



Do Unto Others: A Red Team Ethical Framework for Offensive Rules Of Engagement

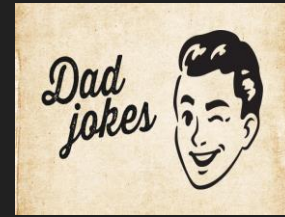
Tarah Wheeler and Roy Iversen

Shmoocon 2020
January 31, 2020

>whoami



@tarah



@royiversen





Privileged Account Compromise and Insider Threat Detection

Survey finds federal agencies embracing zero-trust security model

34% of data breaches are inside jobs



By [Michael Klazema](#)

Published 1 week ago





Privileged Account Compromise and Insider Threat Detection

CASE DISMISSED —

Exonerated: Charges dropped against pentesters paid to break into Iowa courthouse

Dismissal is a victory for the security industry and the customers who rely on it.

DAN GOODIN - 1/30/2020, 5:57 PM

34

breaches are inside jobs

By [Michael Klazema](#)

Published 1 week ago



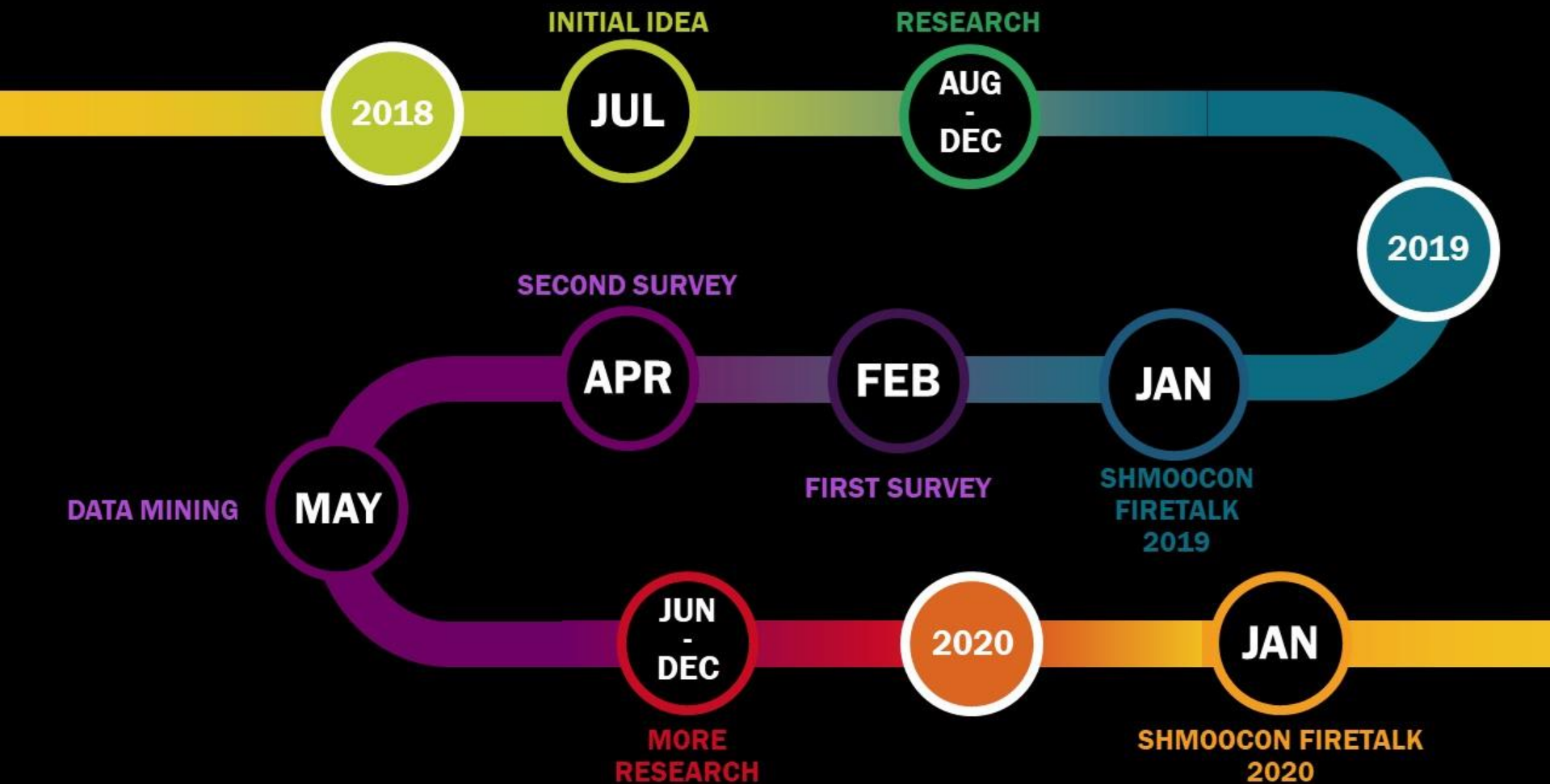


The Road so Far...

Last season on Shmoo-pernatural...

THE ROAD
SO FAR...







Roy Iversen
@royiversen

I had a great time presenting our Firetalk at [@shmoocon](#) with [@tarah](#) on Friday. Want to help out? Go to our survey at [redteamsurvey.com](#) (redirects to Surveymonkey) and tell us which red team exercises you think cross the line.

7:44 AM · Jan 20, 2019 · [Twitter for Android](#)



Tarah
@tarah

Say, are you in information security and stuck behind a computer like me and [@royiversen](#) right now? Would you please consider doing a 2 min, 2 question survey on offensive security/red team tactics between beers and Overwatch/PUBG?


[redteamsurvey.com](#)

9:31 PM · Apr 5, 2019 · [Tweetbot for iOS](#)



Tarah
@tarah

I and [@royiversen](#) would like to request your assistance in responding to and spreading this survey on Red Team Ethics in information security. It is 2 questions, will take less than 3 min, and will help us to understand offensive security ethical choices. [redteamsurvey.com](#)

 [surveymonkey.com](#)

Survey on the Ethics of Offensive Security

10:01 AM · Apr 2, 2019 · [Hootsuite Inc.](#)

SURVEYS!



The Improved Survey

1. Which of these potential offensive security tests do you feel are always wrong and should never be used in a sanctioned test?

- | | |
|---|--|
| <input type="checkbox"/> Send a phishing email | <input type="checkbox"/> RAT (remote access Trojan) a non-work device (laptop/tablet/phone) or a device belonging to a family member |
| <input type="checkbox"/> Target the company receptionist for sensitive information | <input type="checkbox"/> Using debt or other problems from OSINT (public info) to blackmail an employee |
| <input type="checkbox"/> Send emails threatening legal action | <input type="checkbox"/> Threaten to harm an employee's family members |
| <input type="checkbox"/> Impersonate an executive and spoof their email to send orders to employees | <input type="checkbox"/> Compromise legal or confidential documents inside the company |
| <input type="checkbox"/> Involve external or unaware parties and trick them into aiding you | <input type="checkbox"/> DoS/DDoS the organization |
| <input type="checkbox"/> Phish the CEO or other VIPs, making executives look bad or stupid | <input type="checkbox"/> Destroy production data/systems as part of an attack or test |
| <input type="checkbox"/> Point out the flaws in a colleague's work especially if they are friendly or important | <input type="checkbox"/> Planting actual or fake illegal content on a machine to blackmail user |
| <input type="checkbox"/> Bribery | |
| <input type="checkbox"/> Any other ideas that occur to you? | |

2. Which of these roles describes you best

- ☐ Red team/Pentester - tests your own organization
- ☐ Red team/Pentester - tests other organizations
- ☐ Security but not Red team/Pentester
- ☐ IT but not Security
- ☐ Other (Non IT)

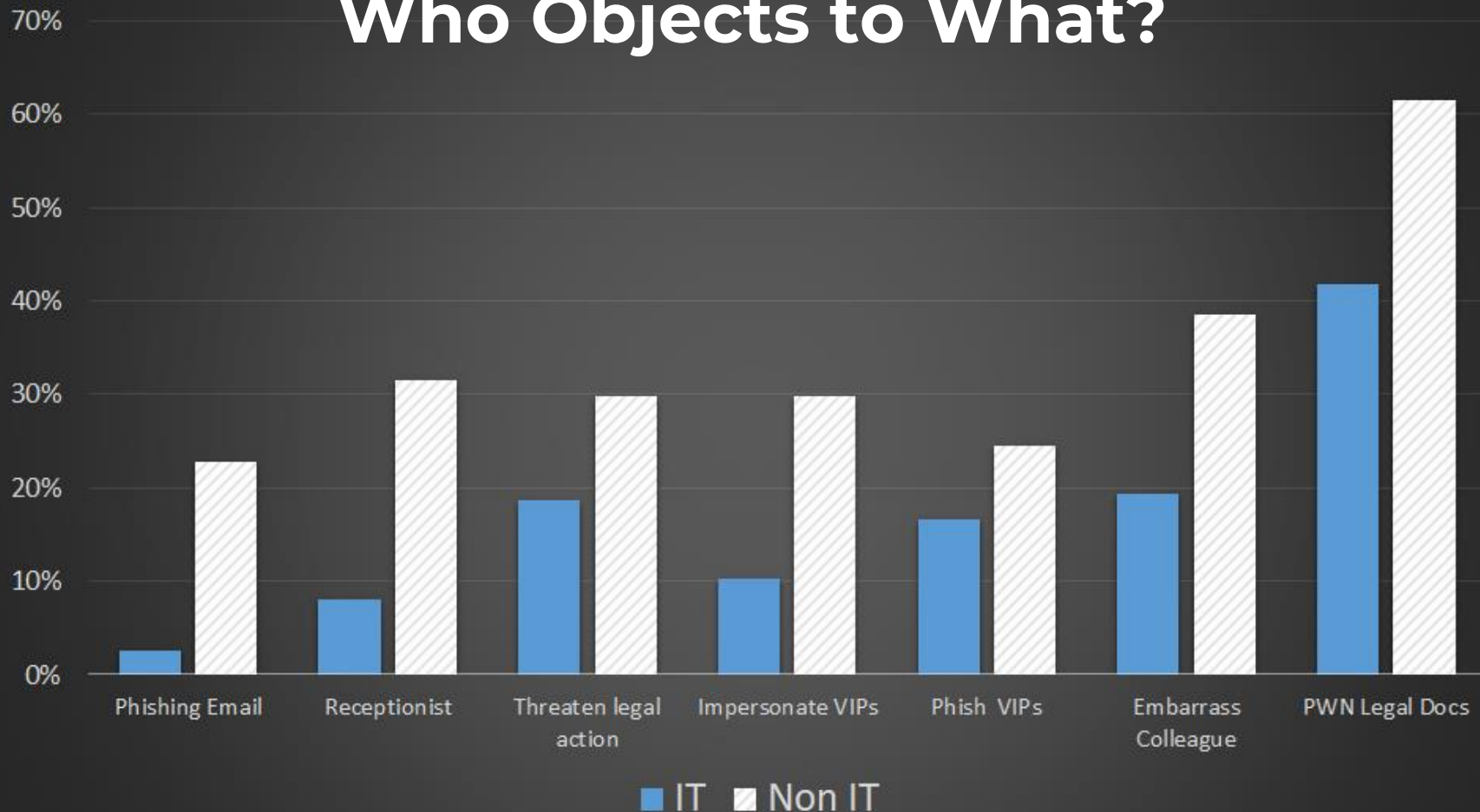
| | |
|-----|---|
| 68 | IT but not Security |
| 57 | Other (Non IT) |
| 93 | Red team/Pentester - tests other organizations |
| 81 | Red team/Pentester - tests your own organization |
| 239 | Security but not Red team/Pentester |
| 3 | Unknown (LLamas? Superimposed state of both IT and not IT?) |



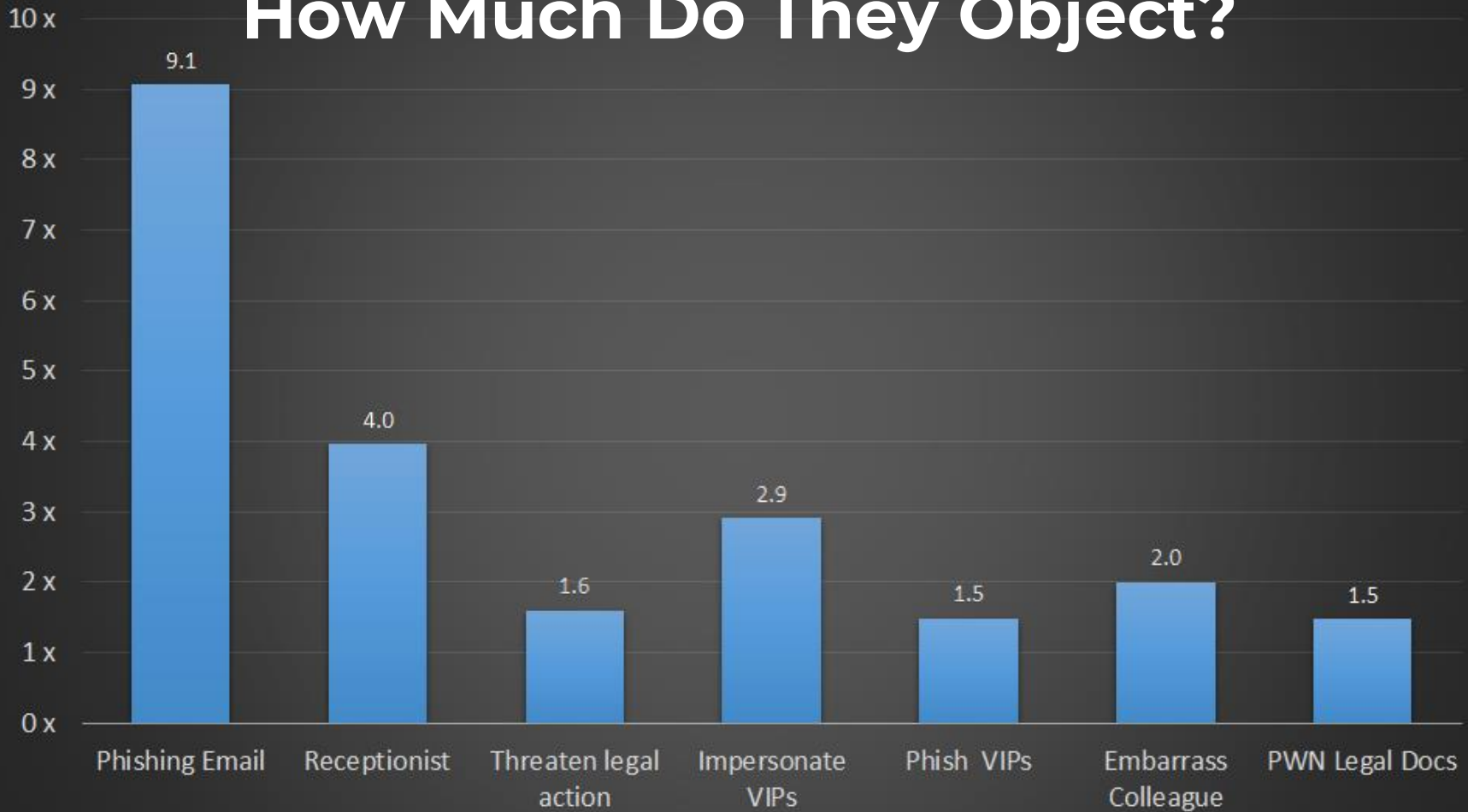


All the Objections

Who Objects to What?



How Much Do They Object?



Non-IT Objections

NON IT respondents are about 50% more likely to object to

- Threatening legal action
- Phishing CEOs and VIPs
- Messing with legal docs

3 times more likely to object to impersonating VIPs

4 times more likely to object to targeting the receptionist

And over **9** times more likely to object to phishing

9x

Security vs All Other Respondents

70%

60%

50%

40%

30%

20%

10%

0%

Non-Security team respondents:

*2x - 4x more likely to object to
these than **Security Teams!***

Phishing Email

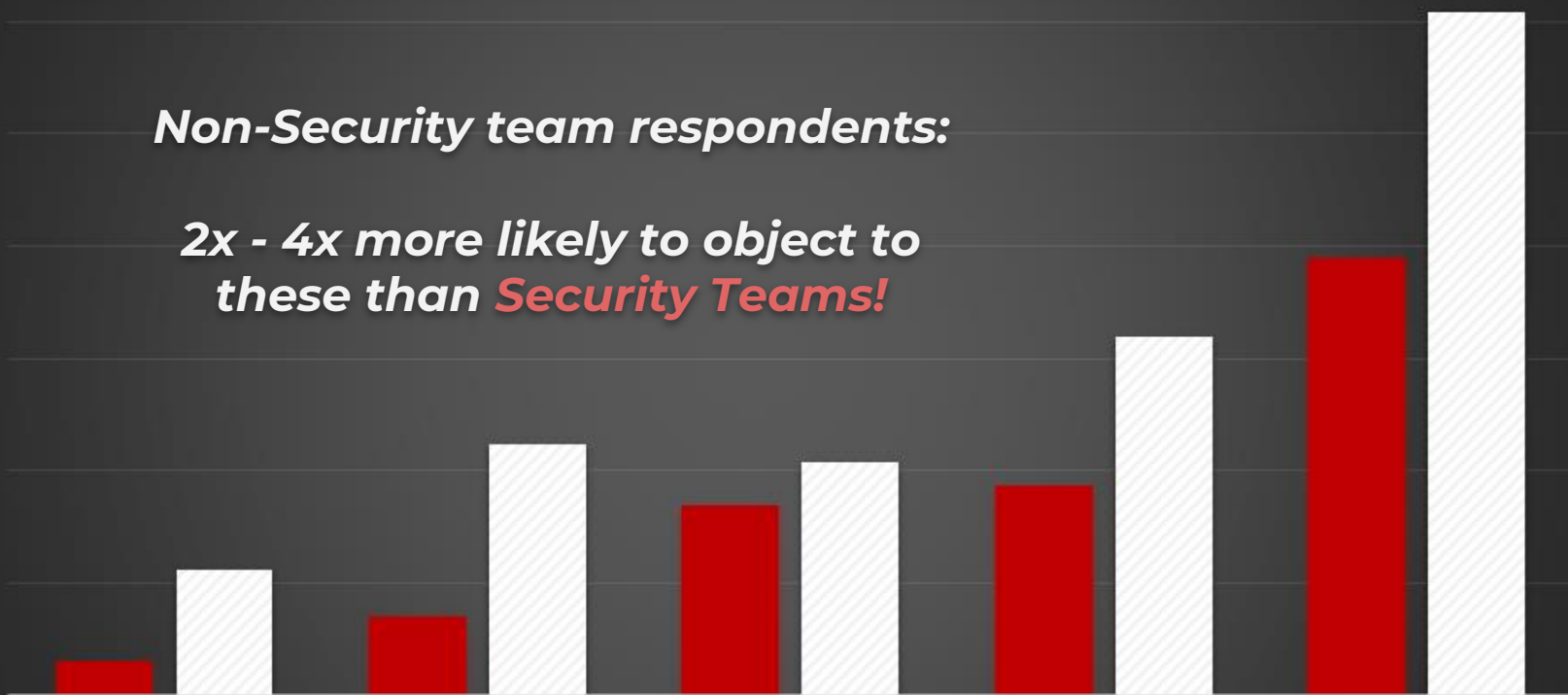
Receptionist

Phish VIPs

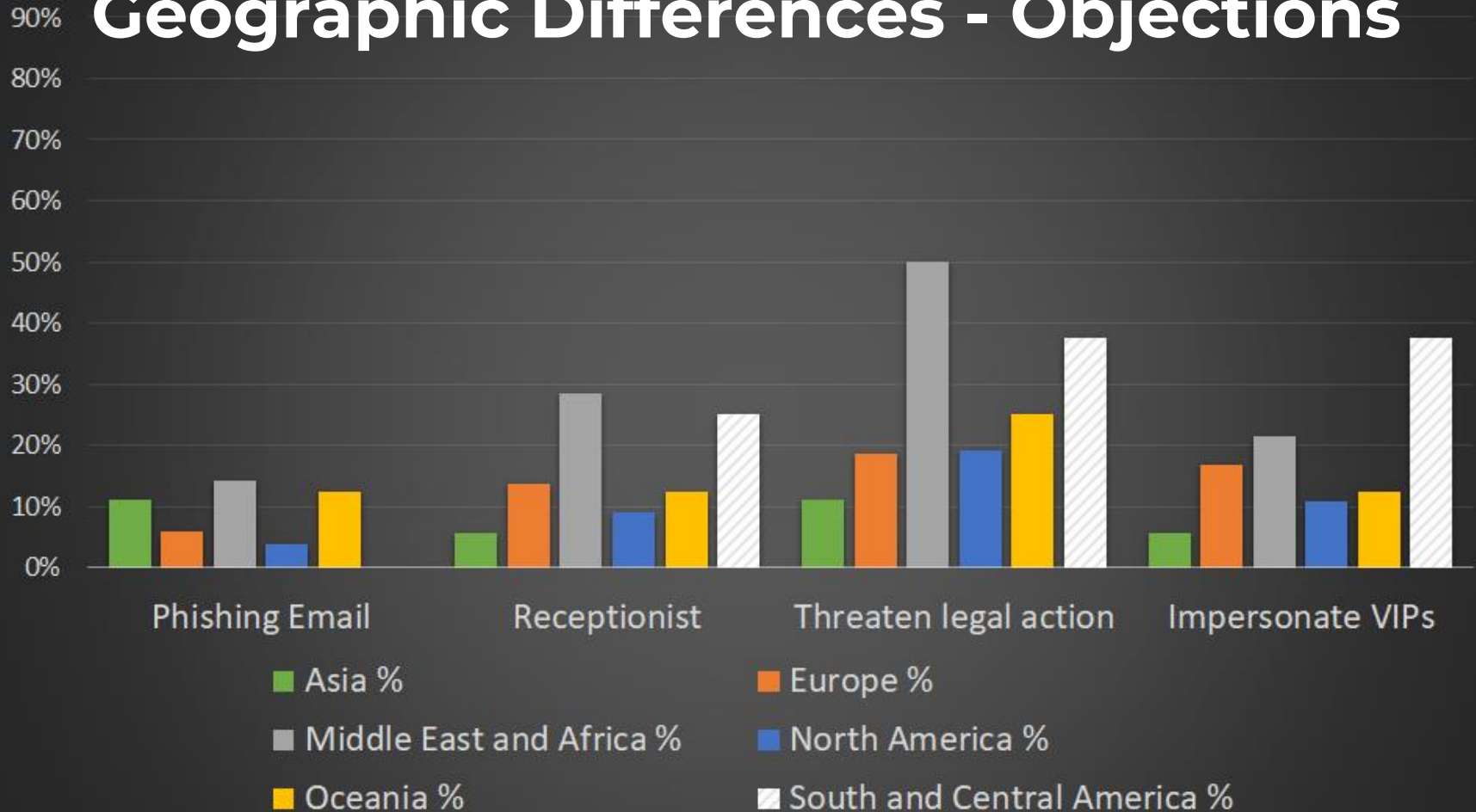
Embarrass Colleague

PWN Legal Docs

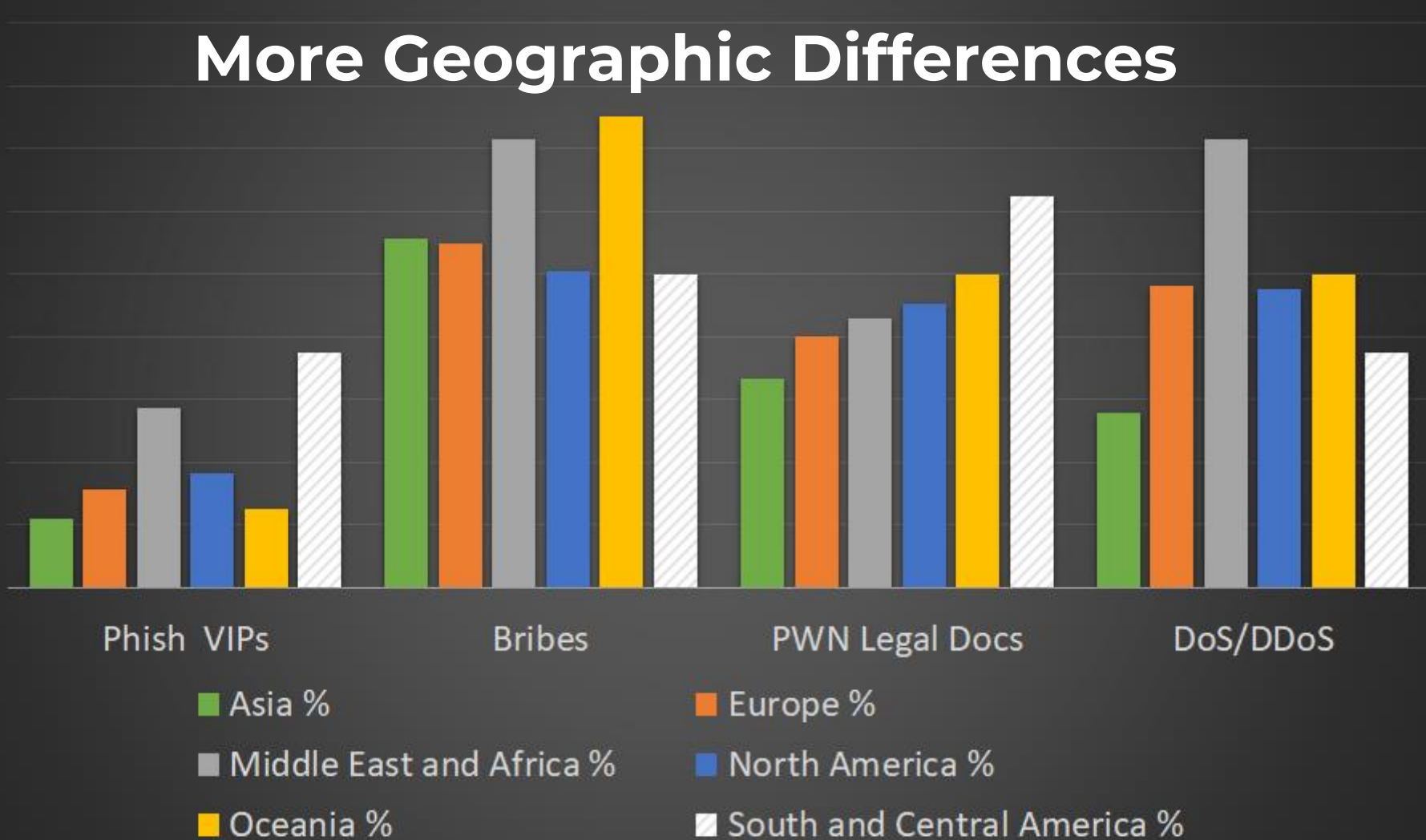
■ Security ■ All other Respondents



Geographic Differences - Objections



More Geographic Differences





**BUT
WAIT**

**THERE'S
MORE**

A/B Testing!

1. *Which of these [tests] do you feel ... should never be used in a sanctioned test*

VS

1. *If you found out a coworker had used any of these potential [tests] during a sanctioned test inside your company, which of these would negatively affect your opinion of that coworker?*

“As long as you don’t test *ME*.”

If YOU are the target of social engineering,
you are **1.5x - 4x** more likely
to object to these tests



Conclusion?

Humans are bad at being objective.

* *Footnote for those reading these slides later:
Takeaway is NOT that you should avoid all of these tests
It's to be AWARE of the biases, and the impact they can have on your teams, colleagues and clients*



The Future

Next Steps

- Looking for a home for this research
- New Survey with Better sample sizes
 - Geographically
 - Job roles
- We would LOVE HELP
 - Help us come up with even better questions!
 - Help us analyze the new data

Sources & Resources

Good research isn't conducted in a vacuum. We build on those that come before us!

Project github repo

<https://redteamethics.com/> (redirects to <https://github.com/redteamethics/redteamethics>)

Research:

- Mouton, Francois & Malan, Mercia & Kimppa, Kai & Venter, H.s. (2015). Necessity for ethics in social engineering research. Computers & Security. 55. 114 - 127. 10.1016/j.cose.2015.09.001.
- Mouton, Francois & Malan, Mercia & Venter, H.s. (2013). Social Engineering from a Normative Ethics Perspective. 10.1109/ISSA.2013.6641064.
- Faily, Shamal & Jacob, Claudia & Field, Sarah. (2016). Ethical Hazards and Safeguards in Penetration Testing.
- "Social Engineering in IT Security: Tools, Tactics, and Techniques: Testing Tools, Tactics & Techniques"
- Mouton, Francois & Malan, Mercia & Leenen, Louise & Venter, H.s. (2014). Social Engineering Attack Framework. 10.1109/ISSA.2014.6950510.

Blog posts

- <https://jacobian.org/writing/social-engineering-pentests/>
- <https://medium.com/starting-up-security/red-teams-6faa8d95f602>

General social engineering resources of interest:

- <https://opendatasecurity.io/the-most-famous-cases-of-social-engineering/>

Thank You!

YOU

THE COMMUNITY

SHMOOCON FIRETALKS

OUR COLLEAGUES AND FRIENDS

special thanks to

*Anna Friedley and Adaya Queen for priceless input and ideas
and Deviant Ollam for graphic design*

<https://redteamethics.com>



@royiversen
roy.iversen@gmail.com

/reiversen

twitter
email
web
instagram
linkedin
facebook

@tarah
t@tarah.org
<https://tarah.org>
@tarahwheeler
/tarah
/tarahwheeler

fin