PROTECTING OUR PEOPLE THE AWKWARD BORDER

LAURA BELL

Founder and Lead Consultant - SafeStack

@lady_nerd laura@safestack.io

http://safestack.io

#protectyourpeople

To join the discussion (but play nicely please)

This talk might make you feel uncomfortable.

Sorry.

…I want you to feel uncomfortable

I like people

Border Security

Application Security

Threat Intelligence

people are the path of least resistance

In this talk

The Problem

The need for and lack of human defense

The Tool

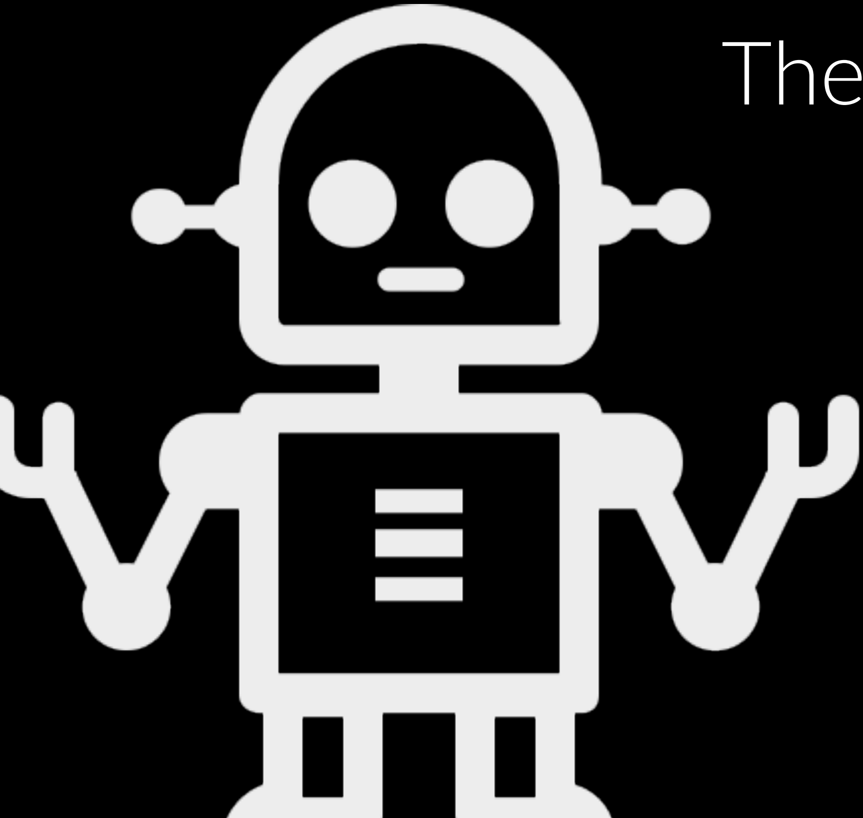
We built AVA… and we think you might like it

The Challenges

Building human security systems is hard…

we are comfortable when we talk about technical vulnerability we do not empathise or sympathise with machines

They are inanimate objects.



technology is only part of the security picture

technology

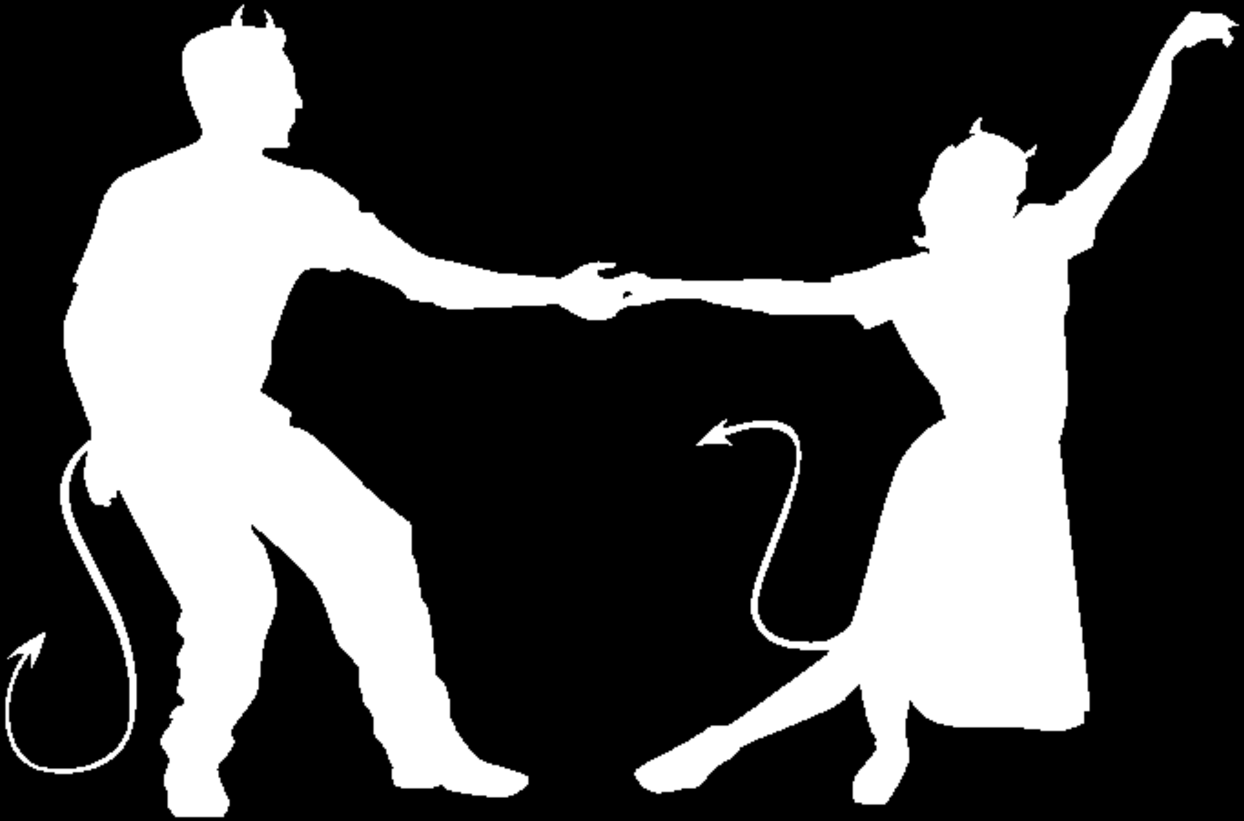
people

process

technical systems are:

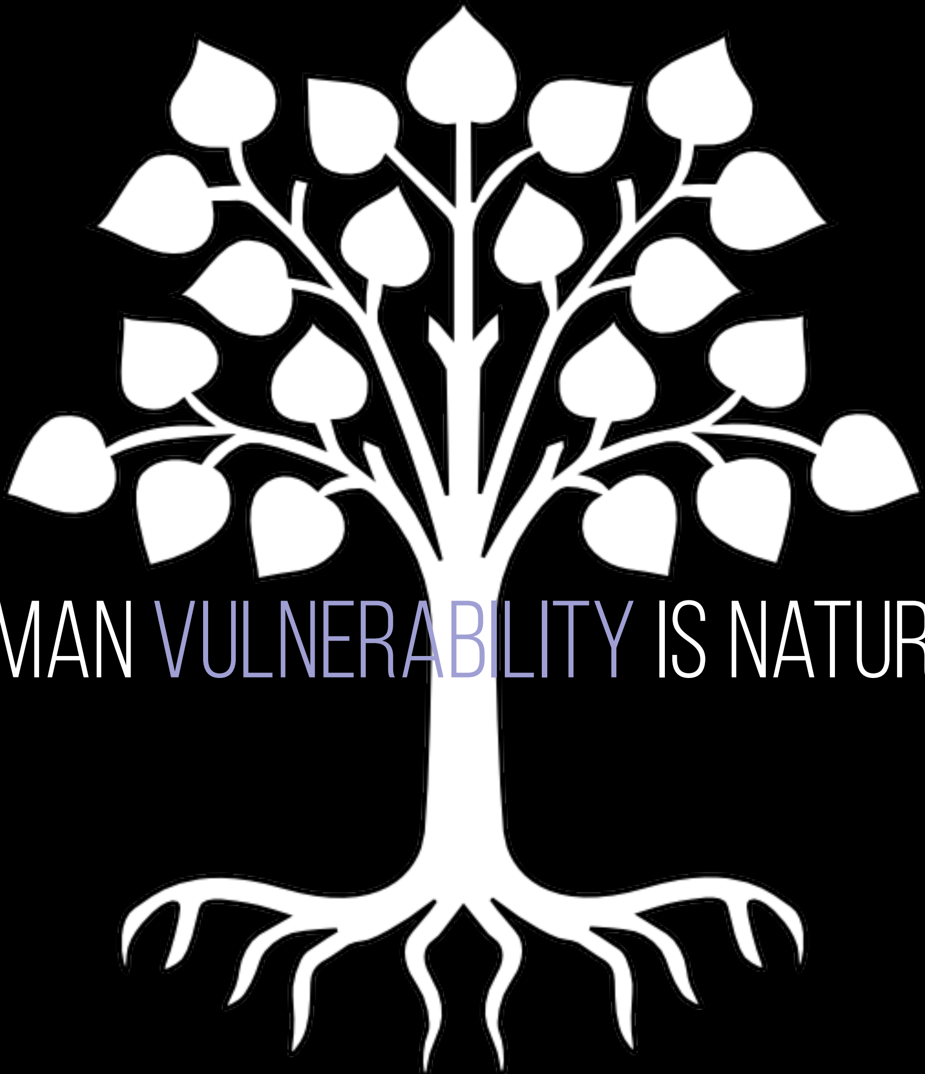
reviewed
scanned
penetration tested

processes are audited



what about people?

The problem with people



HUMAN VULNERABILITY IS NATURAL

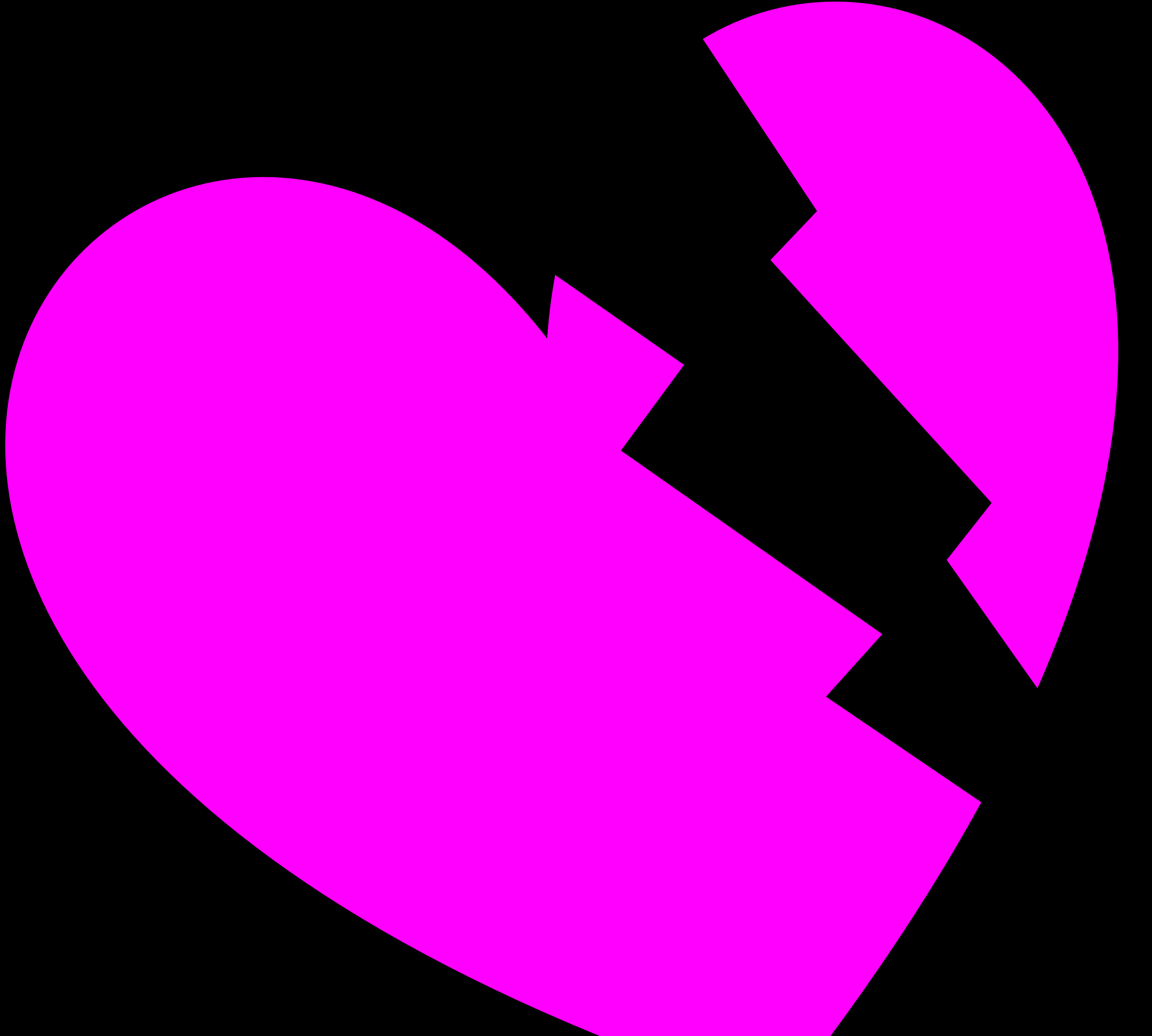
fear of loss

fear of rejection

fear of physical harm

fear of exposure

love



humans are sufficiently predictable to make it suitably annoying when we fail to predict their behaviour.

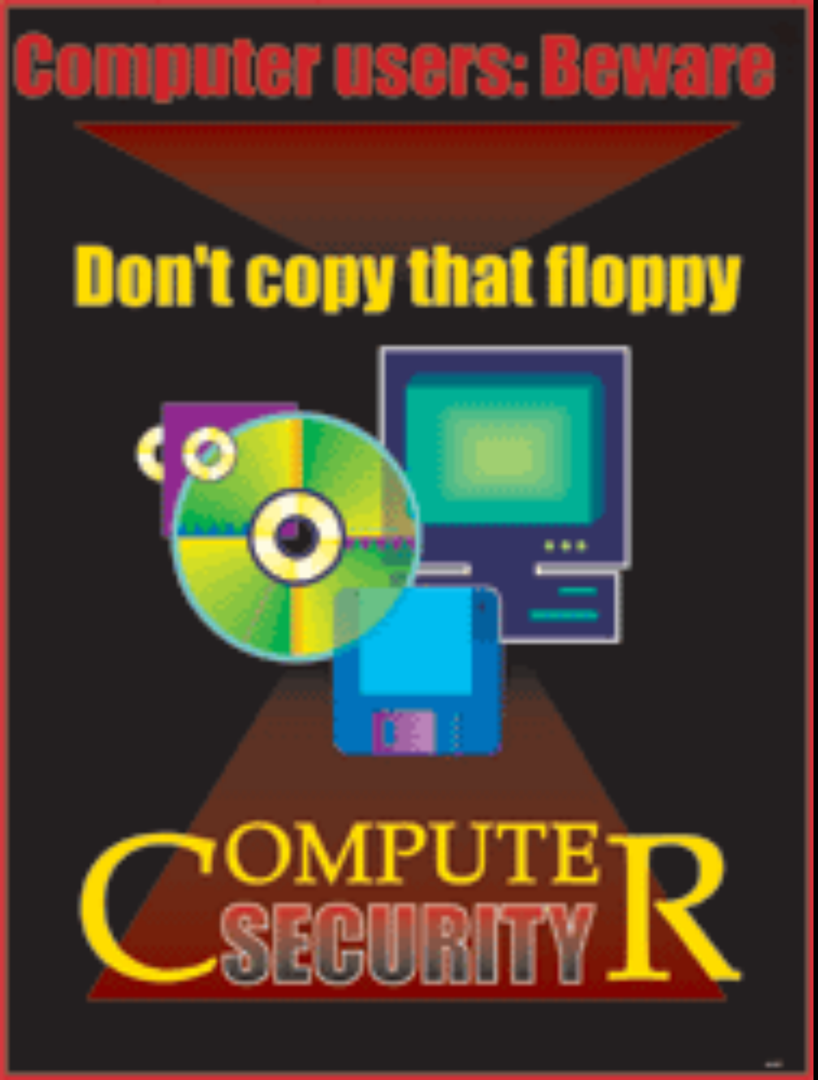
The modern approaches

compliance has us racing to the bottom

we watch video training or e-learning

we tick boxes

we make posters


Computer users: Beware
Don't copy that floppy
COMPUTER
SECURITY

Treat your password like your toothbrush…
Don’t share it with others!
Change it often!
INFORMATION SECURITY IS
EVERYONE’S RESPONSIBLITY

this is not how people learn

go ask the education and psychology communities

this is
adversarial defense

people can’t be taught

people are lazy

people are stupid

RESK
McAnn's BAR
KINKY
OF PARIS
MOVIES
FREE
McAnn's BA
LUCKY BAR

```
s/people/we/g
```

we shame the human victims of human security attacks*

*while secretly doing the exact same things

we forget that we are a connected species

Alex Bramwell

It’s time for the age of collaborative defense

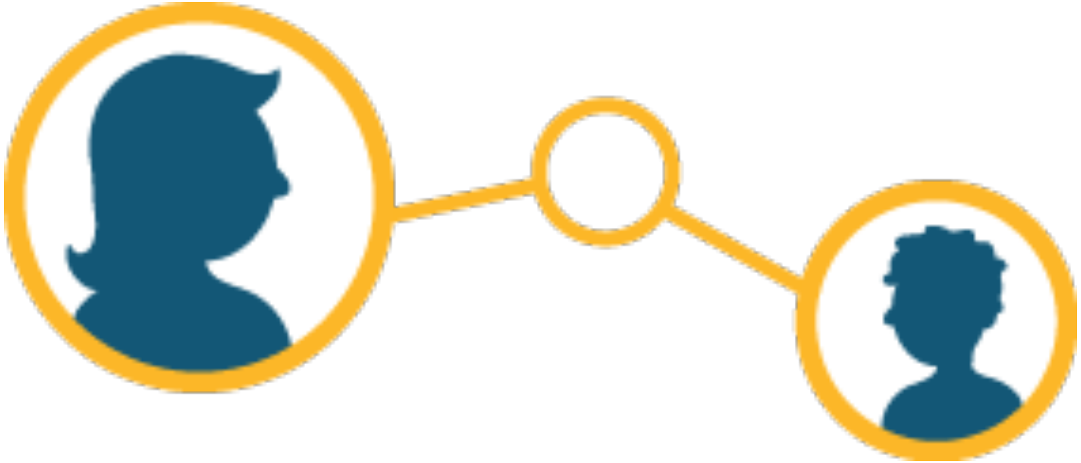
border devices are not enough

AVA

A
FIRST GENERATION
PROOF OF CONCEPT
3- PHASE
AUTOMATED
HUMAN VULNERABILITY
SCANNER

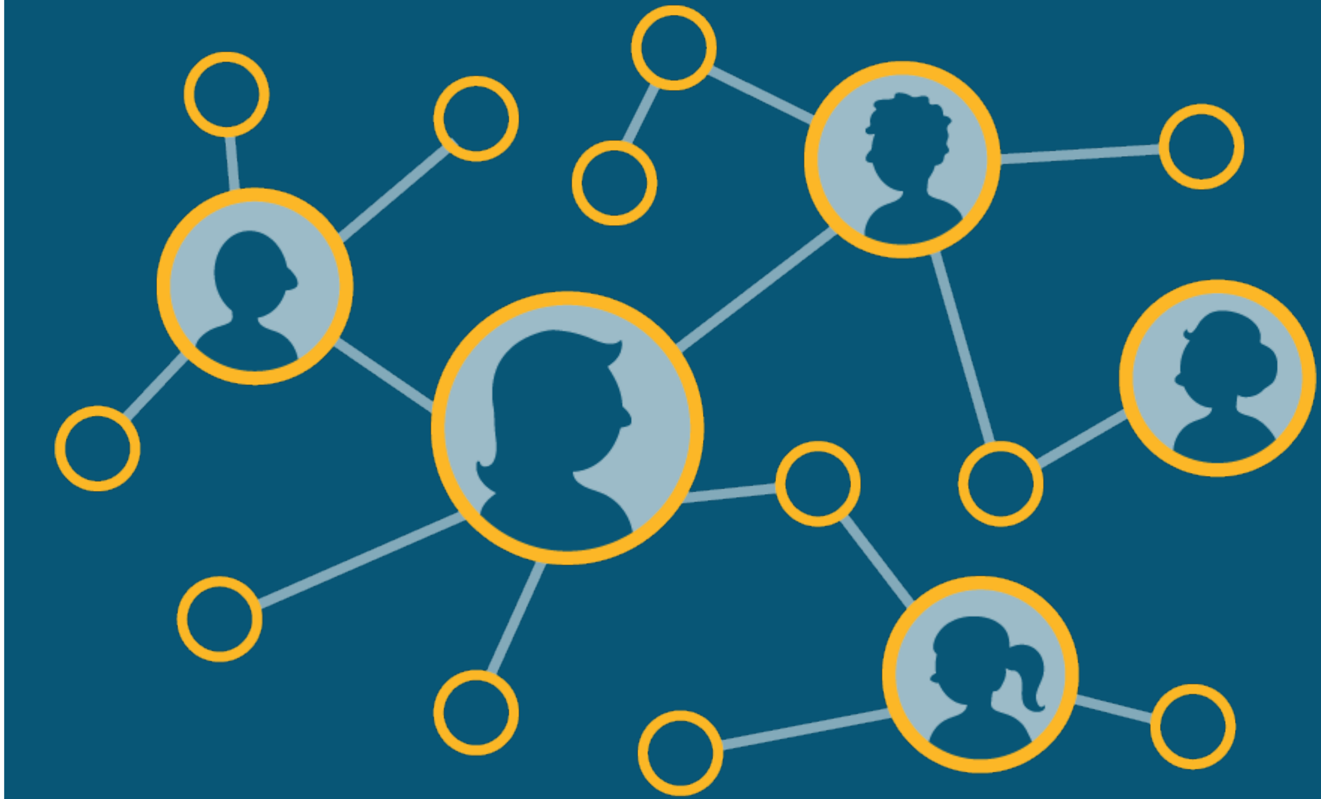
PHASE 1

KNOW



WE DON'T KNOW WHAT OUR ORGANISATIONS LOOK LIKE

HUMAN SECURITY RISK IS MAGNIFIED BY CONNECTION



ACTIVE DIRECTORY
TWITTER
LINKEDIN
FACEBOOK
EMAIL PROVIDERS

→

PEOPLE
IDENTIFIERS
GROUPS
RELATIONSHIPS
DATA

FRIENDS

CONTACTS

FREQUENCY

ALIASES

PROFILES

LAST LOGIN

PW EXPIRES?

DISABLED?

INFLUENCE

ADMIN?

LOCATION

TIME STAMPS

SENDER

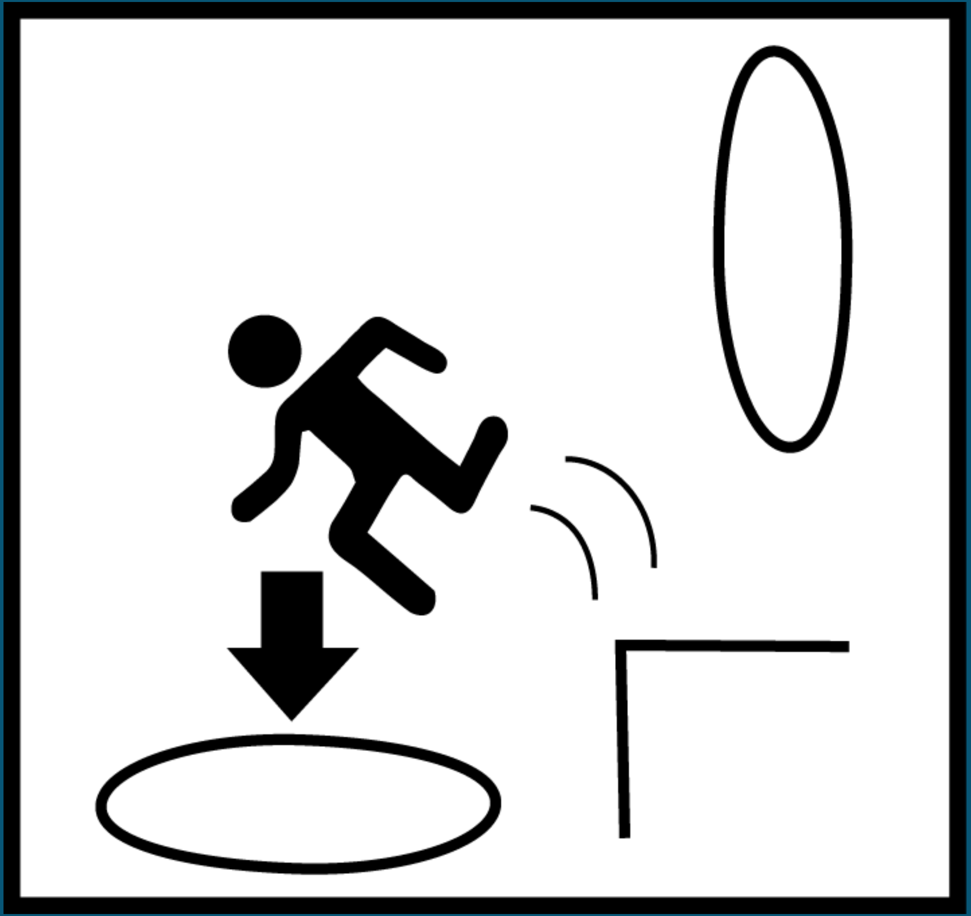
RECEIVER

USER AGENT

PHASE 2

TEST

THREAT INJECTION AND BEHAVIOUR MONITORING



EMAIL

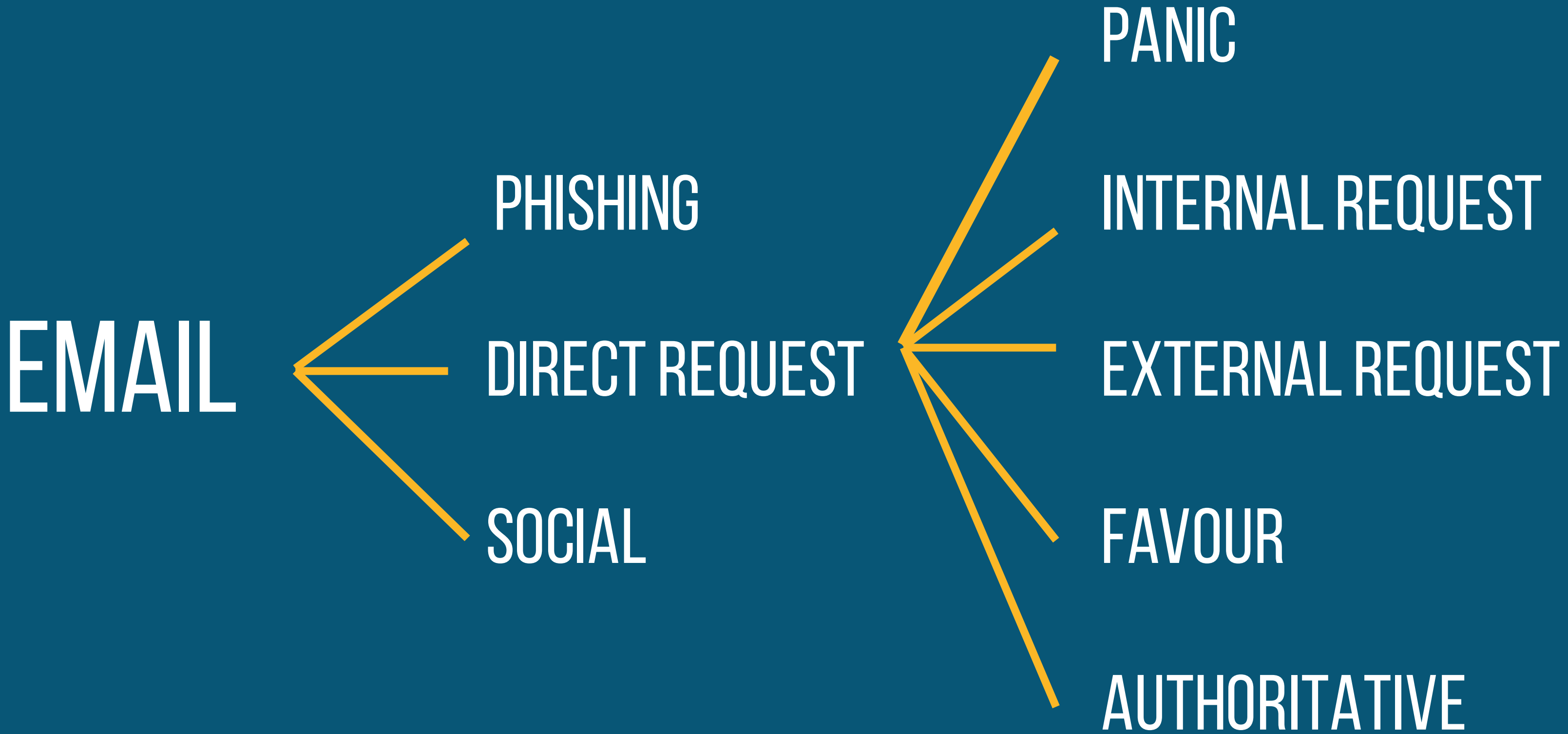
SOCIAL NETWORKS

REMOVABLE MEDIA

FILES AND HONEYPOTS

SMS

ATTACK VECTORS THAT MEAN SOMETHING



EMAIL

- PHISHING
- DIRECT REQUEST
  - PANIC
  - INTERNAL REQUEST
  - EXTERNAL REQUEST
  - FAVOUR
  - AUTHORITATIVE
- SOCIAL

EMAIL ATTACKS THAT GO BEYOND PHISHING

The URL may be different on different messages.
Subject: Security Alert: Update Java (*See Kronos Note)
Date: February 22, 2013

USER GENERATED AND PUBLICLY SOURCED ATTACKS

If you require assistance, please contact the Help Center.
****

****

Oracle has released an update for Java that fixes 50 security holes, including a
critical hole currently being exploited in the wild.
The IT Security Office strongly recommends that you update Java as

REMOVING THE BOUNDARIES BETWEEN BUSINESS AND PERSONAL

SECURITY FAILS WHEN IT IS TREATED LIKE A SPECIAL EVENT

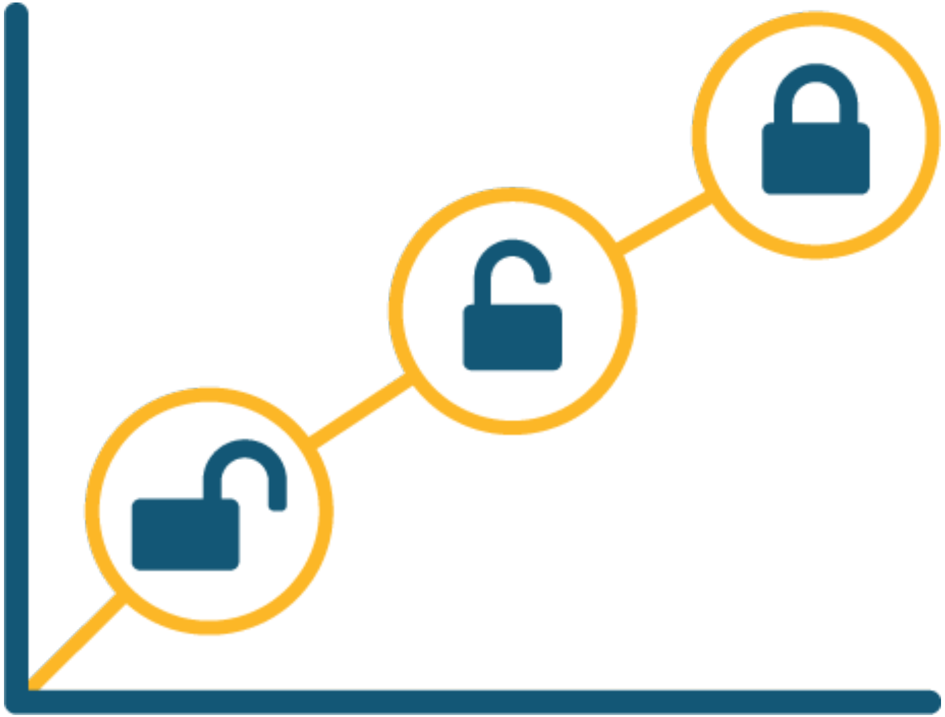
INSTANT, SCHEDULED AND RECURRING

GIVE THE OPTION OF SUCCEEDING
AND REINFORCE GOOD BEHAVIOURS

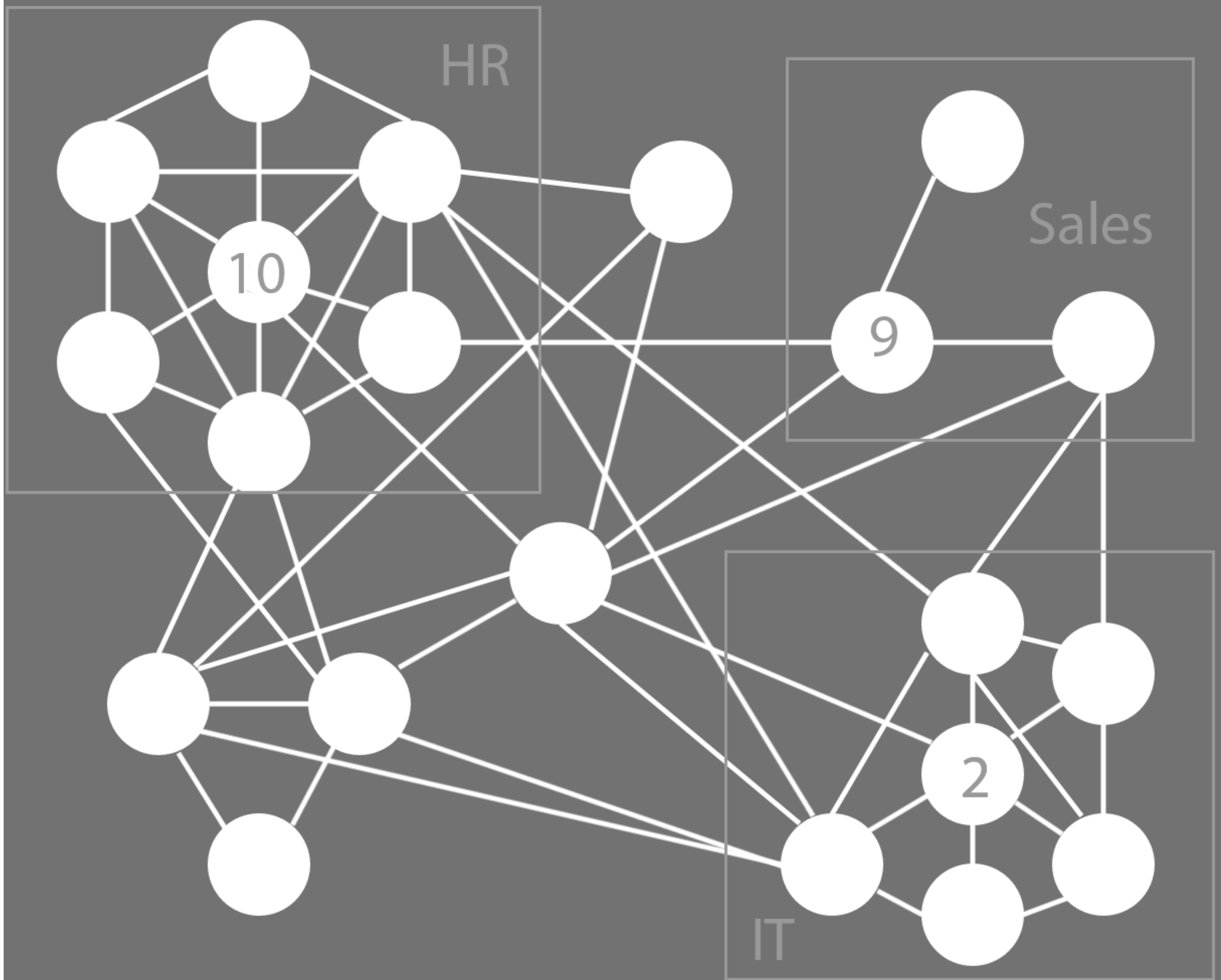
PHASE 3

ANALYSE

BEHAVIOUR VS. TIME



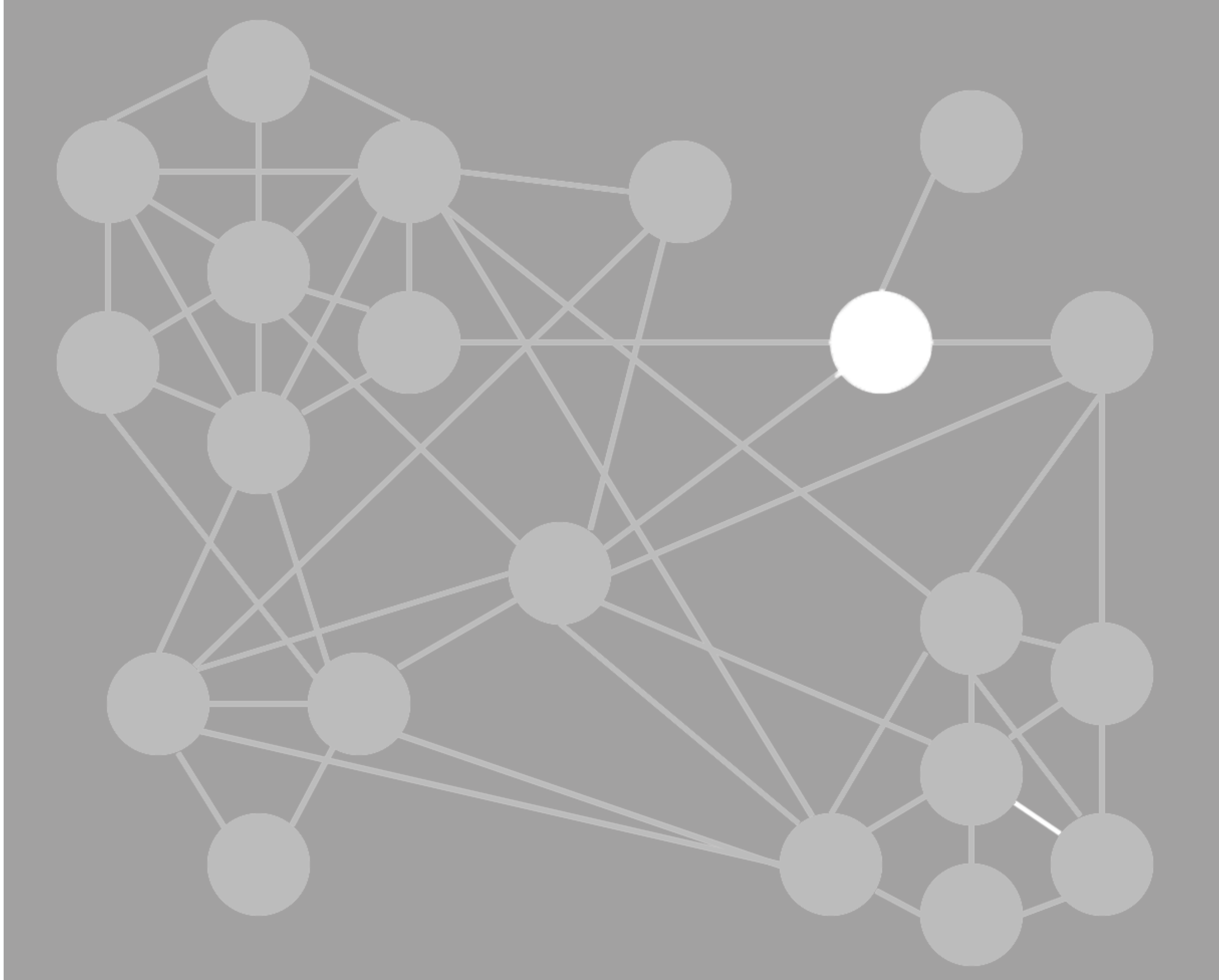
MEASURING IMPACT OF TRAINING



AND NOW FOR SOMETHING A LITTLE BIT DIFFERENT

BRIDGES, WEAK LINKS AND TARGETING

PIVOTING AND PROPAGATION



YOU KNOW WHAT WOULD BE FUN?

PREDICTIVE RISK BEHAVIOUR ANALYSIS

TECHNOLOGIES

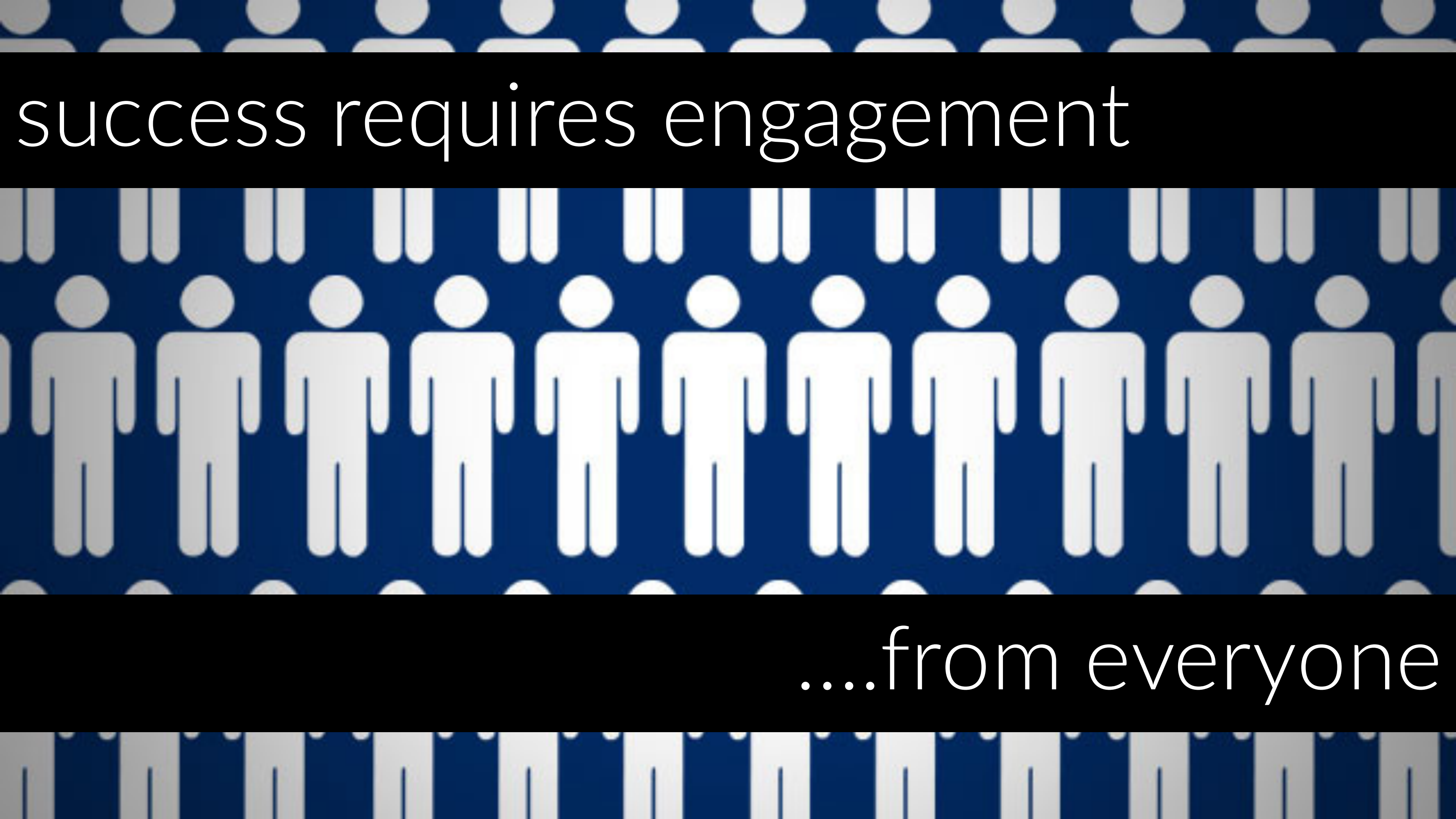
- DJANGO
- POSTGRESQL
- CELERY
- REDIS
- BOOTSTRAP

- OPEN SOURCE
- GPL
- DOCKER

- INTEGRATES WITH EXCHANGE, OFFICE 365, AD AND GOOGLE APPS FOR BUSINESS

The challenges

a public interest security tool



success requires engagement

....from everyone

is this even legal?

The law in this space is immature

publically available
previously known
already published

can we assess human vulnerability on this scale compromising the privacy the people we assess?

Know

Update

Privacy is about protecting people

Delete

Ask

yeah, if you could just give me access to all the information you have…
that’d be great

No.

AVA Ethics and Privacy Board

Objective, Representative, Independent, Collaborative

new members welcome to apply

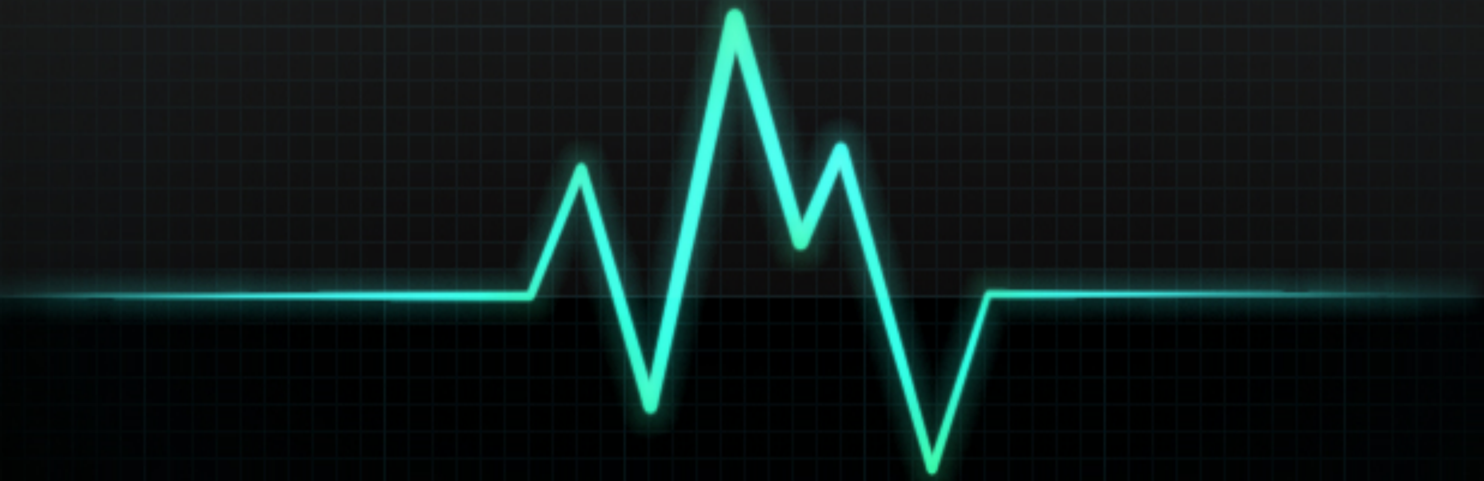
Open. Honest. Plain English

Providing people with the information they need to protect themselves and their privacy

Is this technically possible?

Building new things is hard

Scale that has to be visible



Nobody has time for more appliances

Where next?

From research project to real life

Testing
Continuous Integration
Roadmap development
Feature development

Security culture change as a service?

Ethics board

Developers

Testers

Contribution

Documentation

Sociologists

UX and design

volunteers wanted

safe
consensual
human security
science

TL;DR

We have a people problem

Attackers will choose the path of least resistance and we are not prepared

AVA is an early alpha prototype

We want a future of continuous human vulnerability assessment

The road ahead is hard

Privacy, ethics, momentum, security, scaling and much more

LEARN MORE OR GET INVOLVED

https://github.com/SafeStack/ava
now with docker build

@avasecure
http://avasecure.com
http://ava.rtfd.org/
hello@avasecure.com

QUESTIONS?

#protectyourpeople

LAURA BELL

Founder and Lead Consultant - SafeStack

@lady_nerd laura@safestack.io

http://safestack.io