Version 0.5

Working paper only; not yet peer-reviewed and fact-checked. Consume at your own risk

What We Do Unto Others: Red Team Engagements, Hurt Feels, And Ethical Penetration Testing

Roy Iversen & Tarah Wheeler

Abstract

What are the effects of red team tactics on the people who conduct them as well as the people who become the targets? We talk about offensive security as if it exists in a vacuum without human cost, and it's time to look at the consequences of treating humans as checkboxes.

In 2019, we, Roy Iversen and Tarah Wheeler conducted an initial and then a more detailed survey on how offensive security researchers (the polite phrase for "hackers") are perceived when they test inside their own companies or others. We began with an initial session at ShmooCon in Washington, DC, and then expanded to a set of questions that had some surprising results both within information security and in the larger tech industry. We have refined a detailed survey conducted across the wider information security community. We have nearly 600 respondents already who have answered questions about bribery, threats, and other potential tactics in offensive security testing to determine whether or not some things are always wrong...and while most ethical choices appear at first to be obvious, our research revealed a surprising outcome which we will share with all of you.

Introduction

Those of us who conduct offensive security campaigns use all the tactics of threat actors. We prepare TTPs, gather information, engage the enemy, attack and capture objectives, and pivot victory into further maneuvers. While there are technical specifications about best practices in offensive security methods, our industry is lacking on ethical guidance. Most available literature and discussion at best focus on the legal issues, and rarely or never discuss the role of ethics in our profession.

One thing we do not discuss often enough--or at all--is the effects of red team tactics on internal company morale. What does it mean to lie, cheat, and steal when engaging in testing a company's defenses, and is it smart to permit employees of a company to deceive others? Are there ways to avoid detrimental effects to the perceived integrity of the security professional? For the first time, we can show the ideal conduct of an ethical red team engagement, versus the elements best reserved for external third-party engagements.

We conducted significant research including an initial 40-person survey on detailed tactics and the ethics of conducting red team engagements. In the first version of our survey regarding ethical conduct, we found that threatening family members was the activity most perceived as unethical, and that planting criminal evidence on someone's computer to blackmail them into complying with a red team engagement was the second most significant tactic which the community found distasteful and wrong.

These results in an initial poll encouraged us to refine our research further and conduct a survey with even wider exposure, taking greater care in the quantitative survey design, in which we learned even more counterintuitive facts about the conduct and ethics of red teamers, including their propensity to target high-value executives in order to make examples of them, even if the scoping documents did not explicitly request this tactic. In our second survey, widely responded to by the security community and the public, we received nearly 600 responses to a single question about whether certain tactics were acceptable or not… but what respondents did ***not*** know was that we were running two surveys in parallel (aka a split test or A/B test)--one framing the questions based on the respondent conducting tests, and the second had the identical questions, but framed as a scenario in which the respondent were hypothetically being targeted by such a campaign.

Key Controls

There are key security controls tests which are part of any well-protected company, and some of these tests should not be assigned to or performed by security personnel.

Let's develop out that concept in this paper that demonstrates some of the ethical and professional incentives for internal security personnel.

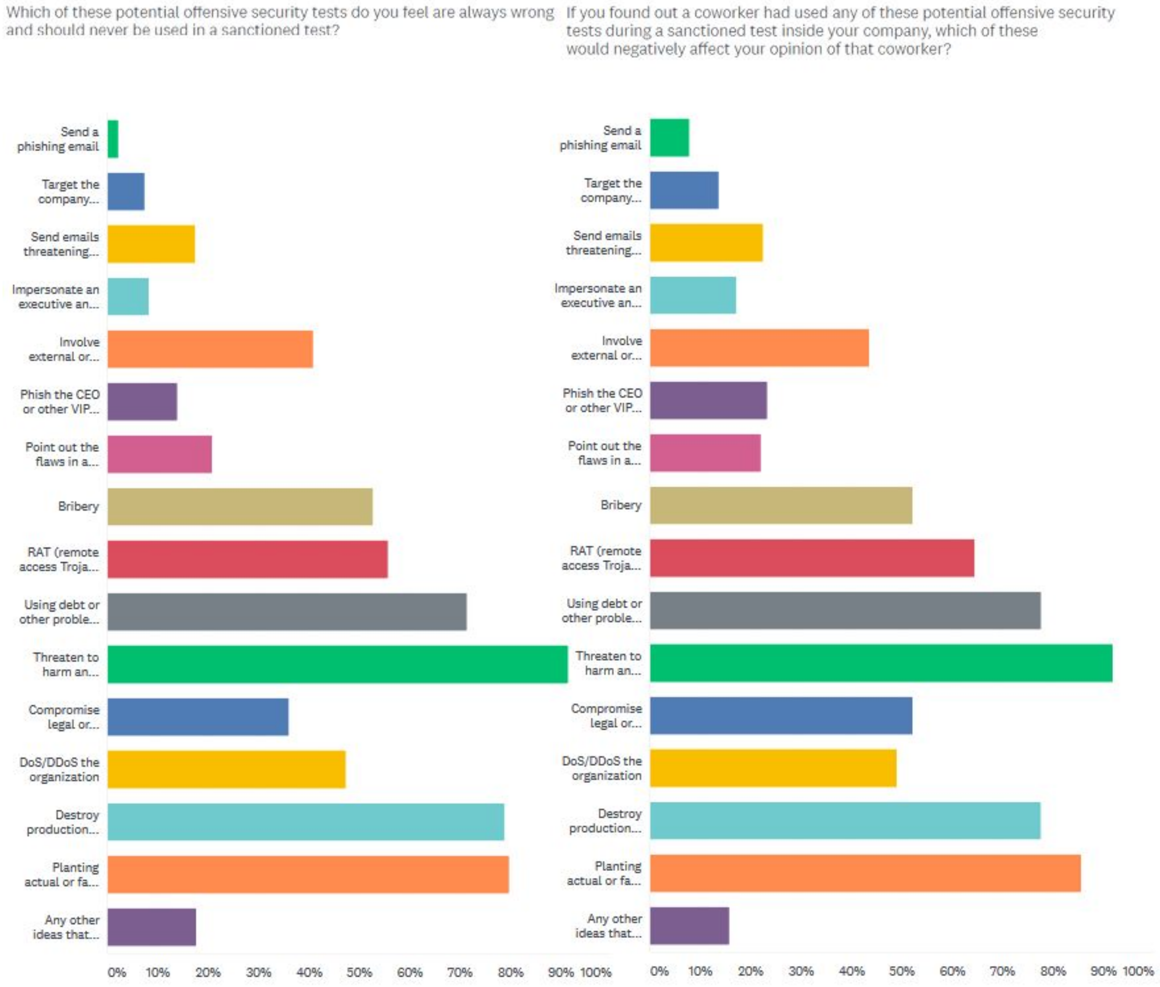
We will 1) describe the results of our original research, 2) draw conclusions about the classes of tests that showed large discrepancies in whether a given test was considered ethical or appropriate, and 3) identify areas where further research is called for.

.

Results

What we found was surprising and counterintuitive. Respondents (even professional security experts) were reportedly 450% more likely to be morally fine with conducting certain often-used tests on *other* people than they are with having tests run against ***themselves.*** We used these results to show the community's perspective on the absolute ethics of certain kinds of offensive security testing.

Note the dramatic differences in framing--especially in the phishing, bribery, and especially in pointing out a colleague's flaws-- in the A/B questions below.



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

If you found out a coworker had used any of these potential offensive security tests during a sanctioned test inside your company, which of these would negatively affect your opinion of that coworker?

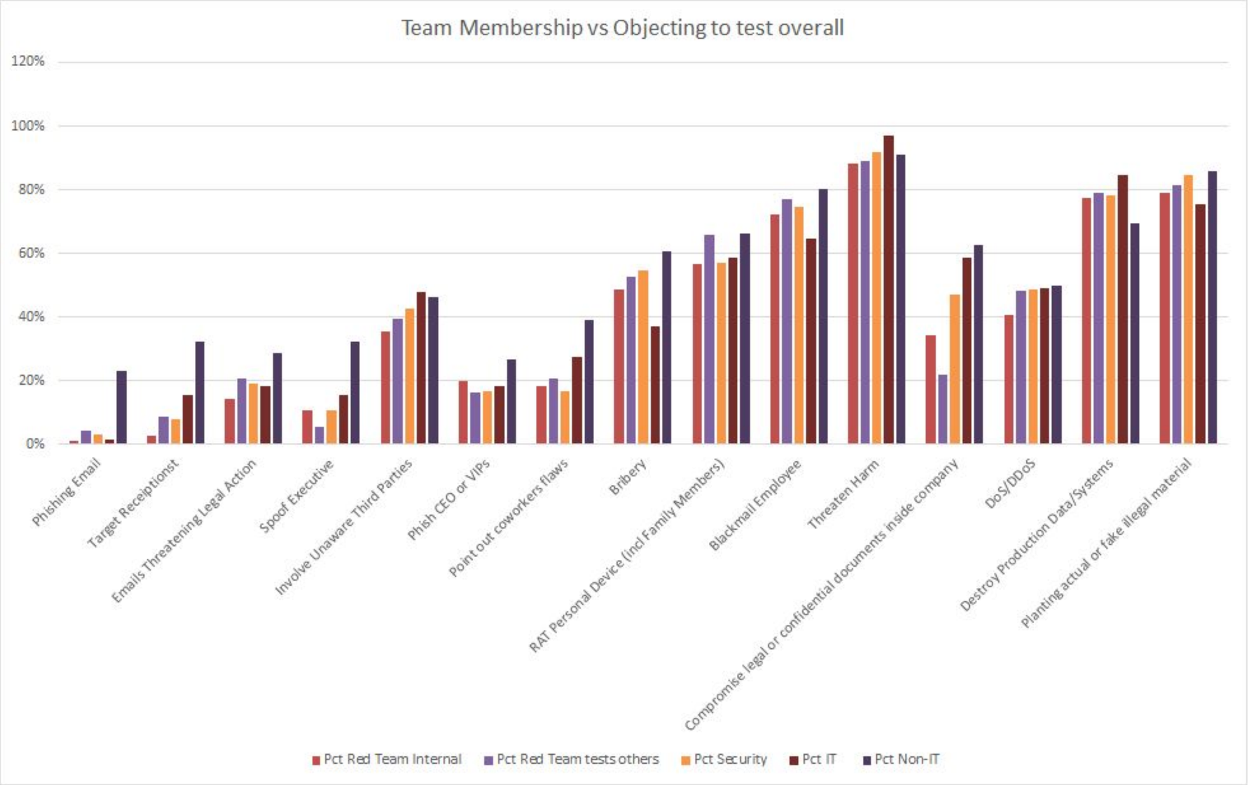
The survey also collected data about the general profession of the respondents, including asking whether people serve as offensive security testers, general security professionals, information technology pros, or in other professions. For instance:

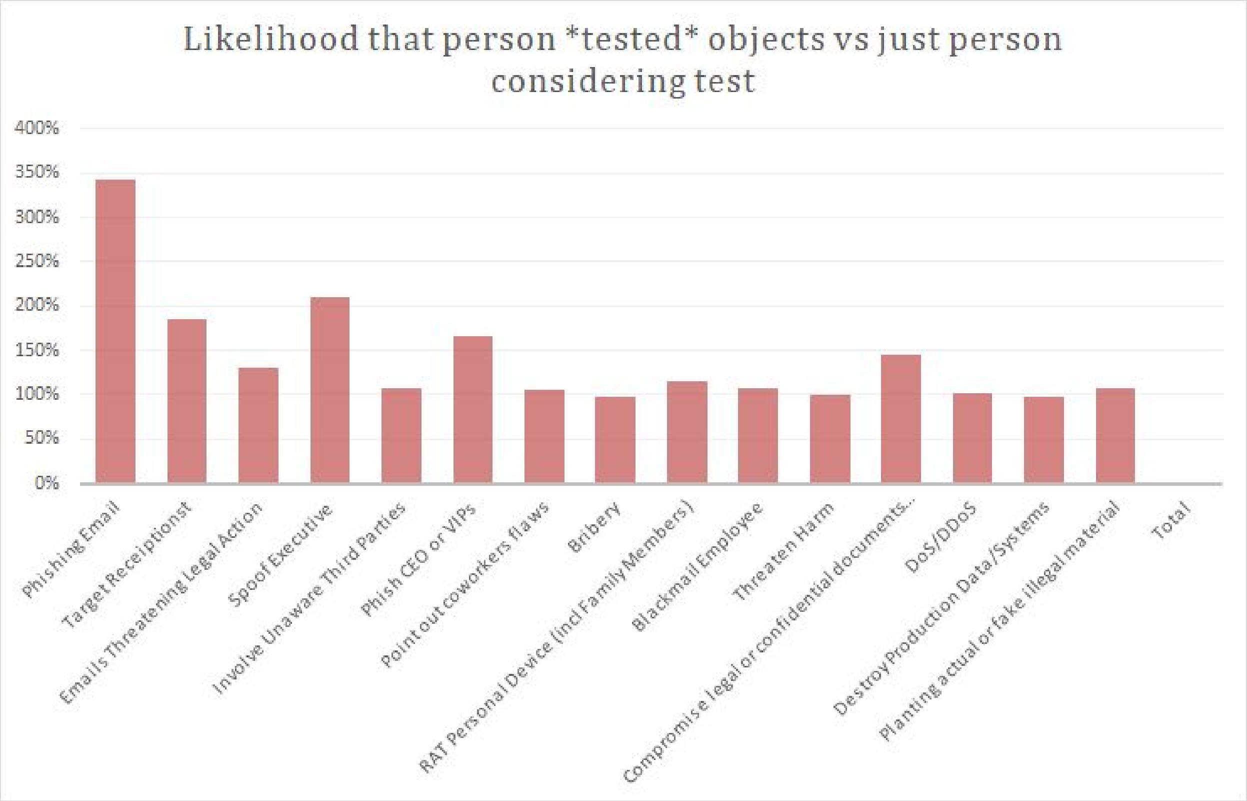
- The data shows that non-IT members are more likely than the other groups to object to most of the tests, but dramatically more so for topics such as phishing or when the testing impacts receptionists, executives or coworkers.

- External red team members care less about compromising legal or confidential documents

- IT teams (Non-security) care more than other groups about the impact to production data and systems.

It also lets us start a discussion about best practices when engaging in *internal* penetration testing (testing your own organization) and the impact of deceptive social engineering and phishing techniques on company morale, and consider whether some exercises are better left for external consultants or hypothetical tabletop exercises.




Likelihood that person *tested* objects vs just person considering test

Affected Classes of Security Controls Testing

Typically, this is where we would review extant literature on ethics and incentives in information security regarding HVT social engineering for internal red teams, but we appear to be the first to research this topic. The closest work to ours might be the SANS Top 20 Critical Security Controls and the research done to find out what is on people's minds.

Our results...

- The data shows that non-IT members are more likely than the other groups to object to most of the tests, but dramatically more so for topics such as phishing or when the testing impacts receptionists, executives or coworkers.

- External red team members care less about compromising legal or confidential documents

- IT teams (Non-security) care more than other groups about the impact to production data and systems.

...help us draw some conclusions about who should be assigned certain classes of security controls testing. These observations can be used when scoping contracts with external teams and constructing rules of engagement.

First, for social engineering attacks such as phishing, vishing, and staff deception especially focused on high value targets such as executives, we can see that internal red teams are improperly incentivized to perform well on those tasks. Making the CEO look like a fool isn't a quick trip to an outstanding performance review, a raise, and promotion tracking or leadership training.

> *"Making the CEO look like a fool isn't a quick trip to an outstanding performance review, a raise, and promotion tracking or leadership training."*

Takeaways for boards overseeing cybersecurity measures in publicly traded companies could consist of: 1) hearing a direct presentation at a half-yearly minimum from the internal head of information security, whether that is at the CISO level or (if your company hasn't matured enough to realize you need one) from whatever beleaguered IT manager has infosec on their plate as well as their normal job, 2) demanding HVT (high value targets) be in scope for red team engagements and pentesting, whether internal or externally sourced, and 3) understanding the incentives for doing a good job and succeeding in compromising targets inside the company.

There's a reason the head of Internal Affairs at police bureaus do not report directly to the police chief: you cannot effectively inspect and regulate your boss. That's the same kind of psychological effect we see working here in internal red team engagements

> *"There's a reason the head of Internal Affairs at police bureaus do not report directly to the police chief: you cannot effectively inspect and regulate your boss."*

Anecdotally, we have heard internal red teamers describing scoping for engagements that disinclude the most likely targets—executives—because those same executives did not wish to have the potential interruption to their services that the discovery of poor security awareness would entail. This is unfortunate, as rapid, constant testing that perpetually integrates small changes leads to the strongest defense of any company.

It is unsurprising to the authors that when faced with a different framing of the same question, that the results were so dramatically different. Understanding cognitive bias in information security and how we frame the ethics of what we do is the goal of this research.

Future Research

Information security is a relatively new field, and the practice of conducting internal security evaluations in cyberspace is quite new. What might surprise many people is that there may only be 3-6 people total at even the largest Fortune company dedicated to internal security testing. Of course, security companies that sell penetration tests and red team engagements as part of their product have a much larger employee base of people with those skills, but they are not directed inwardly as part of the support operations of the company--instead, they're the product the company sells. Think of it the same as a company that sells an HRIS (human resources information system) product to other companies; they still have an internal HR department that's likely much, much smaller than the sales staff and engineers selling their HR product.

It's also common for HRIS companies to not actually use their product inside their own company to manage their own employees--in tech, we call this either "eating your own dogfood" or "drinking your own champagne". One of the reasons companies like Microsoft and Google have built good office suites is they force their own employees to use those products, and this leads to quick fixes that are focused around enterprise service. In security, when this doesn't happen, we call this "arrant hypocrisy" among other less polite names, and it's rampant among security companies.

As industries become more and more mature, process and expectations mature as well. HR as we know it didn't exist 40 years ago, and in 20 years, Gen Z security professionals will shudder to think of the primitive state of internal security controls and testing we all dealt with at this point in time.

We intend to run this survey once a year, iterating for methodological improvements and wider reach.

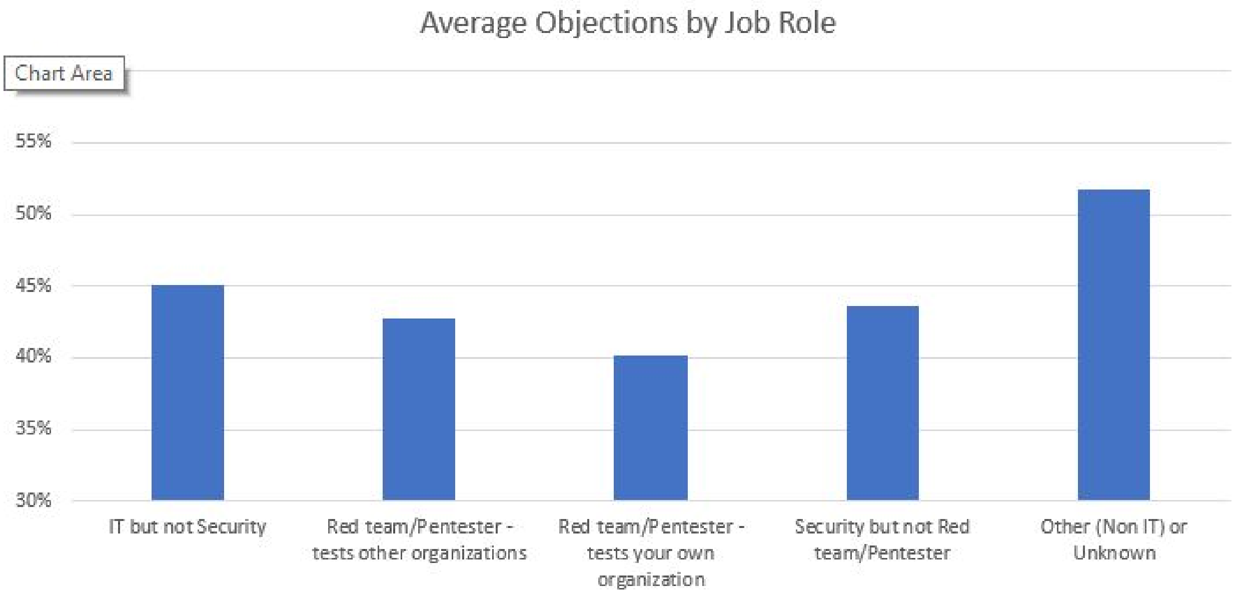
The next quantitative research methodology improvement will be to reach a curated standard n for the survey, which will include closer demographic tracking as well as baseline questions to help people self-identify. One potential error in our math is that women and underrepresented minorities are more likely to think of themselves as "not a real infosec professional" yet, and as a result, we may have skewed results from the exact populations we want to hear from. This requires collaboration with someone skilled in current survey design methods, and at least one good geographer/data scientist.

We welcome collaborators in this research, encourage further exploration of these topics, and look forward to a potential next iteration of this test, which could incorporate our learnings from these research results and focus in on the largest gaps between employee incentives and executive behavior.

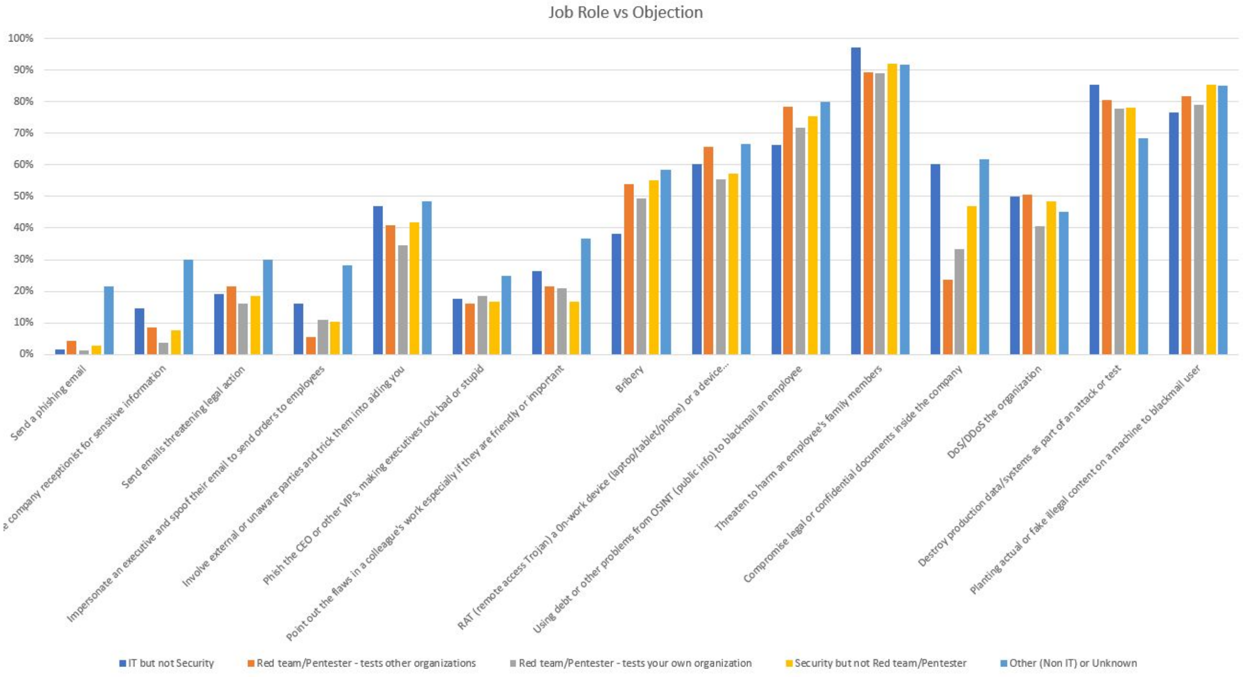
Author Biographies

Tarah Wheeler is an offensive security researcher, political scientist in the area of international conflict, and poker player. She is Cybersecurity Policy Fellow at New America as well as an information security industry senior executive. She is a cybersecurity expert for the Washington Post and a Foreign Policy contributor on cyberwarfare. @tarah

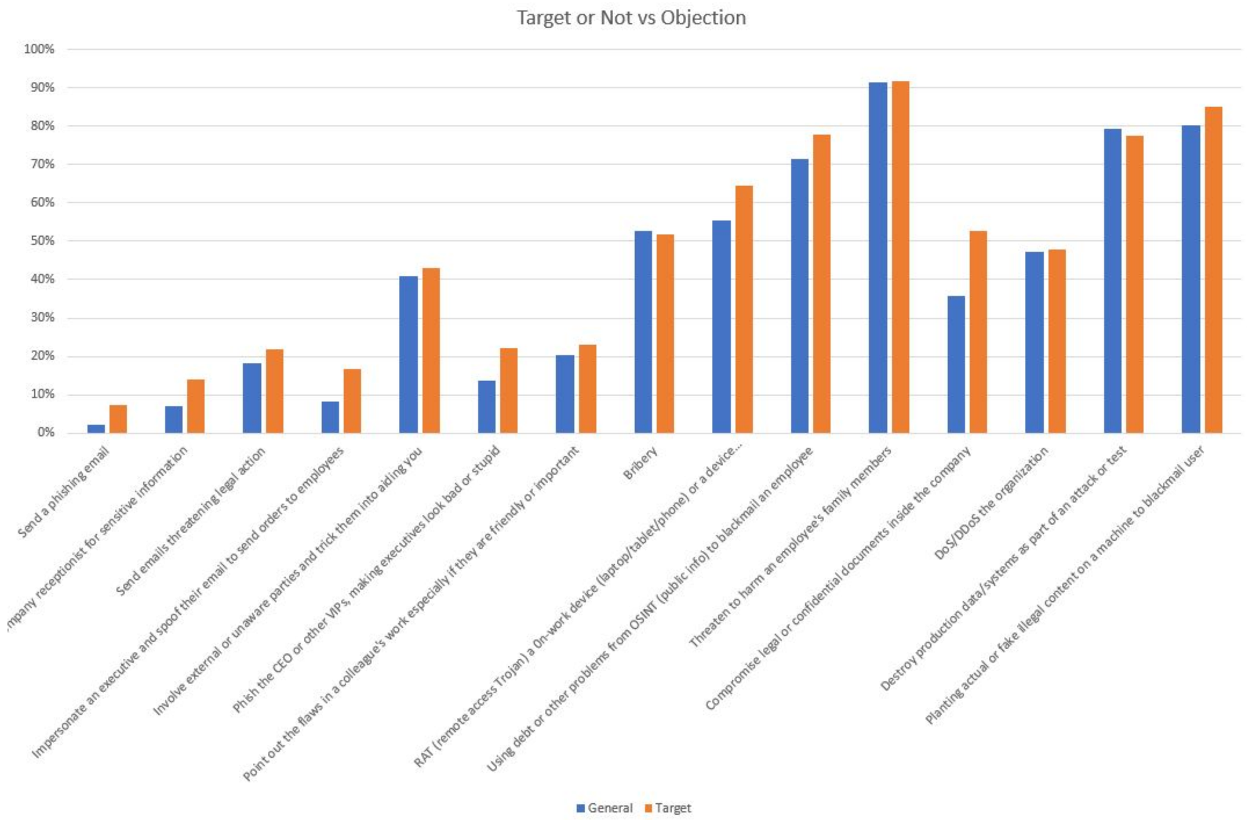
Roy Iversen is Director of Security Engineering & Operations at Fortalice Solutions, where he leads a team of security engineers and incident responders. Prior to joining Fortalice, Mr. Iversen served under the CISO as Director of Security Operations Division at the U.S. General Services Administration (GSA). @royiversen



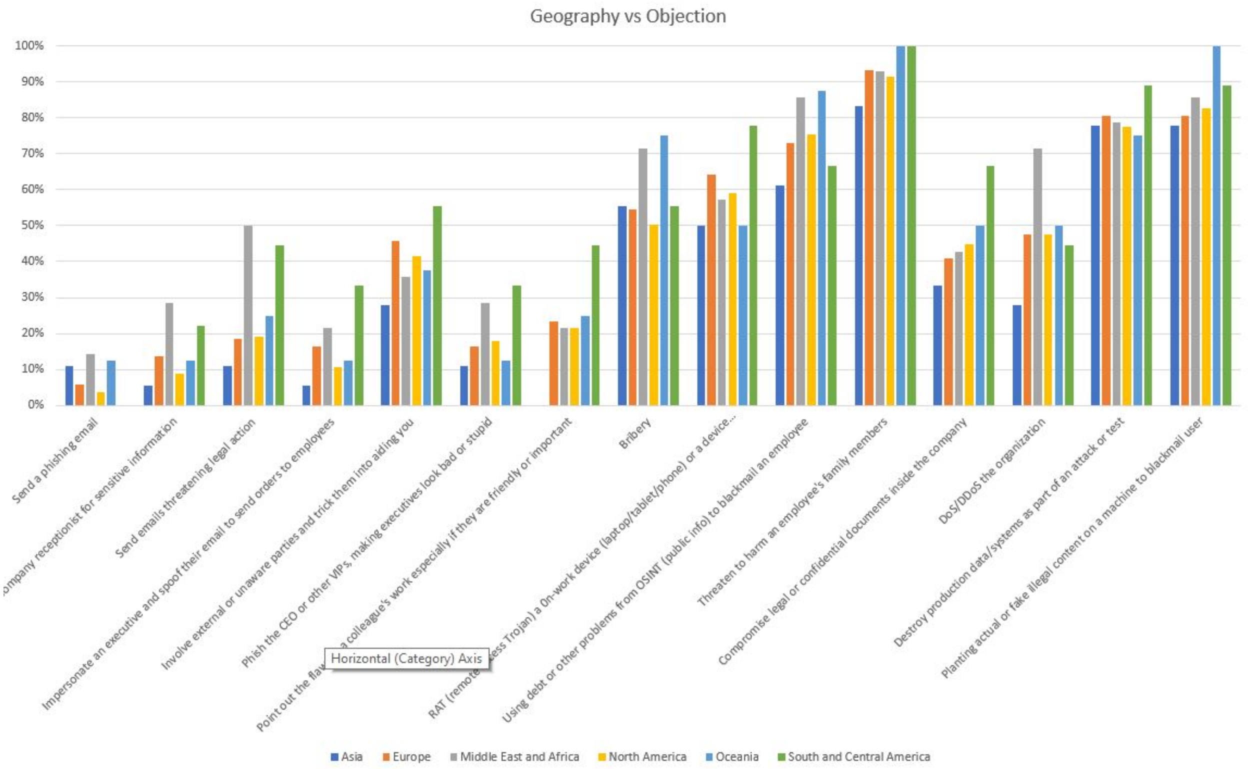
Above: Average objections to the tests - Other/Non IT objected to 13% more of the tests on average than internal red teamers.



Job Role vs what they object to



Those targeted are more likely to object than those just considering the scenario.


Geography vs Objection
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Send a phishing email
ompany receptionist for sensitive information
Send emails threatening legal action
Impersonate an executive and spoof their email to send orders to employees
Involve external or unaware parties and trick them into aiding you
Phish the CEO or other VIPs, making executives look bad or stupid
Point out the flaw a colleague's work especially if they are friendly or important
RAT (remote ess Trojan) a 0n-work device (laptop/tablet/phone) or a device...
Bribery
Using debt or other problems from OSINT (public info) to blackmail an employee
Threaten to harm an employee's family members
Compromise legal or confidential documents inside the company
DoS/DDoS the organization
Destroy production data/systems as part of an attack or test
Planting actual or fake illegal content on a machine to blackmail user
Horizontal (Category) Axis
Asia
Europe
Middle East and Africa
North America
Oceania
South and Central America