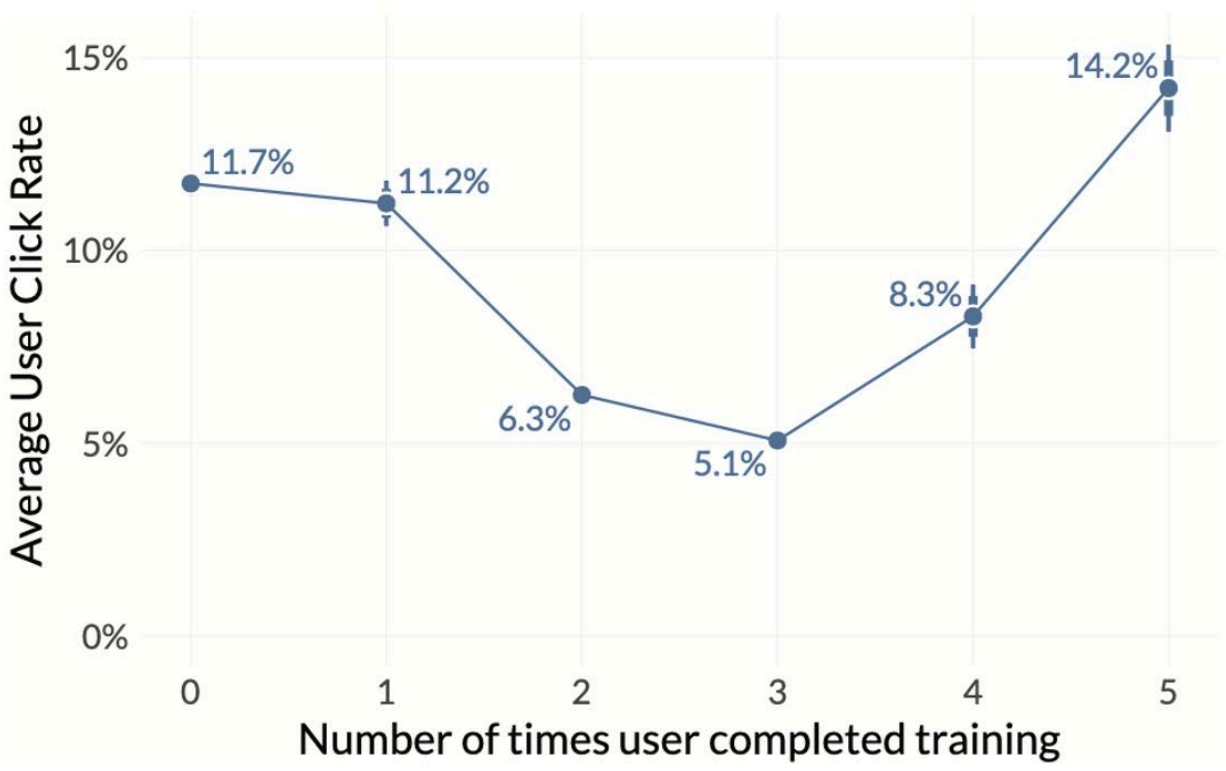
RSAConference2022

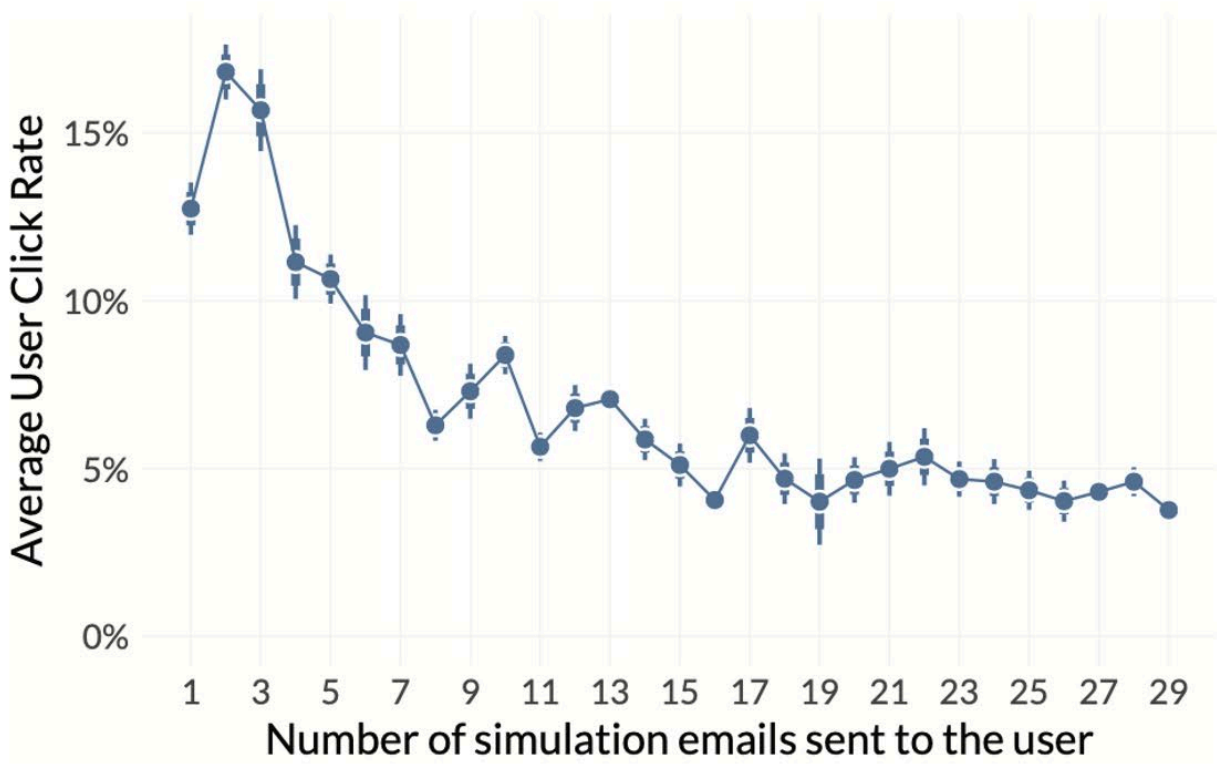
Lessons in Managing Human Risk

Signals of human risk are complex and intercorrelated

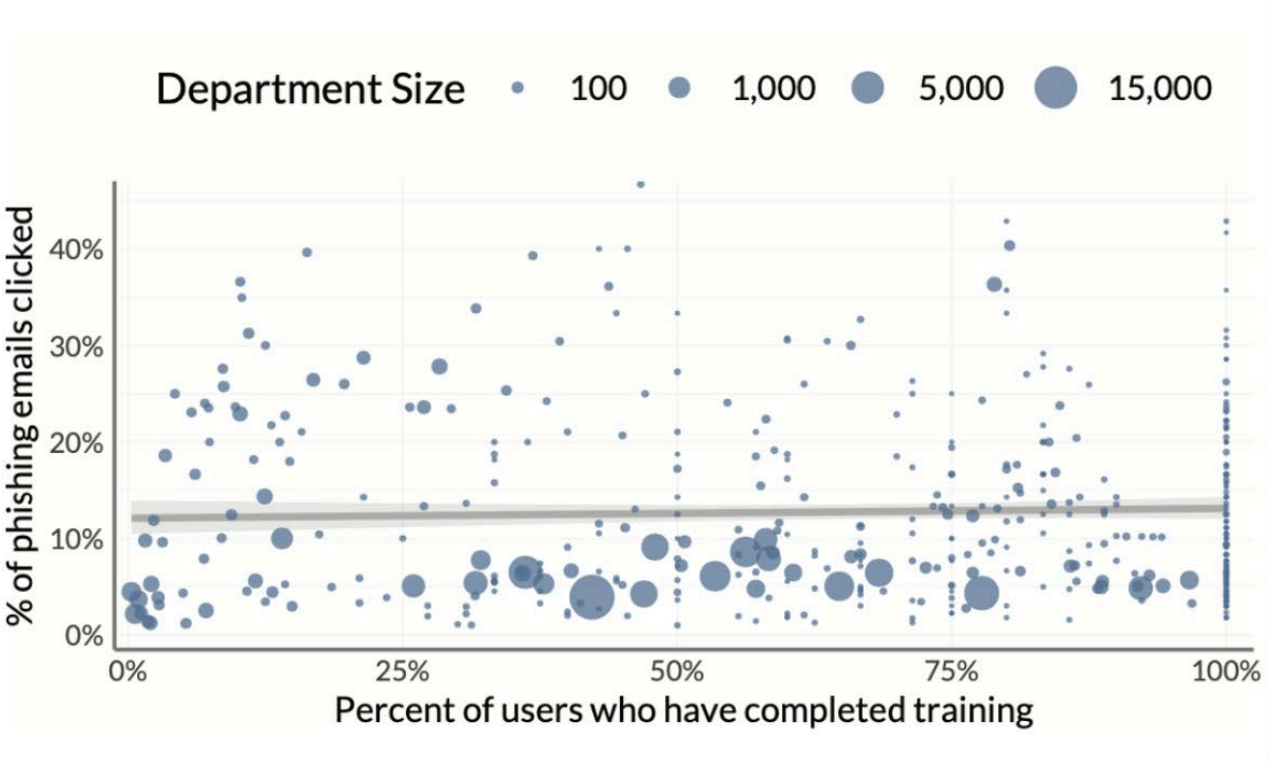


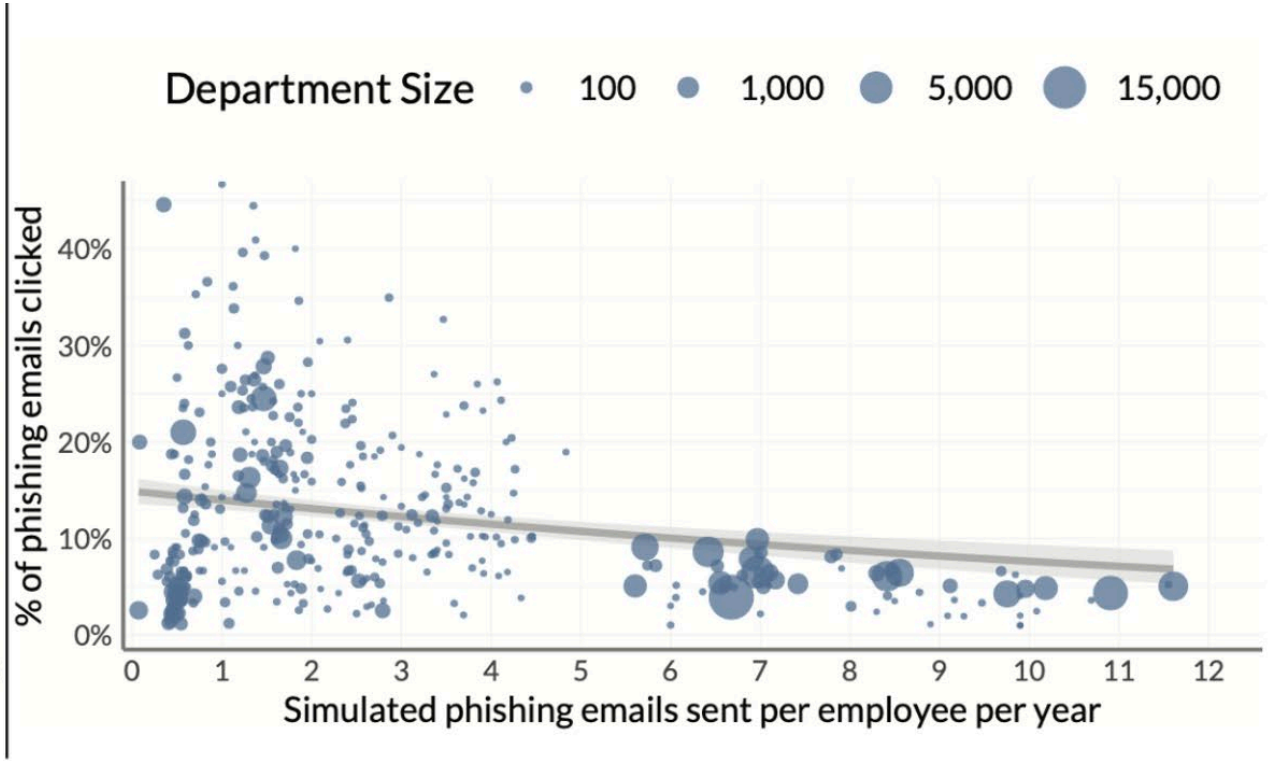
Training doesn't solve human risk



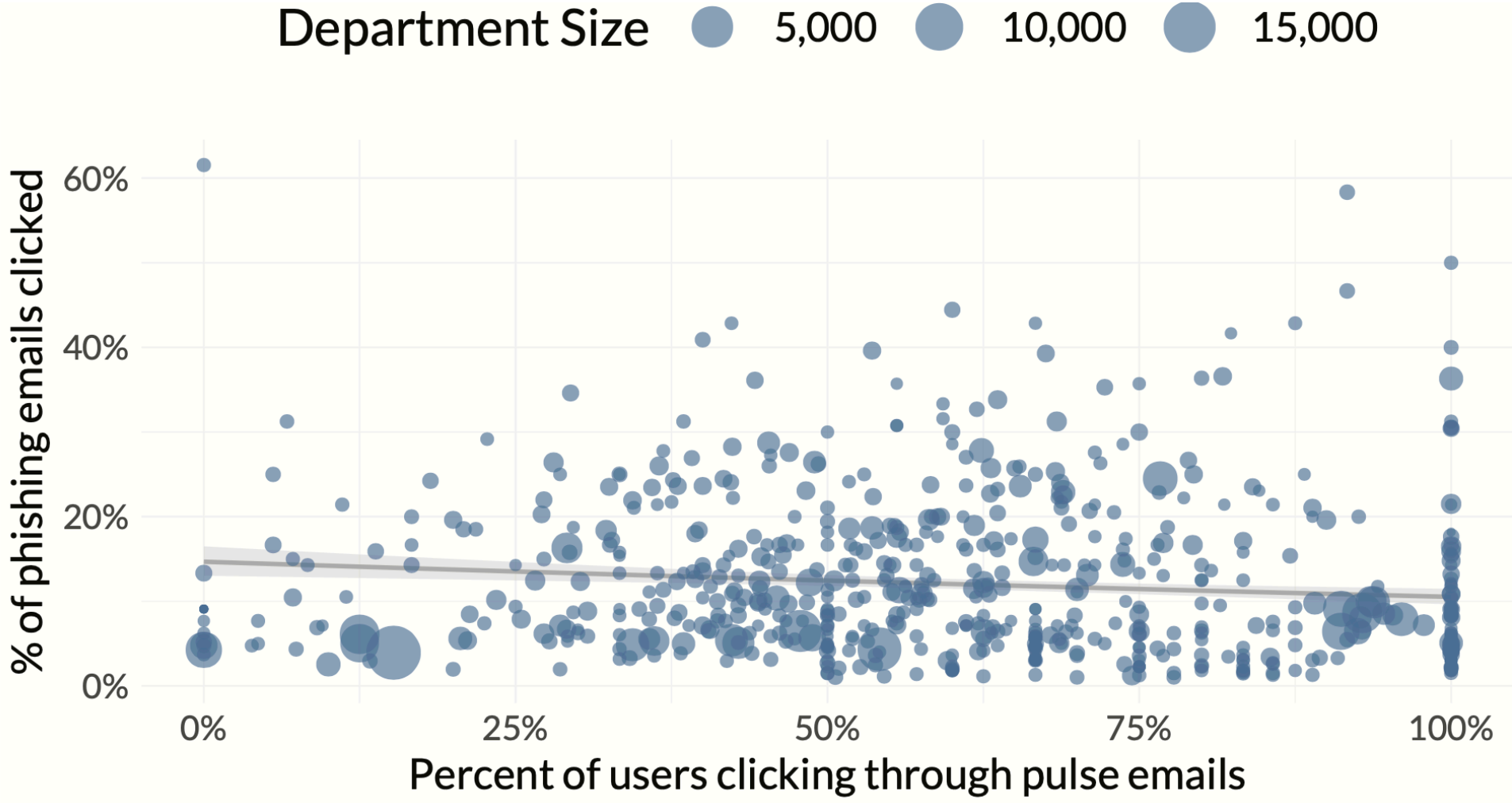


Groups are harder to manage than individuals





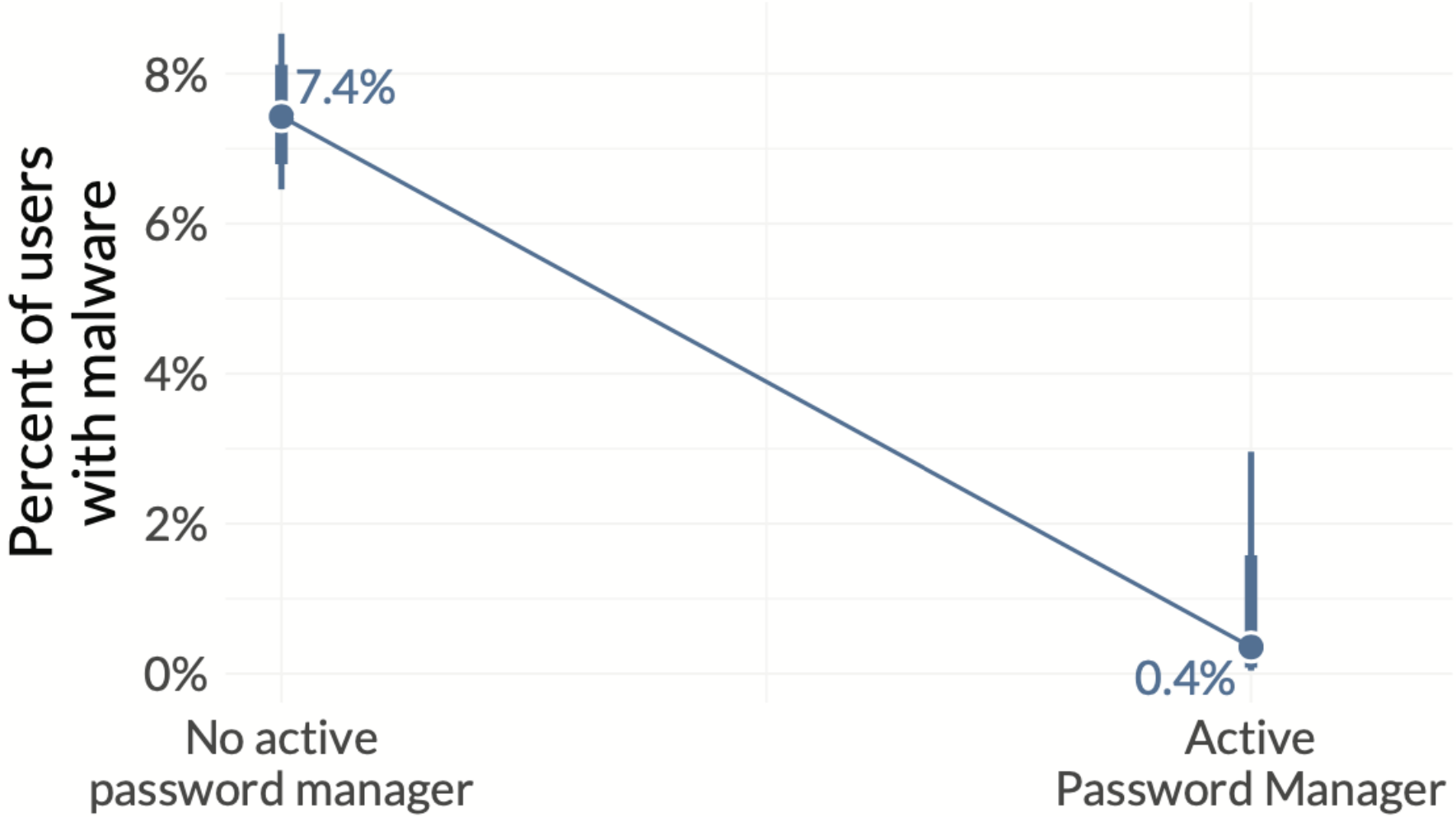
Benchmarking is better than a briefing



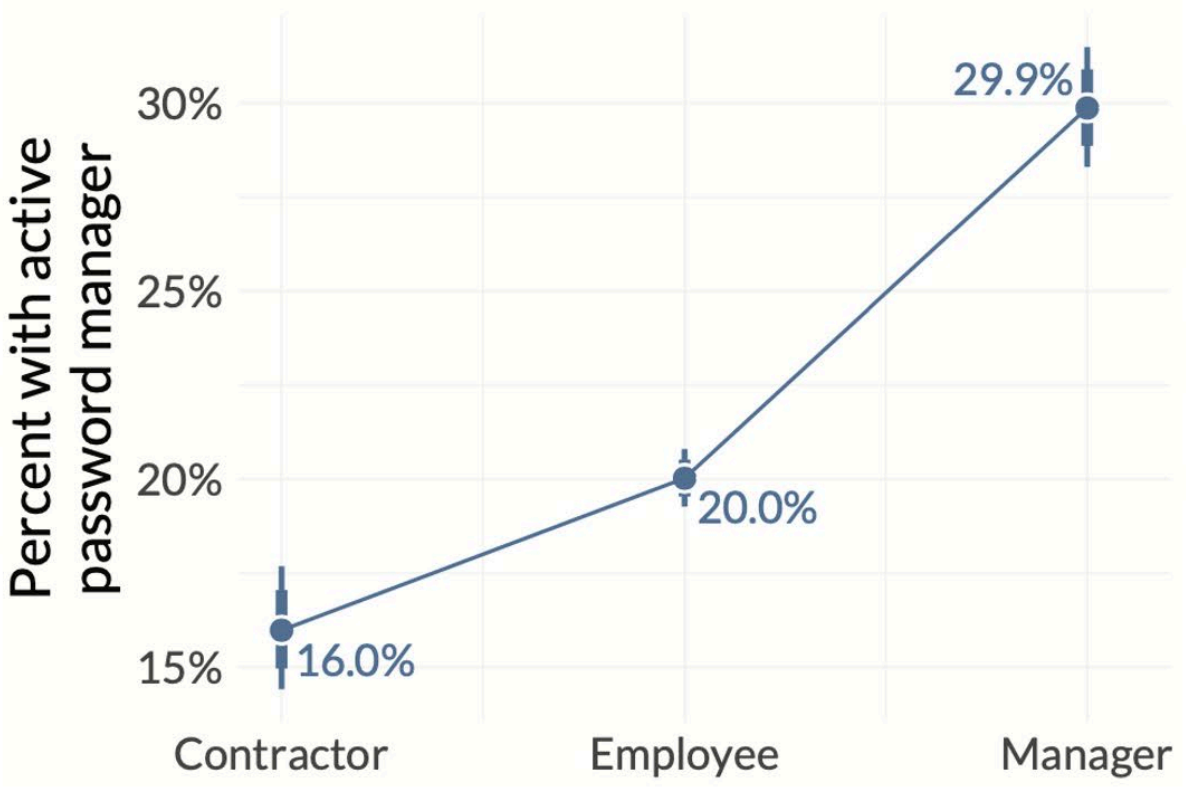
Benchmarking is better than a briefing

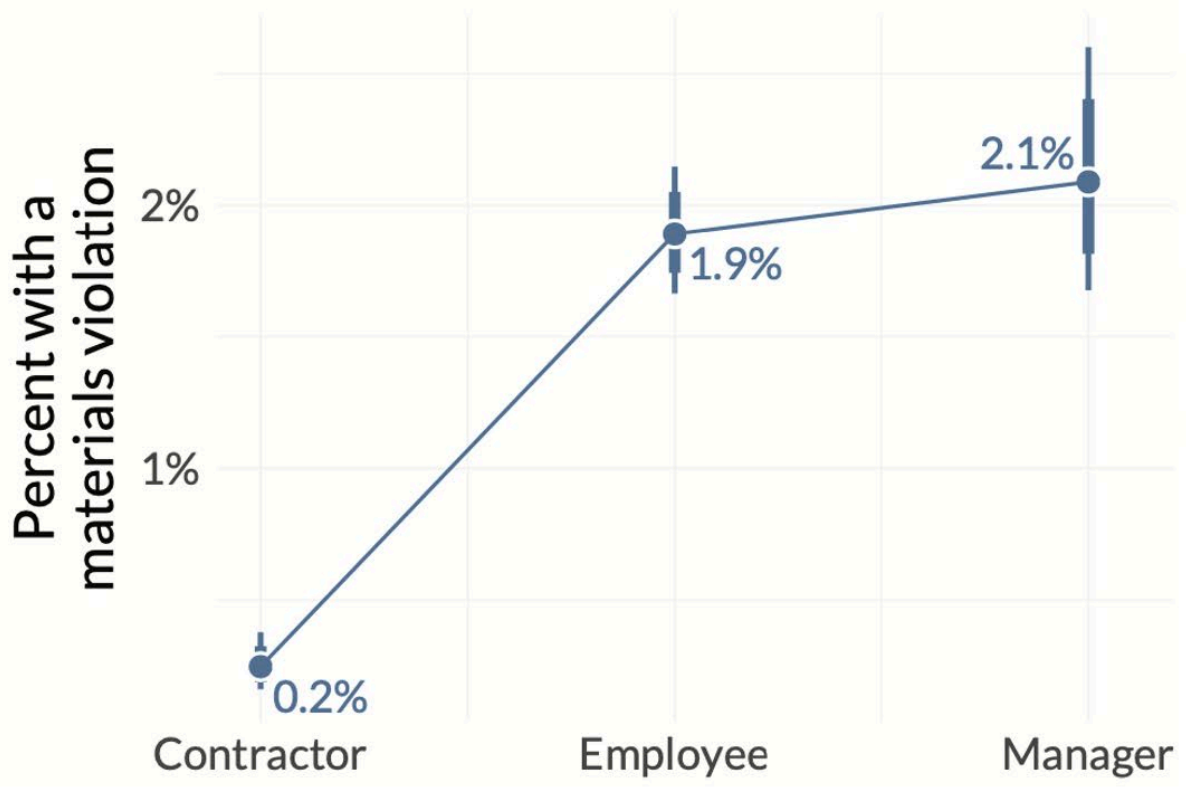
More broadly, this hints that strategies like benchmarking and proactive actions may hold greater promise for reducing human risk than mandatory or punitive interventions.

Equip users to do the right thing

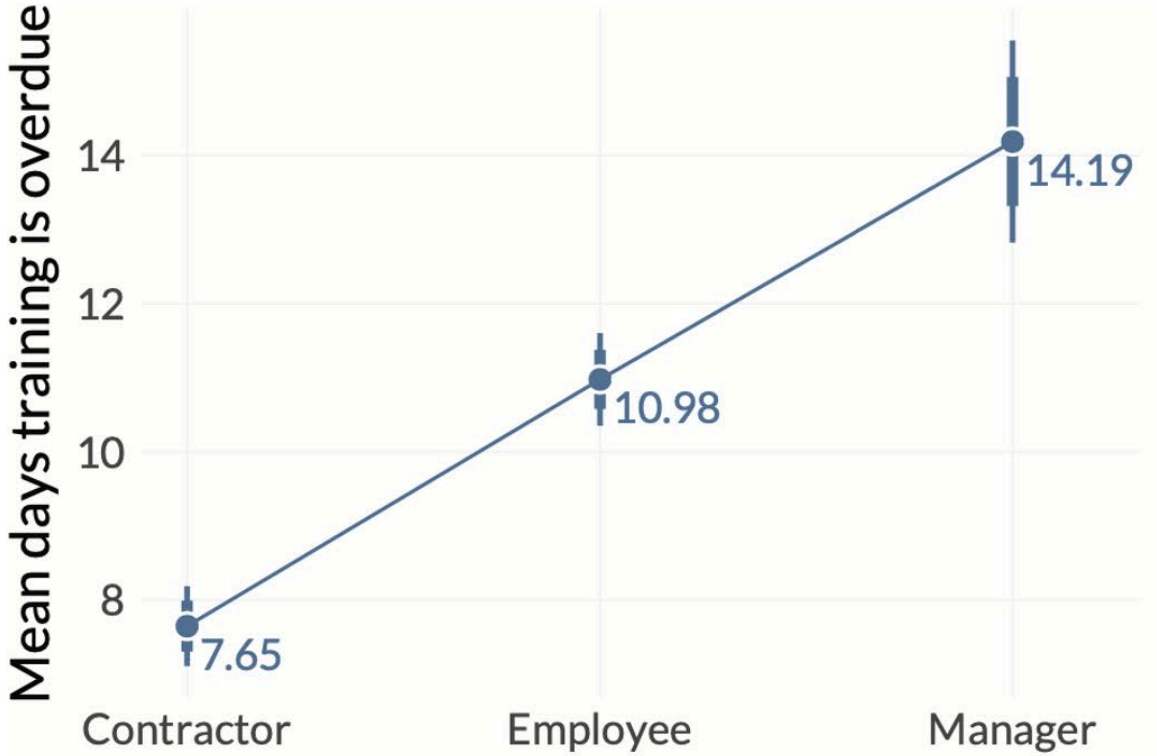


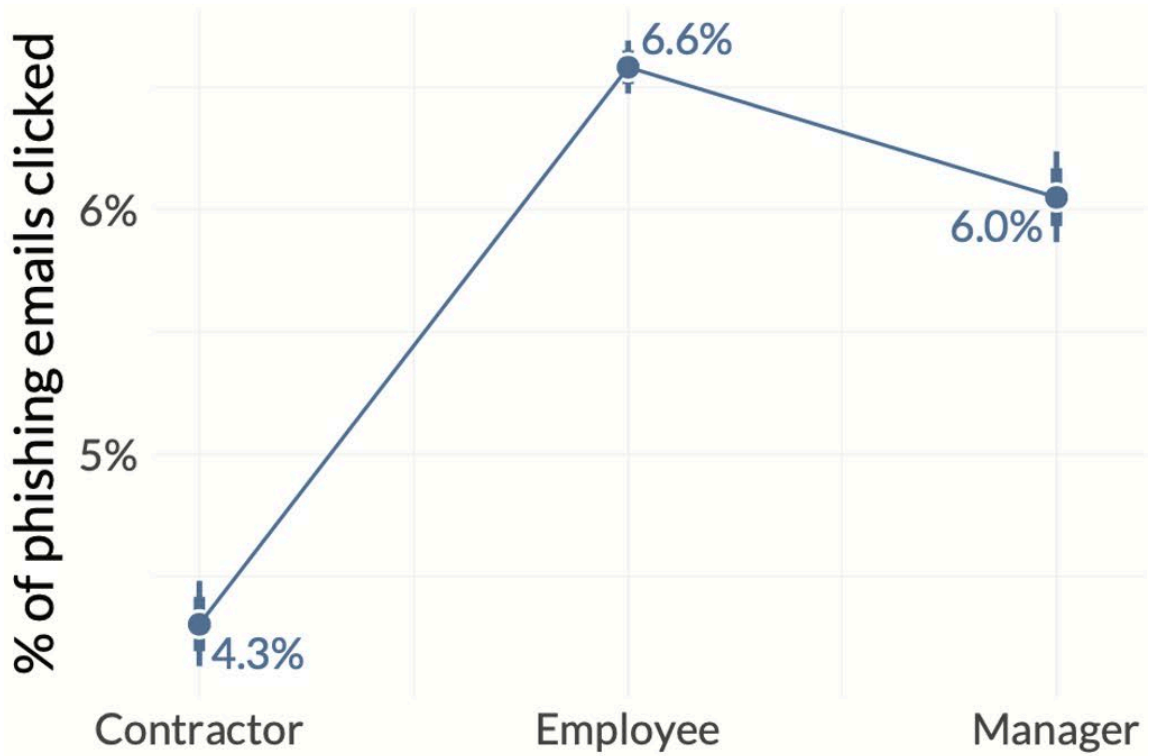
Human risk is a role-playing game



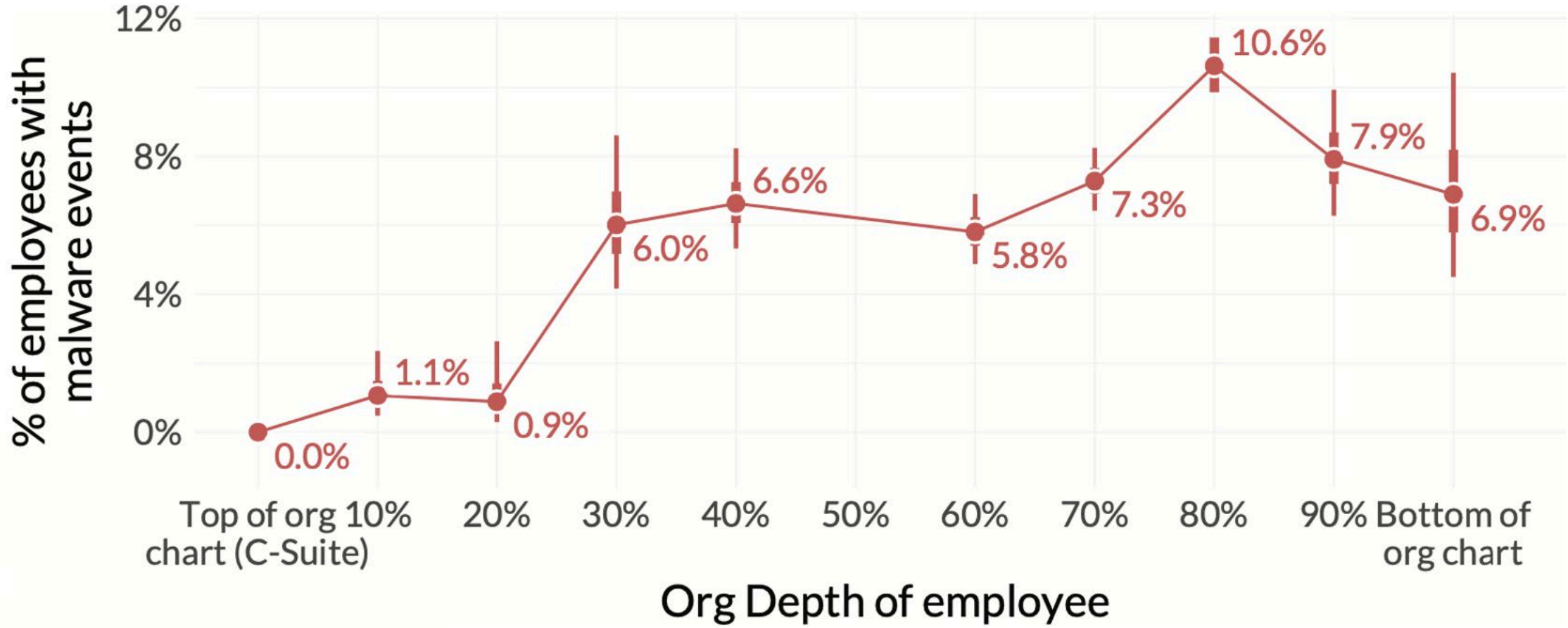


Human risk is a role-playing game





Human risk is a role-playing game



Summary Of Key Findings

- On average, 3% of employee exhibit 2 or more risky behaviors likely to introduce incidents
- 15.6% of users will click through one phishing email per year. 1% will click more than 12 a year (~ ONCE A MONTH)
- 18% of employee have riskier browsing habits than the average employee
- Too much security training (3+) and simulated phishing (11+) can be counter-productive.
- First-line managers are most likely to introduce malware than any other leadership role.

Applying These Findings

- Not everyone is the same when it comes to making security decisions.
- One-size-fits all policies are too restrictive for some and not enough for others.
- Pinpointing helps focus our mitigation efforts on areas we have most impact.
- Use insights to work *with* employees instead of *against* to help them improve.
- Iteration, not perfection. You will always have employee who make mistakes. Focus on highest 3% of risky users. Iterate.

RSAConference2022

Questions?