

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: HUM-W02

The Rise of the Cyber Security Culture Hacker

Dr. Christine Izuakor

Senior Manager – Global Security Strategy and Awareness
United Airlines

#RSAC



I engage people.



I will look for you. I will find you.

I will **TRAIN** you.



**Labeling humans as the weakest
link, is a lazy excuse.**



What is a Cyber “Culture Hacker”?



What is a hacker?

A person who uses clever tips or techniques for doing or improving something.

What is culture?

The system of attitudes, values, goals, and practices people follow.

A person who applies clever and creative techniques to transform peoples system of **attitudes, values, goals, and practices** when it comes to cybersecurity.



A large tree stands in a field of green grass under a sky filled with grey and white clouds. The tree's canopy is split: the left side is bare with many thin, intricate branches, while the right side is lush and green with dense foliage.

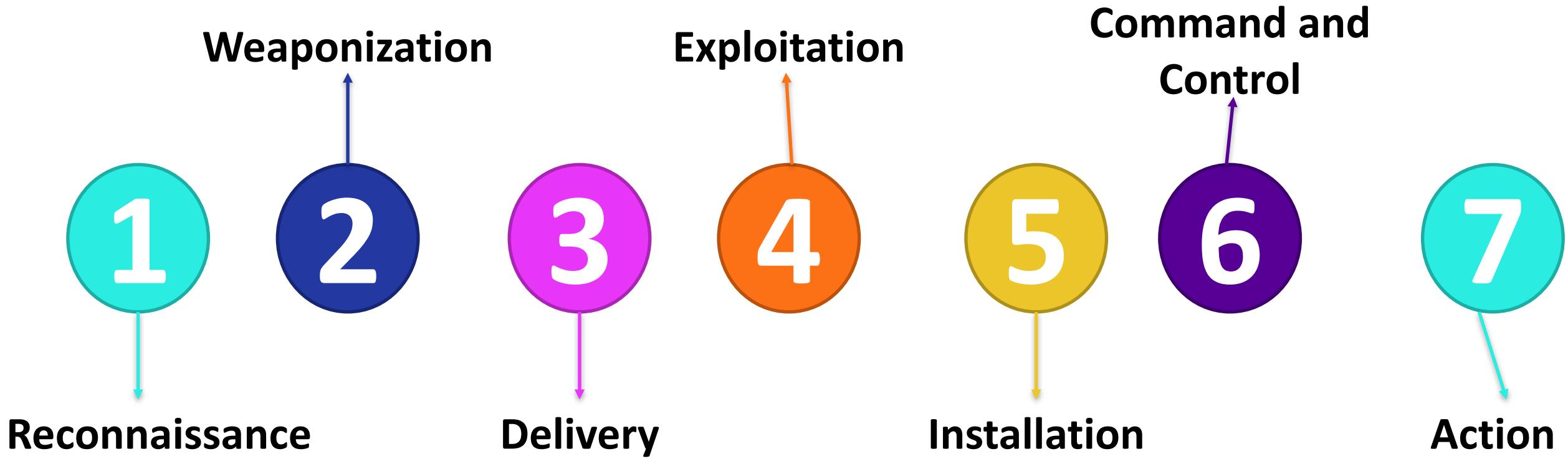
Disengagement

Engagement

Creativity is critical.



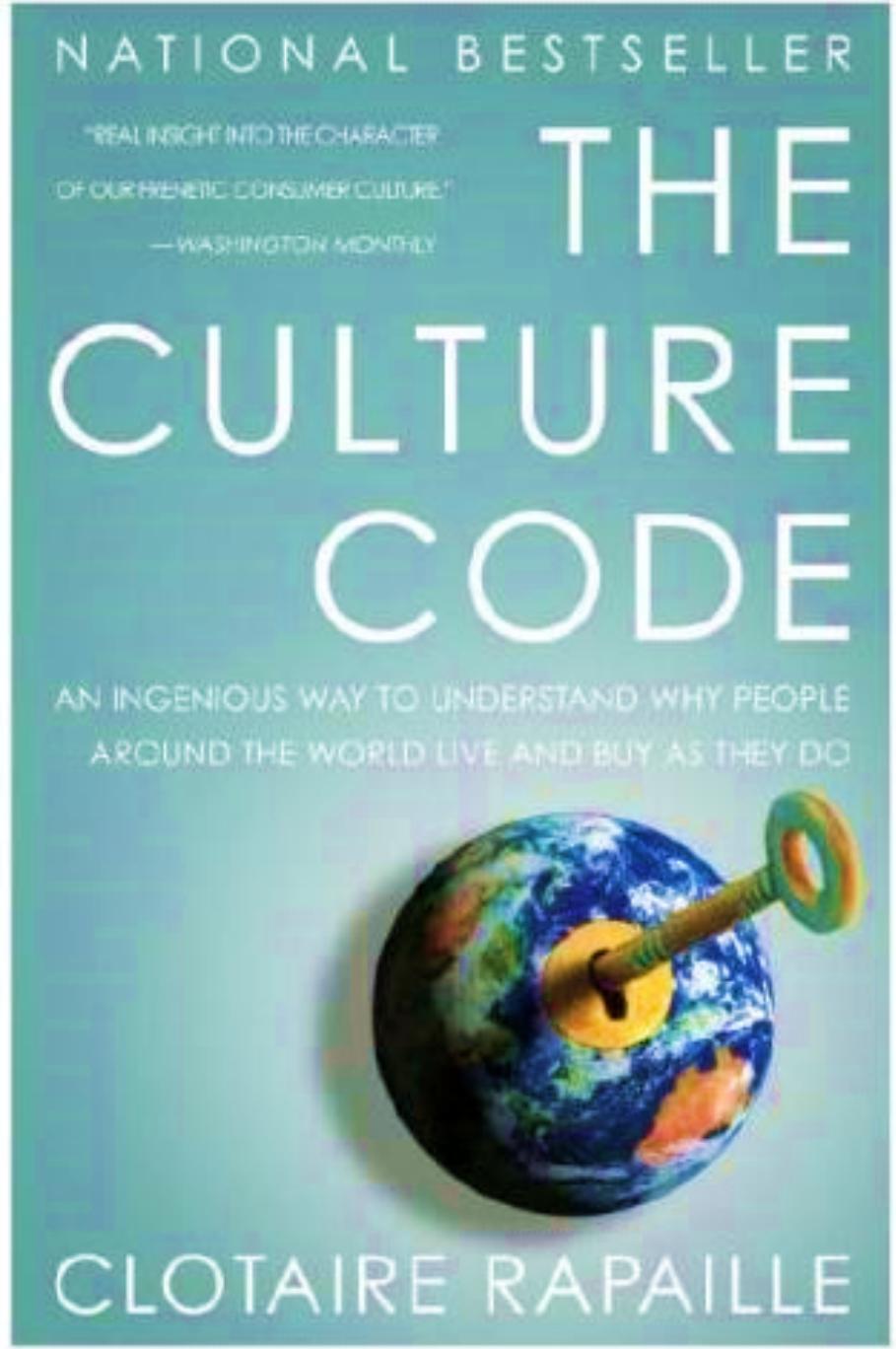
Hacking culture is a lot like hacking systems.



RSA® Conference 2019

Reconnaissance

Understand your target and how they operate.



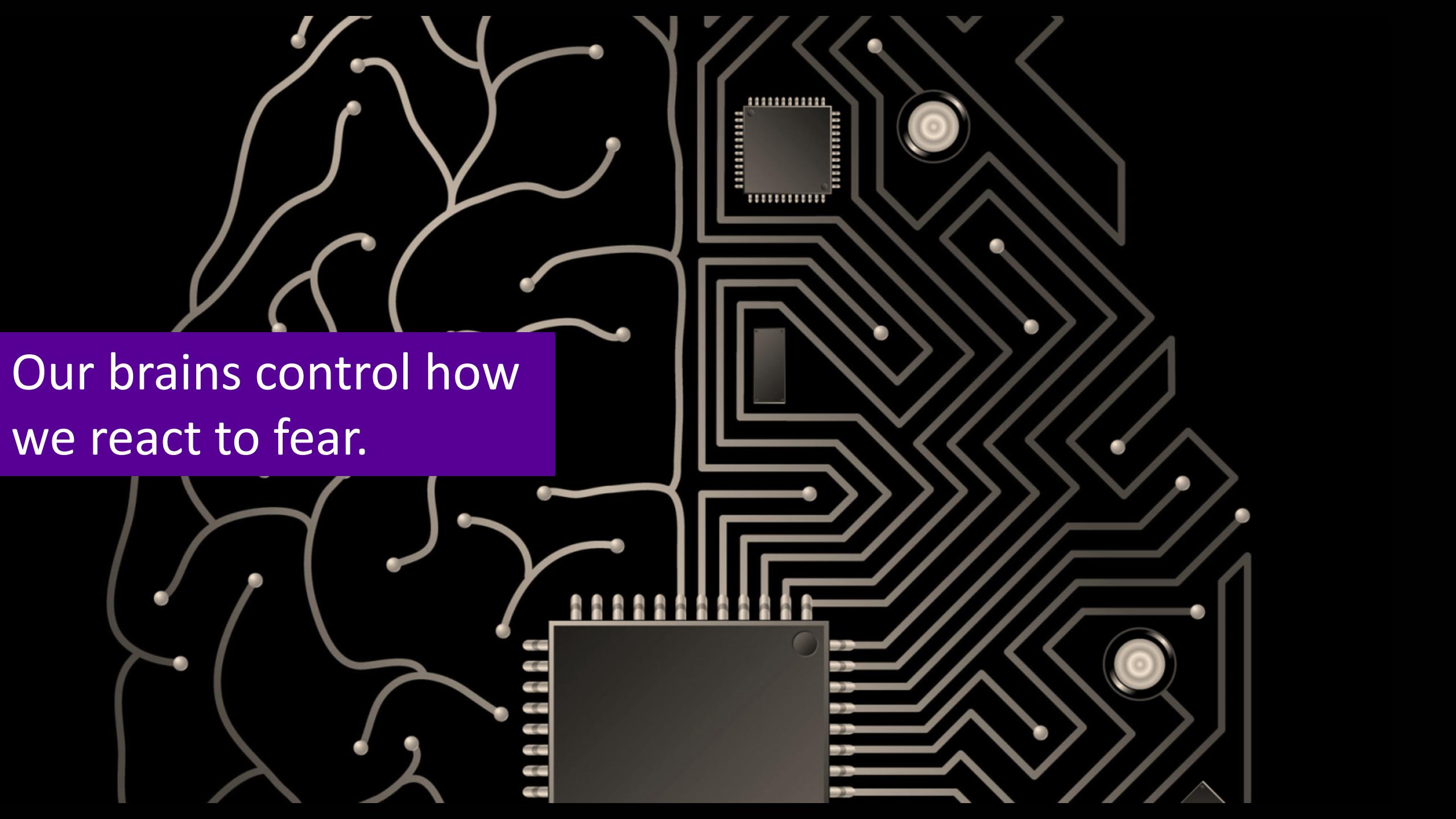
**What is the culture code
for cybersecurity?**

The culture code for cybersecurity is...

FEAR!







Our brains control how
we react to fear.

Productive reaction to fear.

Face it.

Explore it.

Appreciate it.

Respond to it.

In reality, we are lid flippers.

Face It.

~~Explore it.~~

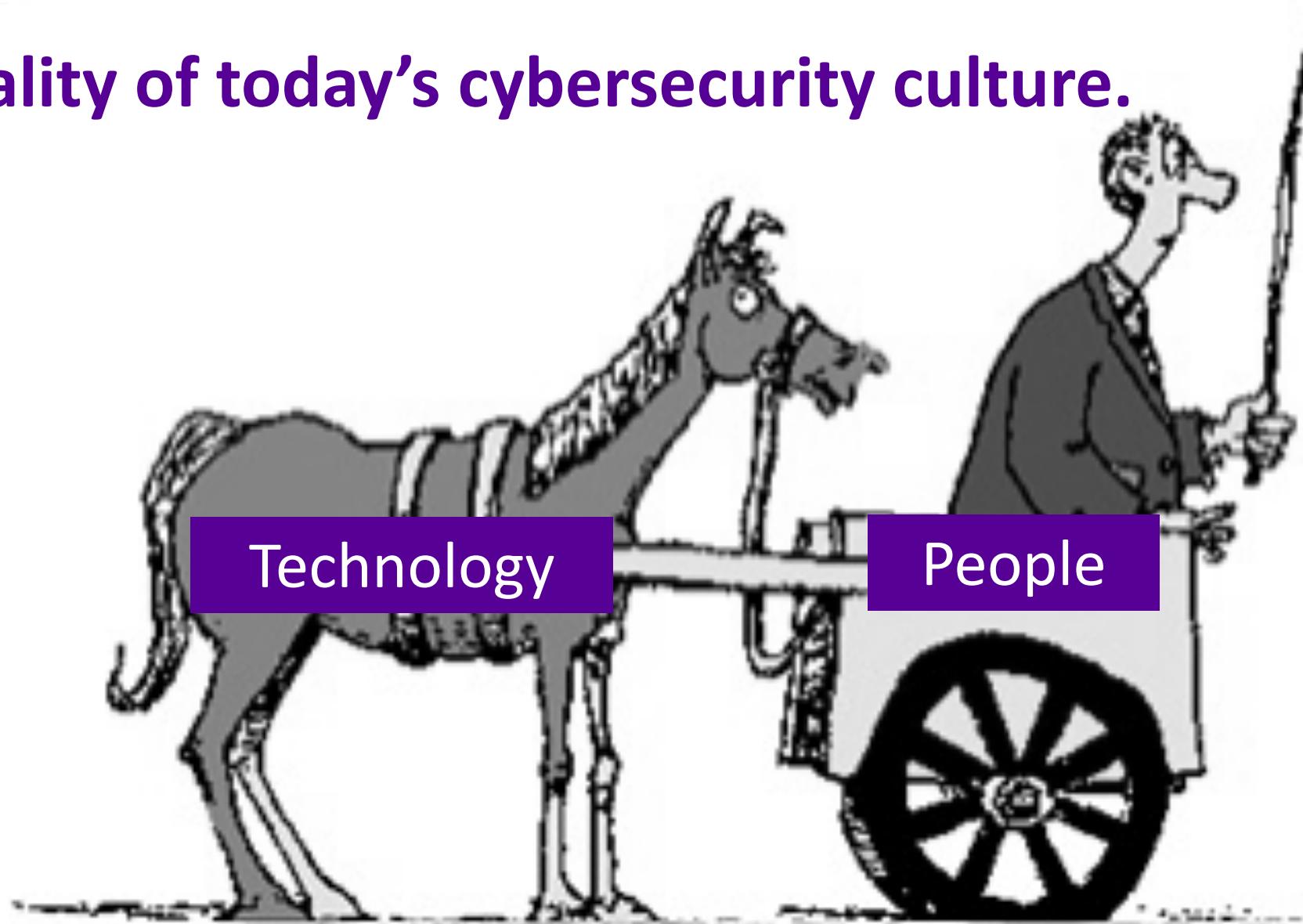
~~Appreciate it.~~

Respond to it.



with Technology!

The reality of today's cybersecurity culture.



Technology should not be driving decisions that impact people. People should be driving technology decisions.



Mass fear is not a technology
problem, it's a people problem.

A close-up photograph of a woman's face. Her lips are painted a vibrant pink. She is holding her index finger to her upper lip, with the word "Shhh..." written in black cursive ink. The background is a solid reddish-pink color.

Attackers know we operate this way,
which is why they target people first.



What's your culture code?

With all attacks there is an end goal...

Malicious
hackers
steal
DATA.



Culture
hackers
steal
FEAR.

Weaponization

Leverage discovered vulnerabilities to craft attack methods.

What weapons do we need?

Strategy

Brand

People

Technology

Process

Weapon 1: Build a strong brand.

Your brand is a promise.



Protect
Our Airline

Relatable, Realistic, and Relevant

Weapon 2: Empower people to live your cyber brand.



Find a way to demystify cybersecurity and create understanding for everyday users.



- ✓ Joint cyber security mission



- ✓ Threats are real, not theory



- ✓ Understand your role



- ✓ We are here to help

Find creative ways to build a strong and diverse cybersecurity talent pipeline.



- ✓ Internship and rotation programs
- ✓ Entry level jobs & transferable skills
- ✓ HR awareness
- ✓ Non-profit partnerships
- ✓ Scholarships
- ✓ Mentoring
- ✓ Next generation awareness events
- ✓ Barriers to entry analysis

Attracting cyber talent is only half the battle.



RSA®Conference2019

Engagement!

Delivery and Exploration

Get your weapons to your target and engage them!

Deliver your weapons and use them to engage people.

Identify available delivery channels.

Intranet Website

Newsletters

Posters

Infographics

NCSAM

Cyber Briefings

SWAG

Awareness Campaigns

Roadshows

Training & Education

Phishing Programs

Low

Level of effort

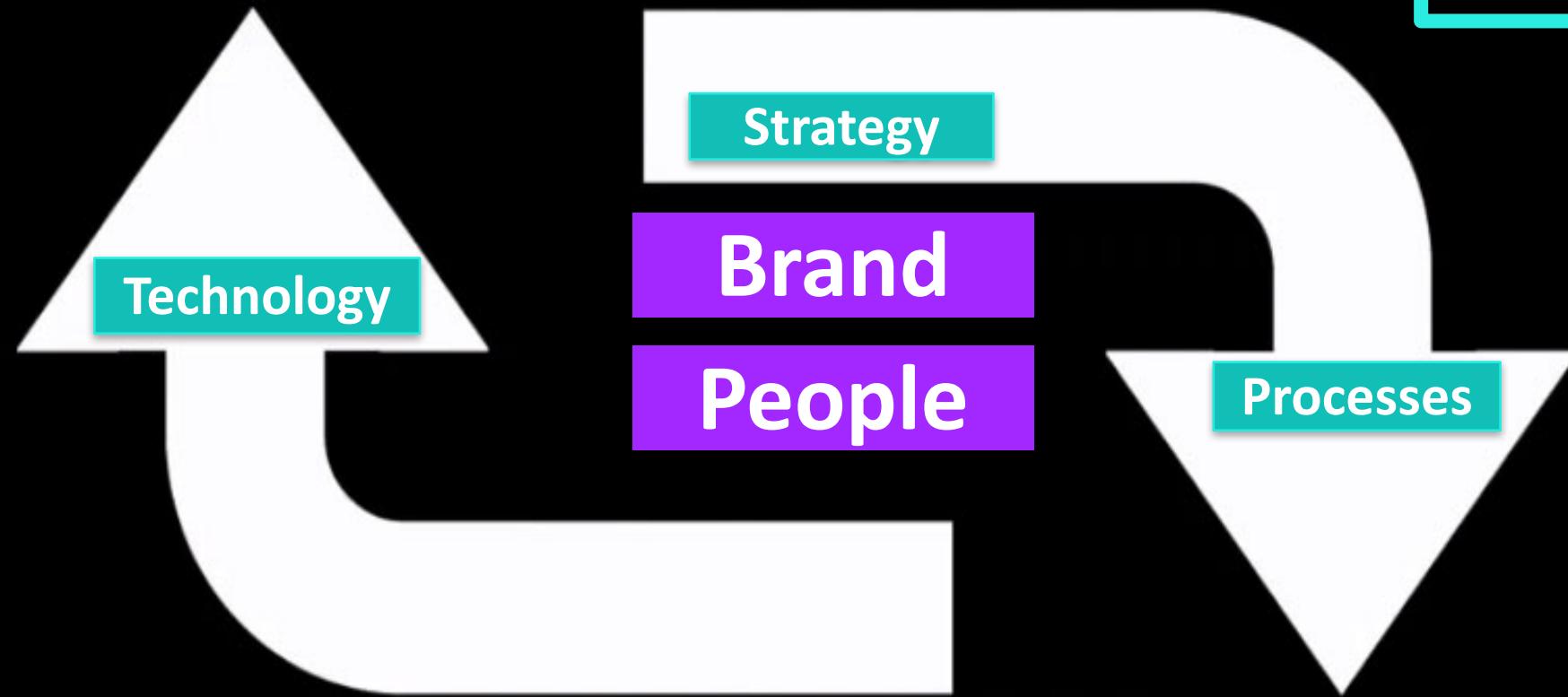
High

RSA® Conference 2019

Installation

Embed your weapons on the target.

Embed cybersecurity into your DNA.



Consistency Toolkit:

- Demystification framework
- Delivery channels

Consistency is key.

Command and Control

Access channels for remote control of targets.

**Enable people
(ambassadors) to do the
right thing, even when
you aren't there.**



Action on objectives

Achieve the objective of the attack.

The final mission is to steal fear.



Reward heroes for doing the right thing, especially when you aren't there. It reinforces everything.

RSA® Conference 2019

Next steps

Start or continue hacking your own cyber security culture!

Take action!

This is your playbook for reducing fear through culture hacking.



1

Reconnaissance

2

Weaponize

3

Deliver

4

Engage

5

Installation

6

Command and control

7

Action



- What's your current cyber culture?
- Who are key players?
- What vulnerabilities exist in relation to people?

- What's your brand? Is it Relevant, Realistic, and Relatable?
- Use the demystifying framework to create a story relevant to your company.
- Get creative with attracting and engaging cyber talent.

- What existing channels can you use to get your brand and message out?

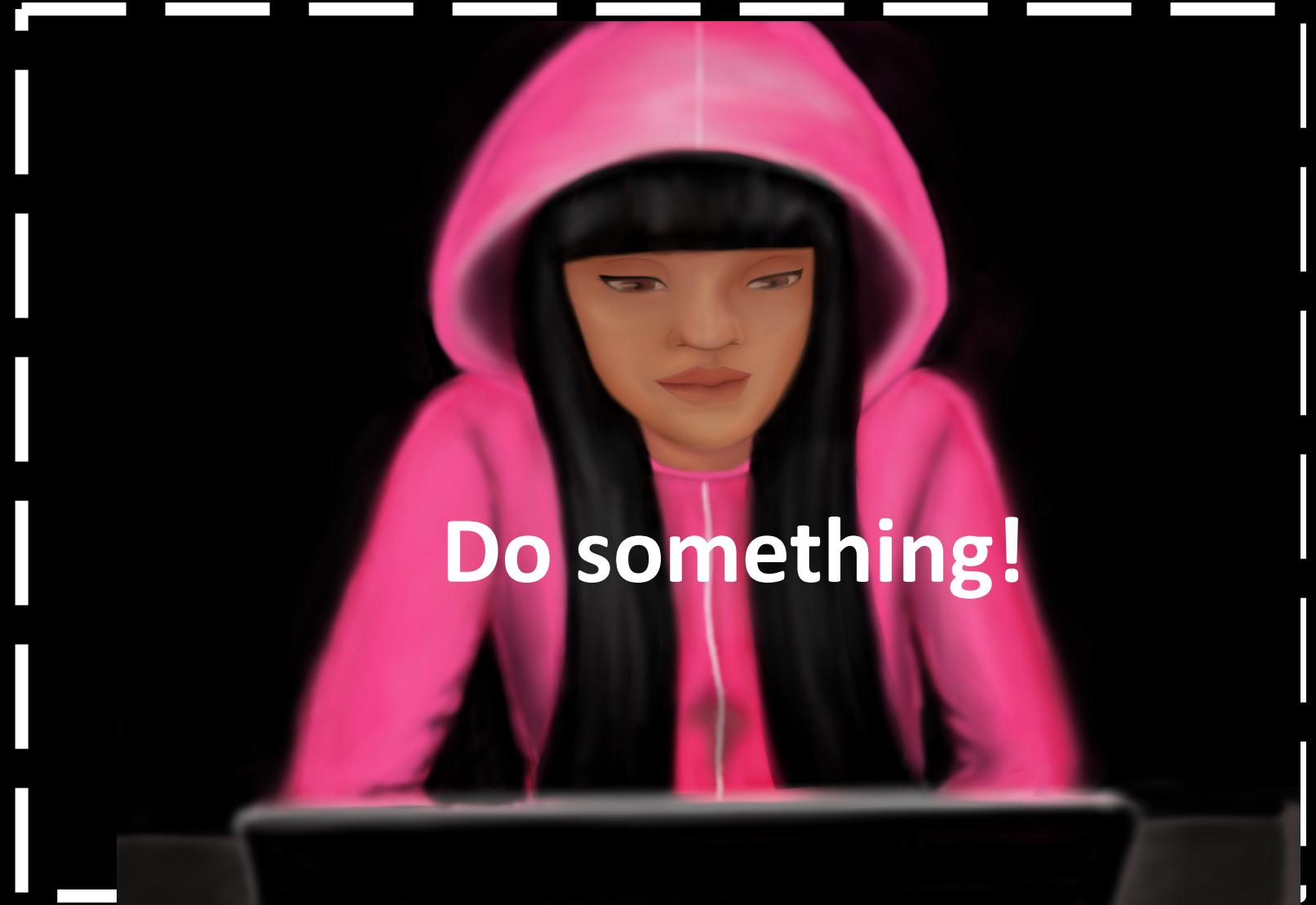
- How can you make what you're delivering fun?
- Get creative in how you leverage each channel to inspire people to think differently, take action, and more.

- Embed cyber security into the DNA of the organization and environment through consistency.
- How can you remind people on an ongoing basis?

- How can you empower people to engage even when your security team isn't around?
- Who are the hidden supporters you can count on to advocate?

- You came to steal fear and if you made it to this point, you probably already have. Find creative ways to reward people and measure your progress.

Cyber culture hacking doesn't just apply to companies.



Do something!

Young girls and minorities can't be what they can't see.

Thank you for joining me!



christineizuakor.com



linkedin.com/in/christineizuakor



Christine.Izuakor@gmail.com