Be cool, Honey Bunny

Working Through Security Vulnerability Disclosure

the scenario

You represent a company.

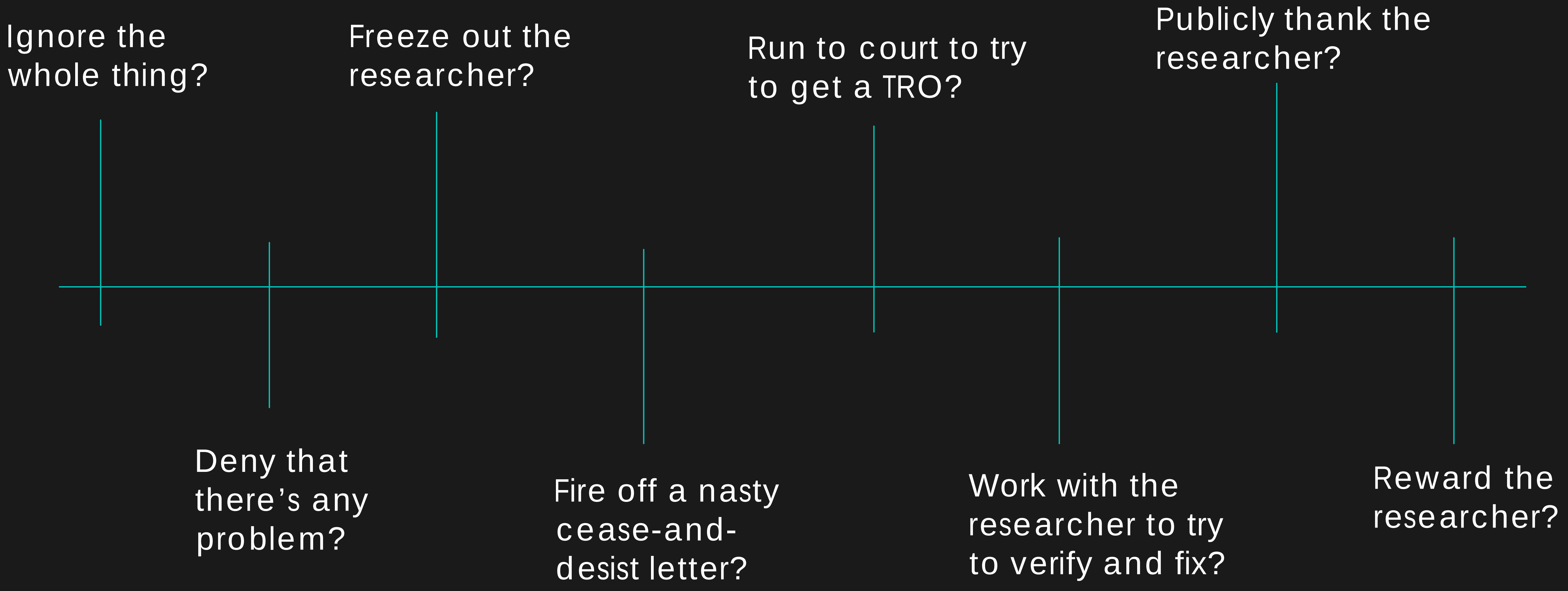
A researcher comes forward to tell your client that there's a massive security flaw in its flagship product.

The researcher intends to go public with this news.

the scenario

What do you do?

decisions, decisions



Ignore the whole thing?

Deny that there's any problem?

Freeze out the researcher?

Fire off a nasty cease-and-desist letter?

Run to court to try to get a TRO?

Work with the researcher to try to verify and fix?

Publicly thank the researcher?

Reward the researcher?

motivations

Researcher

Vendor

motivations / goals

Researcher

- Likely wants the problem fixed
- Likely wants to protect users
- Maybe looking for recognition

Vendor

motivations / goals

Researcher

- Likely wants the problem fixed
- Likely wants to protect users
- Maybe looking for recognition
- Maybe looking for money?

Vendor

motivations / goals

Researcher

- Likely wants the problem fixed
- Likely wants to protect users
- Maybe looking for recognition
- Maybe looking for money?

Vendor

- Should want to fix the problem
- Wants to keep users safe & happy
- Wants to avoid public humiliation
- Wants to avoid legal trouble

motivations / goals

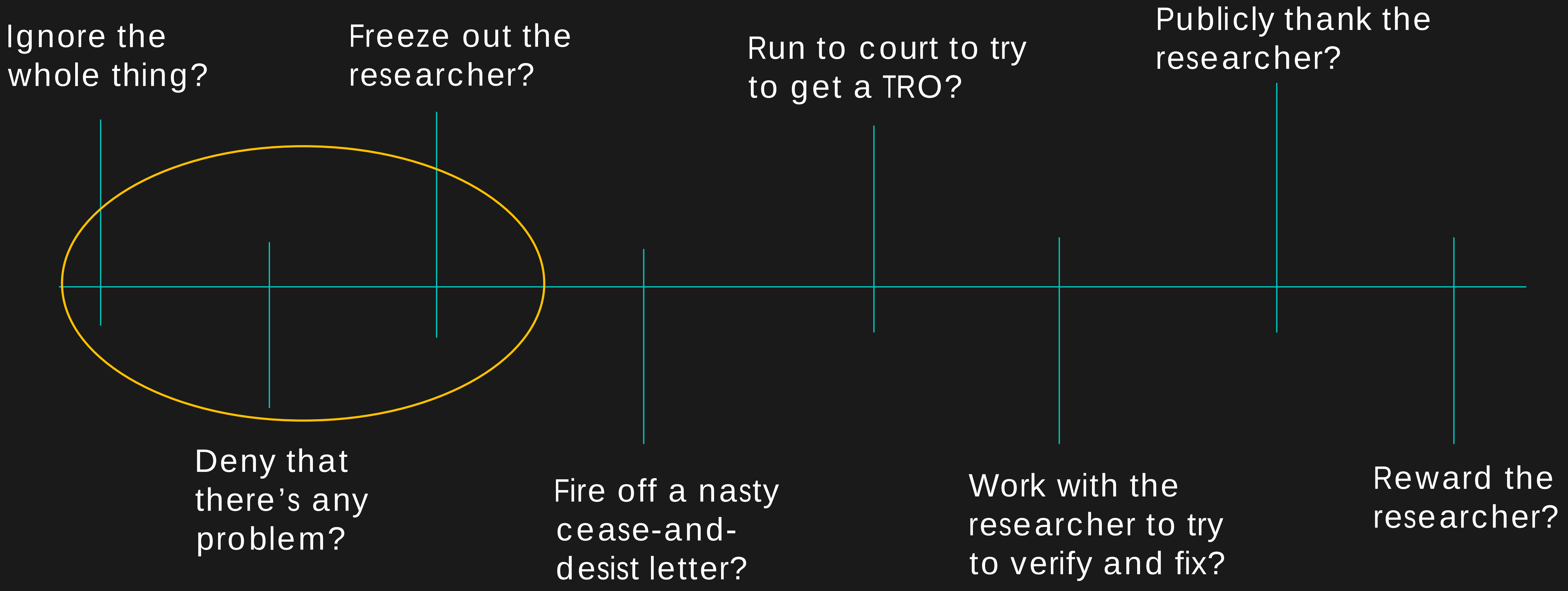
Researcher

- Likely wants the problem fixed
- Likely wants to protect users
- Maybe looking for recognition
- Maybe looking for money?

Vendor

- Should want to fix the problem
- Wants to keep users safe & happy
- Wants to avoid public humiliation
- Wants to avoid legal trouble
- Wants to keep the issue under wraps?
- Doesn't want to put resources toward the issue?

head-in-sand approach



Ignore the whole thing?

Deny that there's any problem?

Freeze out the researcher?

Fire off a nasty cease-and-desist letter?

Run to court to try to get a TRO?

Work with the researcher to try to verify and fix?

Publicly thank the researcher?

Reward the researcher?

head-in-sand approach

PROS

- Maybe nobody will notice
- Maybe a chance to fix on own timetable & terms
- Feeling of not being pressured by outsider
- Possibly can get a jump on the narrative

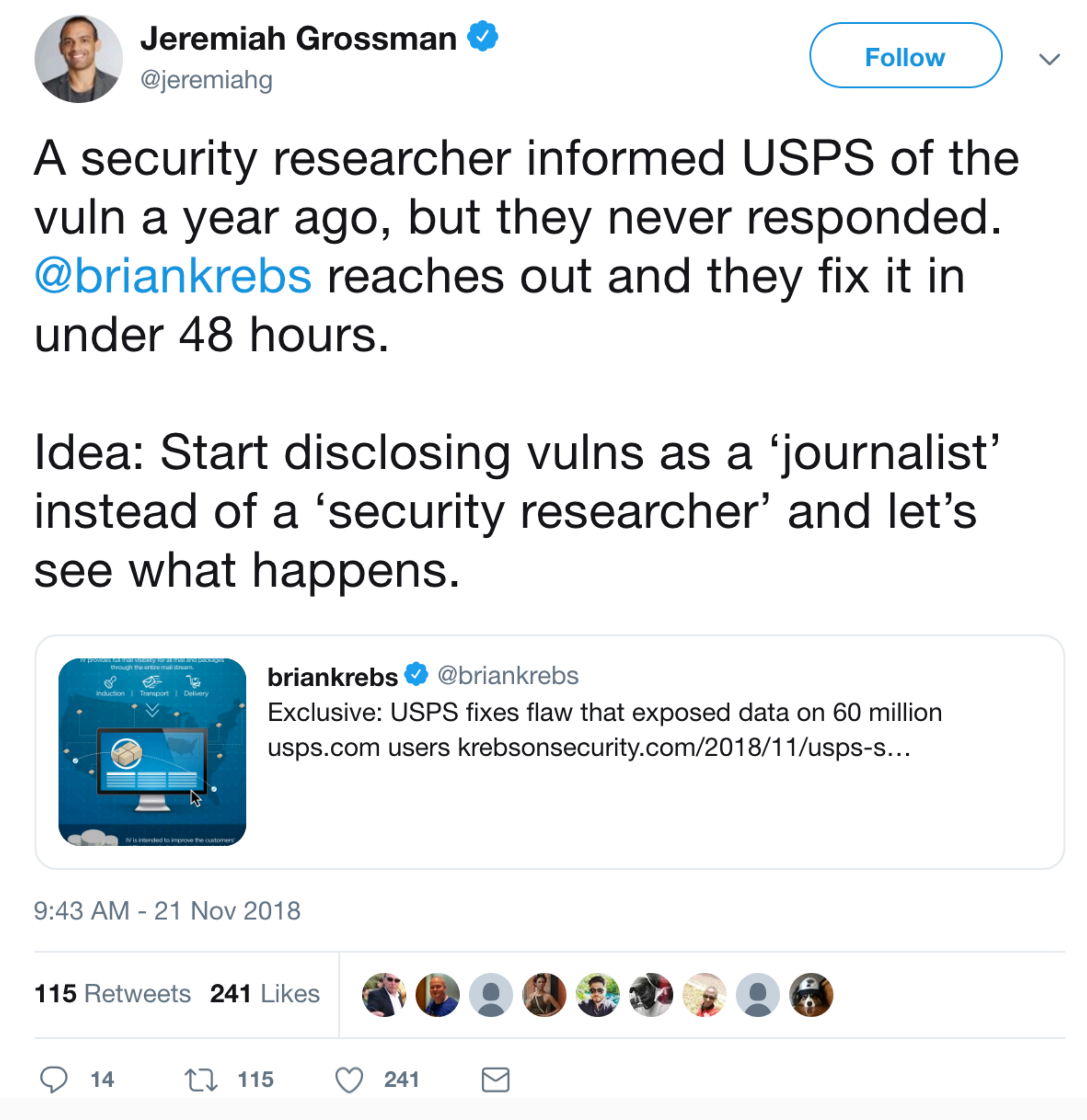
head-in-sand approach

PROS

- Maybe nobody will notice
- Maybe a chance to fix on own timetable & terms
- Feeling of not being pressured by outsider
- Possibly can get a jump on the narrative

CONS

- Likely to fix more slowly because no collaboration with researcher
- Researcher likely to go public anyway
- No input into researcher's narrative
- Researcher may publicly trash vendor



Jeremiah Grossman @jeremiahg

A security researcher informed USPS of the vuln a year ago, but they never responded. @briankrebs reaches out and they fix it in under 48 hours.

Idea: Start disclosing vulns as a ‘journalist’ instead of a ‘security researcher’ and let’s see what happens.

briankrebs @briankrebs

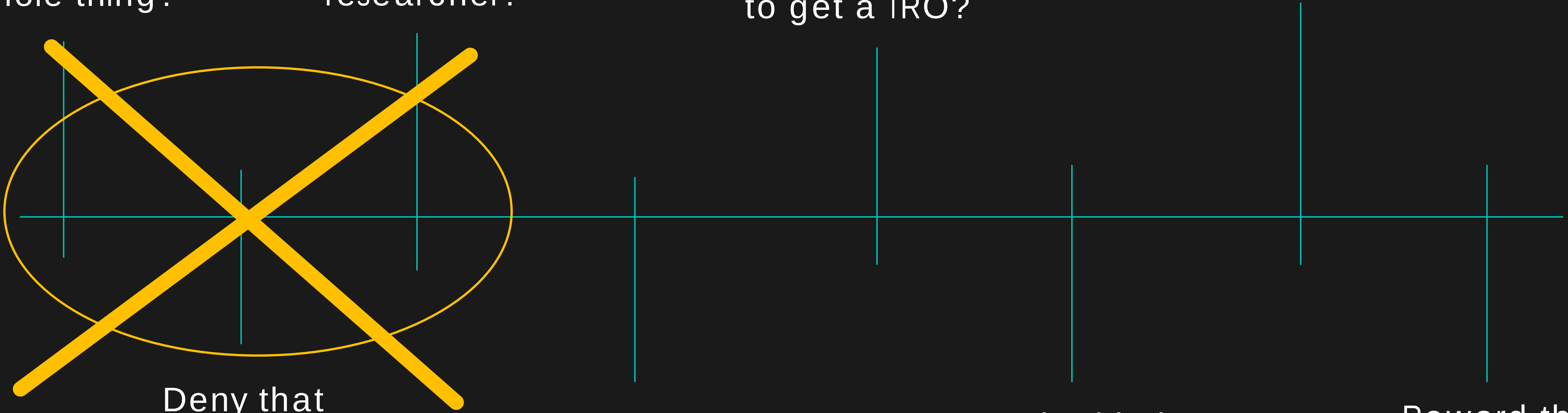
Exclusive: USPS fixes flaw that exposed data on 60 million usps.com users krebsonsecurity.com/2018/11/usps-s…

9:43 AM - 21 Nov 2018

115 Retweets **241** Likes

14 115 241

head-in-sand approach



Ignore the whole thing?

Deny that there's any problem?

Freeze out the researcher?

Fire off a nasty cease-and-desist letter?

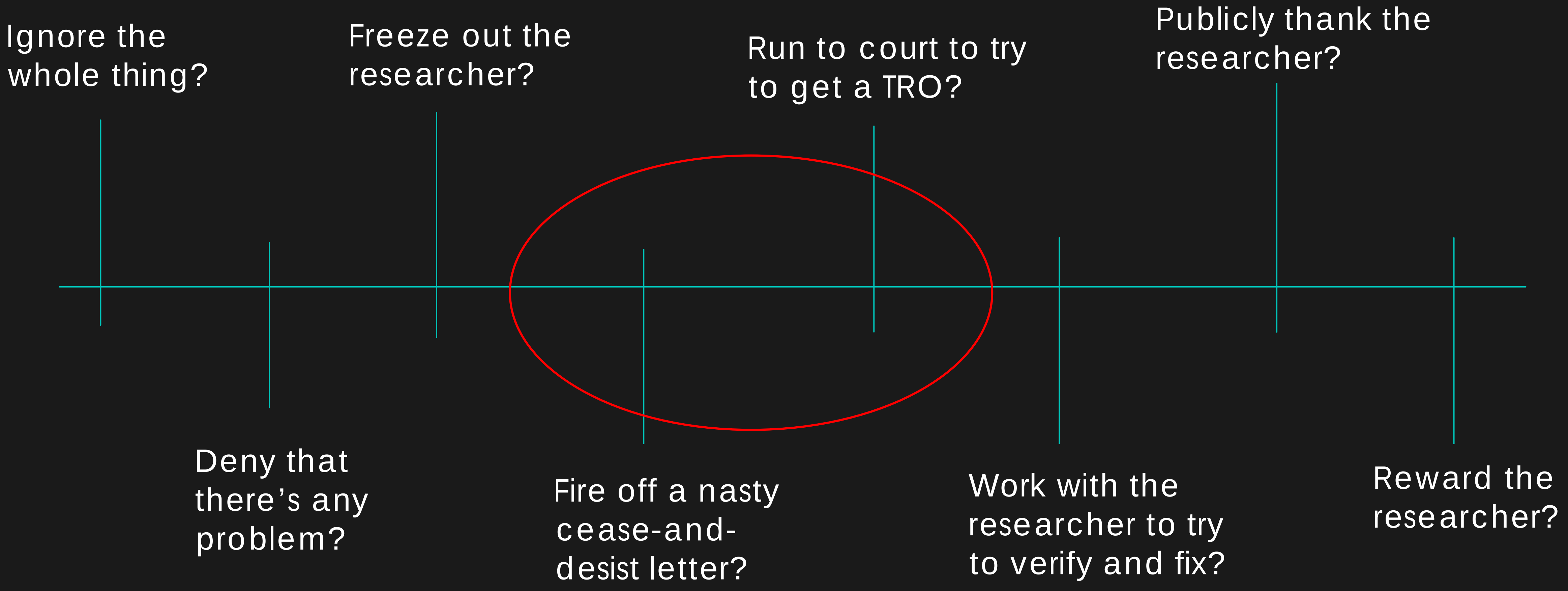
Run to court to try to get a TRO?

Work with the researcher to try to verify and fix?

Publicly thank the researcher?

Reward the researcher?

hostile approach



Ignore the whole thing?

Deny that there's any problem?

Freeze out the researcher?

Fire off a nasty cease-and-desist letter?

Run to court to try to get a TRO?

Work with the researcher to try to verify and fix?

Publicly thank the researcher?

Reward the researcher?

hostile approach

PROS

- You feel like you’re doing something
- The hope is generally to intimidate the researcher into silence, but….

hostile approach

PROS

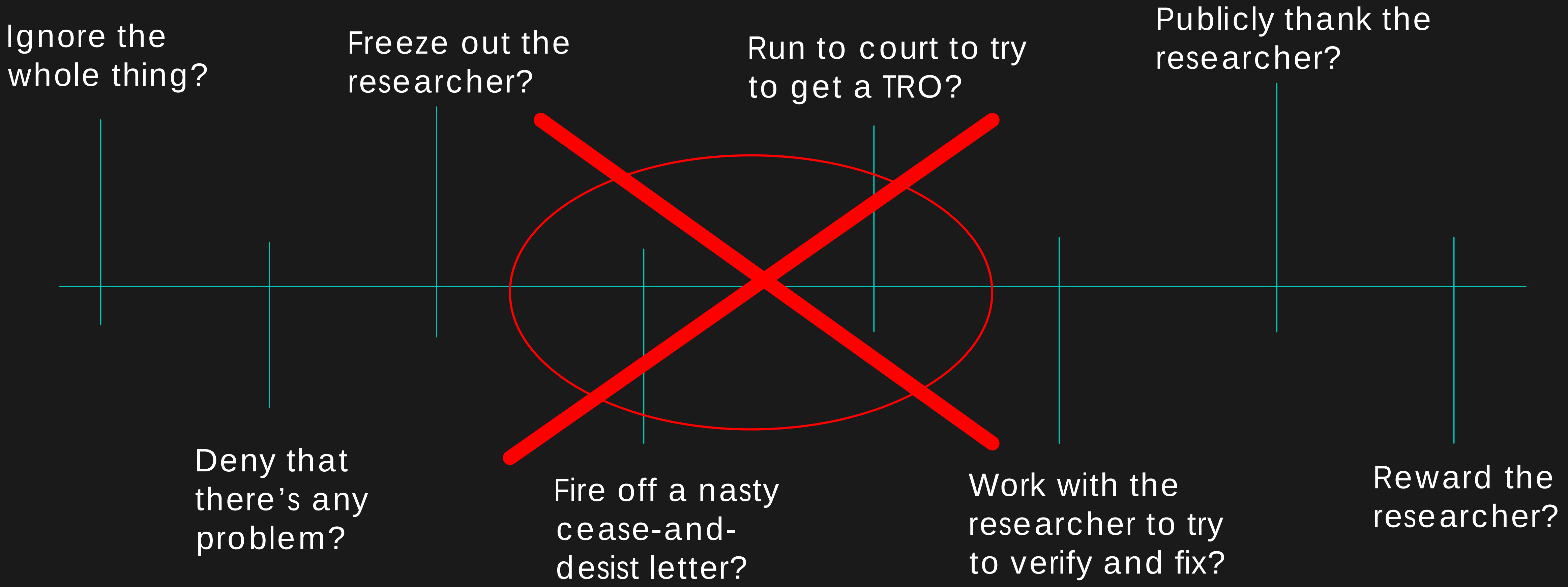
- You feel like you're doing something
- The hope is generally to intimidate the researcher into silence, but....

CONS

- Researcher may well go public anyway
- Any efforts to stop disclosure will probably have First Amendment problems
- Freak out users
- Attract regulatory attention
- Very public bad look

STREISAND EFFECT

hostile approach



Ignore the whole thing?

Deny that there’s any problem?

Freeze out the researcher?

Fire off a nasty cease-and-desist letter?

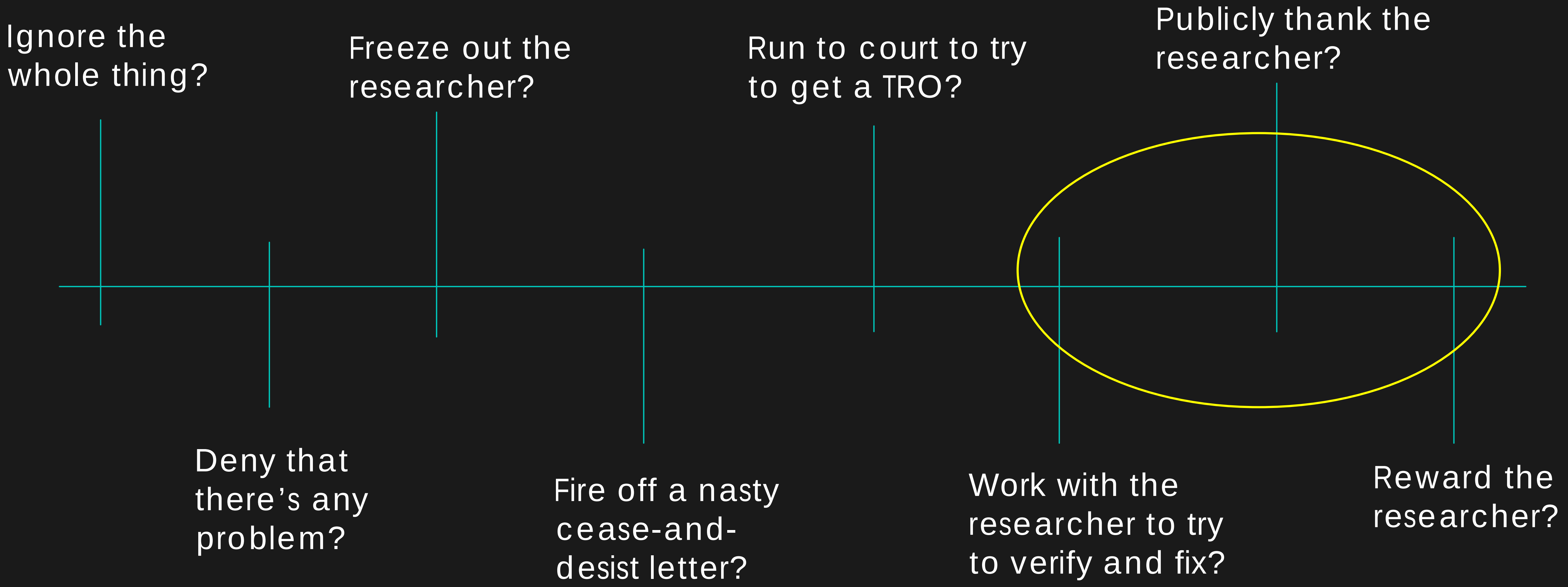
Run to court to try to get a TRO?

Work with the researcher to try to verify and fix?

Publicly thank the researcher?

Reward the researcher?

collaborative approach



Ignore the whole thing?

Deny that there's any problem?

Freeze out the researcher?

Fire off a nasty cease-and-desist letter?

Run to court to try to get a TRO?

Work with the researcher to try to verify and fix?

Publicly thank the researcher?

Reward the researcher?

Be cool, Honey Bunny

collaborative approach

PROS

- Have a new ally
- Likely can fix the problem faster than if doing it alone
- Build goodwill
- Avoid Streisand Effect / PR disaster
- Thoughtful and careful

collaborative approach

PROS

- Have a new ally
- Likely can fix the problem faster than if doing it alone
- Build goodwill
- Avoid Streisand Effect / PR disaster
- Thoughtful and careful

CONS

- Vendor might have to fix faster than they'd ideally like to
- Might have to put resources toward fix they'd rather use elsewhere

THE COLLABORATIVE APPROACH

the key

good communication among the right people

good communication

- Frequent
- Detailed
- De-escalate anger / mistrust
- Focus on solving the problem

the right people

- Not customer service, lawyers, or PR
- Technical
- “This is just a thing we need to fix.”
- In a position to understand the nitty gritty

practical considerations

- Can the vendor validate the issue?
- How serious is it?
- Is it fixable?
- How long will it take to fix?
- Who else should know?
- Public messaging

complications

Language challenges

Culture clashes

Work needed

Different goals

legal issue-spotting

- Breach of contract
  - Consumer Review Fairness Act
    45 U.S.C. § 45b
- Computer Fraud and Abuse Act / state equivalents
  - C.R.S. §§ 18-5.5-101 & 102
- Copyright / Digital Millennium Copyright Act
- Anti-competition law
- Defamation / trade libel

other legal considerations

Data breach/notification?

Lawsuits?

Regulatory issues?

thanking the researcher

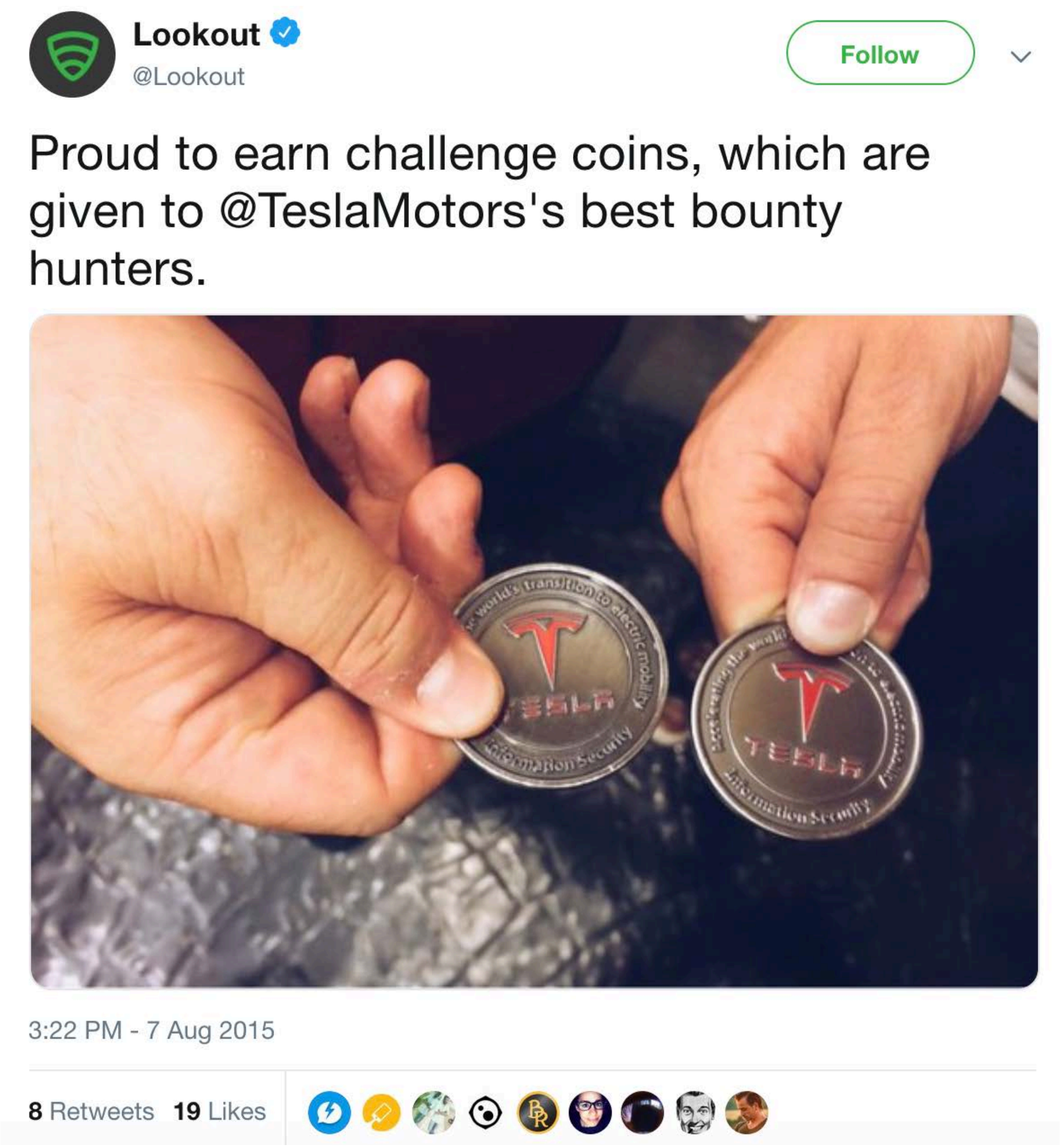
Public recognition

Bug bounty

(HackerOne, Bugcrowd, Synack)

Tokens of gratitude (*e.g.*, challenge coins)

Consider working together in the future

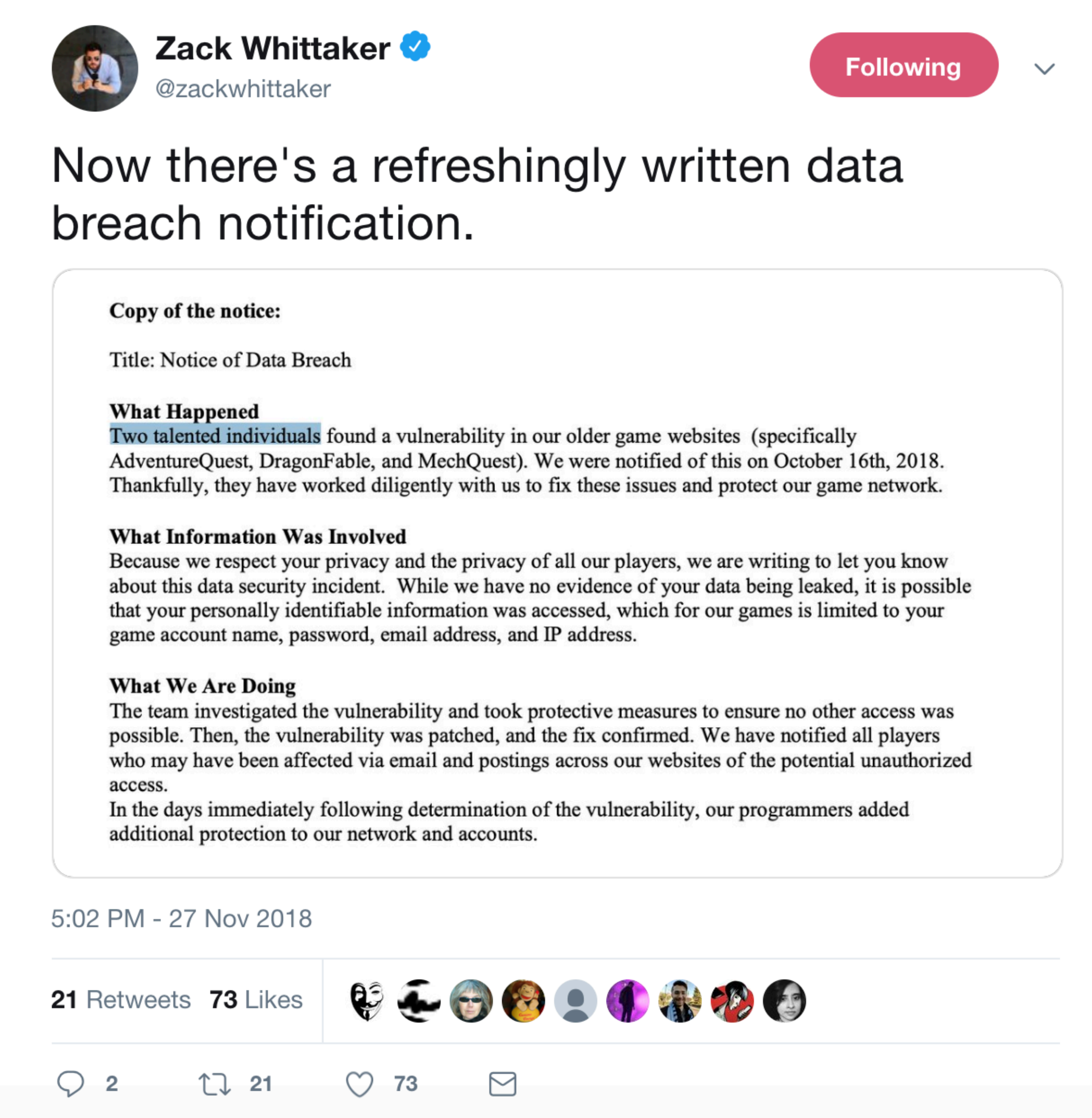


Lookout
@Lookout

Proud to earn challenge coins, which are given to @TeslaMotors's best bounty hunters.

3:22 PM - 7 Aug 2015

8 Retweets 19 Likes



Zack Whittaker
@zackwhittaker

Now there's a refreshingly written data breach notification.

Copy of the notice:

Title: Notice of Data Breach

What Happened
Two talented individuals found a vulnerability in our older game websites (specifically AdventureQuest, DragonFable, and MechQuest). We were notified of this on October 16th, 2018. Thankfully, they have worked diligently with us to fix these issues and protect our game network.

What Information Was Involved
Because we respect your privacy and the privacy of all our players, we are writing to let you know about this data security incident. While we have no evidence of your data being leaked, it is possible that your personally identifiable information was accessed, which for our games is limited to your game account name, password, email address, and IP address.

What We Are Doing
The team investigated the vulnerability and took protective measures to ensure no other access was possible. Then, the vulnerability was patched, and the fix confirmed. We have notified all players who may have been affected via email and postings across our websites of the potential unauthorized access.
In the days immediately following determination of the vulnerability, our programmers added additional protection to our network and accounts.

5:02 PM - 27 Nov 2018

21 Retweets **73** Likes

how to better handle security issues

In-house security team

Pen testing

Vulnerability reporting process

- ISO/IEC 29147
- (vuln disclosure)

- ISO/IEC 30111
- (vuln handling processes)

Bug bounty

A mix or all

discussion?