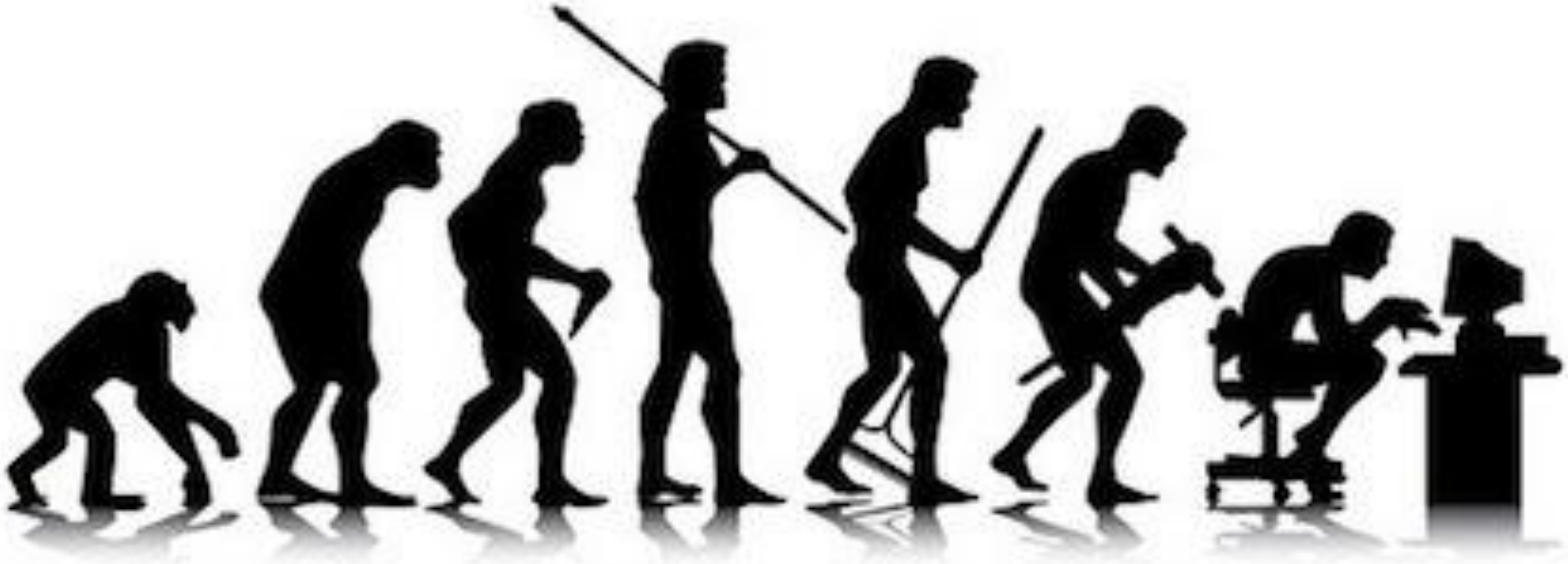
How to Build
Efficient Security Awareness Programs

That Don’t Suck

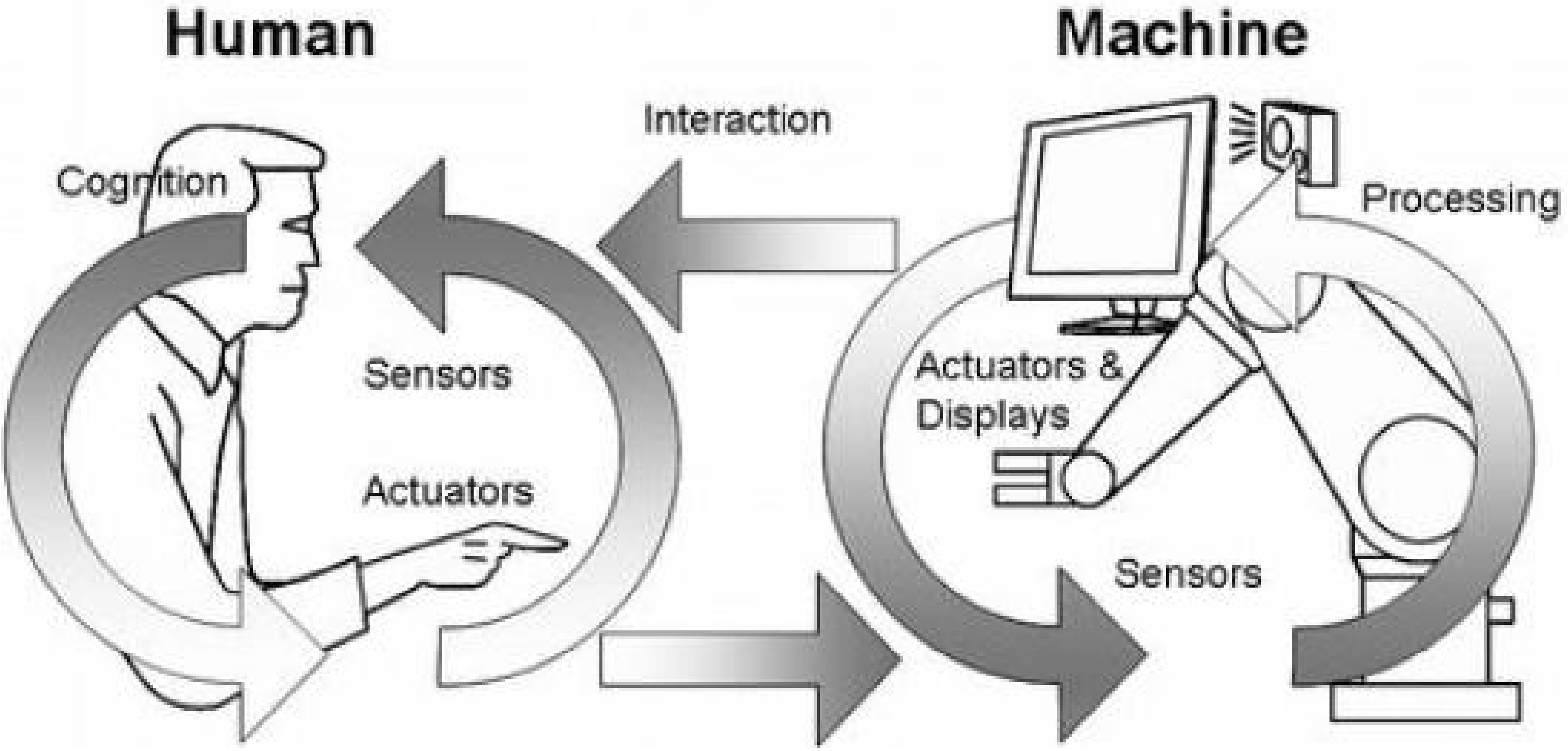
Vlad Styran
CISSP CISA OSCP
Berezha Security



YOU_HAVE
BEEN_HACKED

password123

7eh_vveakest_l1nque!1

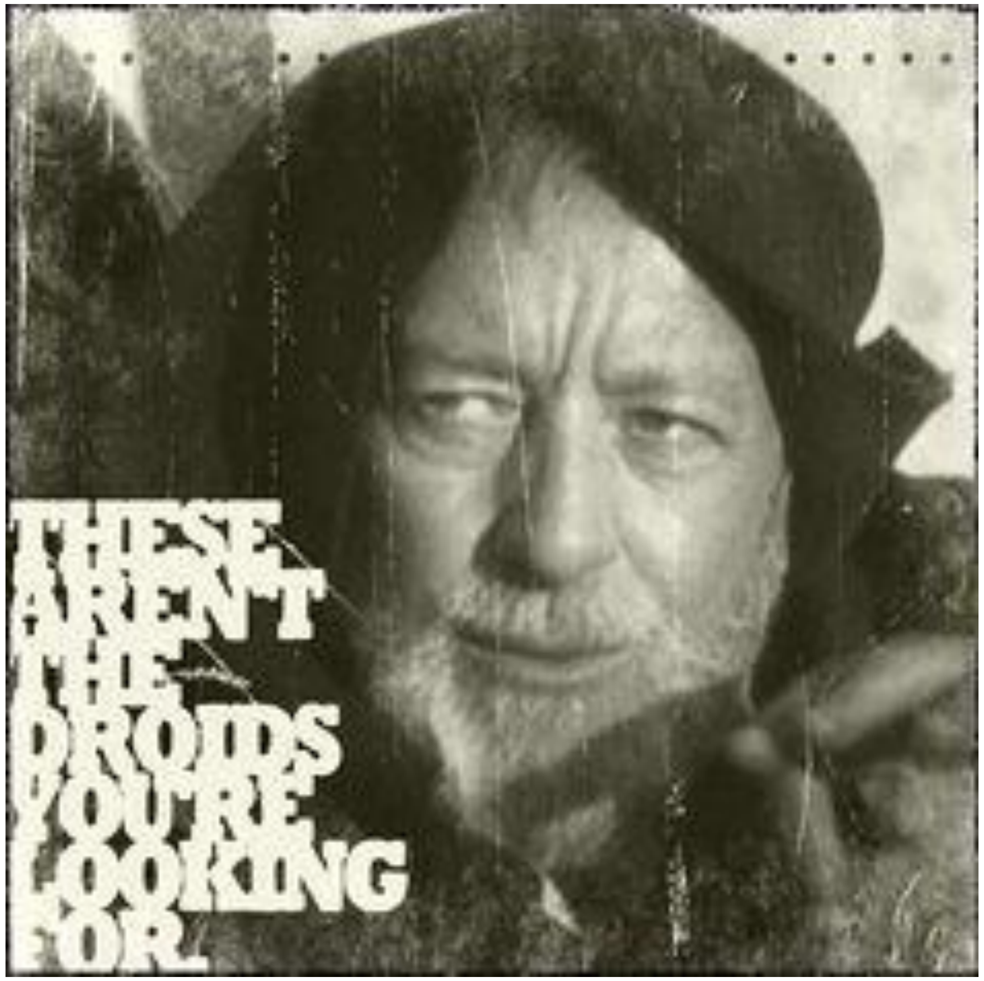

Human
Machine
Interaction
Cognition
Sensors
Actuators
Processing
Actuators &
Displays
Sensors

Social Engineering

Hi-tech & lo-tech human hacking

Influence principles

- Reciprocity
- Commitment
- Social proof
- Authority
- Liking
- Scarcity



Anti- Social Engineering

“Social engineering is cheating.”

– A CISO I once met.

What next?

Raise Awareness

Stop trying to fix human behavior with tech only

Give people responsibility

(back)

Security isn’t always
a business problem,
but it’s always
a human problem

The Tools

Fear

Incentives

Habits

Fear

The key to humanity’s survival

Teaches us to deal with threats

“Dumps” precursors of dangerous events

Moar Fear

We need to be told what to be afraid of

Overdose leads to phobias and disorders

Reasonable amount helps to learn

Memory needs refreshing

Social Incentives

Competition:
getting ahead of others

Belonging:
getting along with others

Social Incentives

Competition:
getting ahead of others

Belonging:
getting along with others

Habits

1. Trigger
2. Routine
3. Reward
4. Repeat

Habits

1. Trigger
2. Routine
3. Reward
4. Repeat

You receive an **email** with an **urgent** request to provide **confidential data**.

The **pizza delivery guy** is **staring at you** while holding a huge pile of pizza boxes at your **office door**.

An **"old schoolmate"** you just met in the street is **asking you** about the **specifics of your current job**.

You receive a **call** from a person that introduces themselves as the **CEO’s executive assistant** and asks you to **confirm the receipt** of their previous **email** and open its **attachment**.

An **attractive, likable human** is asking you to take part in an interview and is going to compensate that with a shiny new **USB drive** (in hope you insert it into your **working PC** later).

Attack methods: phishing, impersonation, elicitation, phone pretexting, software exploits, baiting…

Influence principles: scarcity, reciprocity, social proof, authority, liking…

Security context: anything of personal or business value – privacy, access, trust, confidential data…

Type of attack

+

Influence principle

⊂

Security context

=

PIERCE BROSNAN
I.T.
YOUR LIFE IS NOT SECURE.
the REAL HUSTLE
TIGER TEAM
MR. ROBOT
KEIN SYSTEM IST SICHER
TOM SCHILLING
ELYAS M'BAREK
WOTAN WILKE MÖHRING
ANTOINE MONOT, JR.
HANNAH HERZSPRUNG
TRINE DYRHOLM
WHOAMI
25.09.14
EIN FILM VON BARAN BO ODAR
www.whoami-film.de
SevenPictures

CASE STUDIES

CASE STUDIES

Human is the weakest link;
by default

We can be taught security;
we’re wired for that

Drive security with fear, social
incentives, and habits;
not money

Knowing attack types,
influence principles, and
security valuables is essential

“How to stay safe online” guide:

Text https://github.com/sapran/dontclickshit/blob/master/README_EN.md

Mind map http://www.xmind.net/m/raQ4

Contacts: https://keybase.io/sapran