No cyber without humans

How your organizational culture can boost or cripple your cybersecurity

Septembre 14th, 2022

apalala

A SHORT STORY

Septembre 14th, 2022

Introducing myself

Emmanuel Nicaise

BS IT, MS Clinical Psychology

20+ years in security, CISSP, CISM,…

CISO & cybersecurity consultant

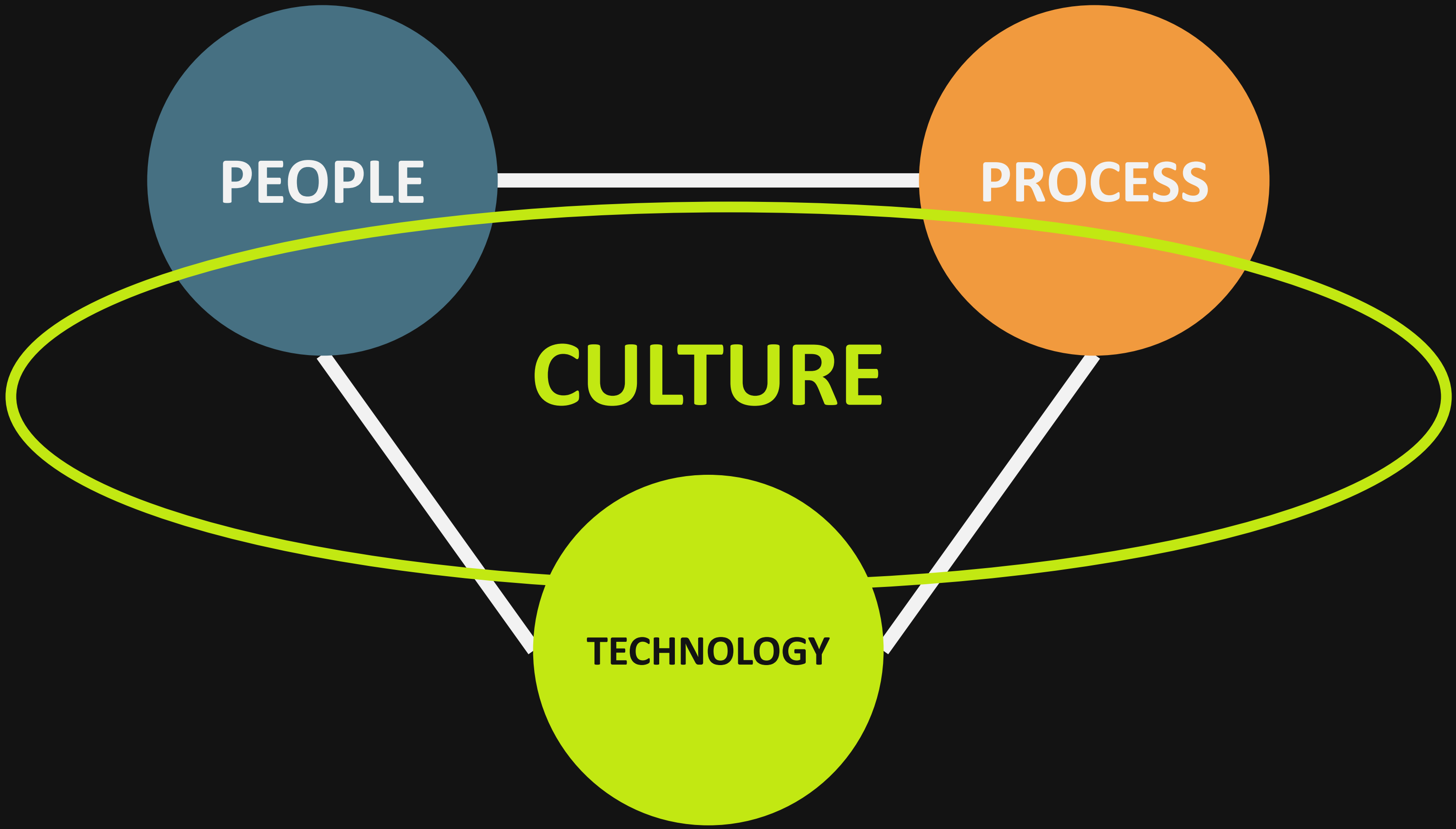
Clinical psychologist & psychotherapist

Trainer for the Cybersecurity Coalition

PhD candidate in social psychology

(focus on vigilance and phishing)

The holy trinity of Business



Culture?

Culture:

The way of life, especially the general customs and beliefs, of a particular group of people at a particular time

(Cambridge Dictionary)

✡ ☩ ✝ ☯

Organisational Culture (OC)

apalala

‘The pattern of shared beliefs and values that give members of an institution meaning, and provide them with the rules for behaviour in their organization’

(Robert Kuttner)

The glue that holds an organization together through a sharing of patterns of meaning. The culture focuses on the values, beliefs, and expectations that members come to share

(Siehl & Martin, 1984)

The way we do things around here

What happens when no one is watching

Why does culture matters?

let's take a concrete example

And start with our risks

Organisation's biggest risks

According to Forbes:

- DATA BREACH
- CLIMATE CHANGE
- THE GREAT RESIGNATION
- OBTAINING TALENTS
- PANDEMIC
- LACK OF INVENTORY
- BURNOUT
- INFLATION
- FINANCIAL CRISES
- FAILURE TO INNOVATE

* https://www.forbes.com/sites/edwardsegal/2022/01/05/the-10-biggest-risks-and-threats-for-businesses-in-2022

Organisation's biggest risks

According to Forbes:

- DATA BREACH
- CLIMATE CHANGE
- THE GREAT RESIGNATION
- OBTAINING TALENTS
- PANDEMIC
- LACK OF INVENTORY
- BURNOUT
- INFLATION
- FINANCIAL CRISES
- FAILURE TO INNOVATE

Under organisation's control:

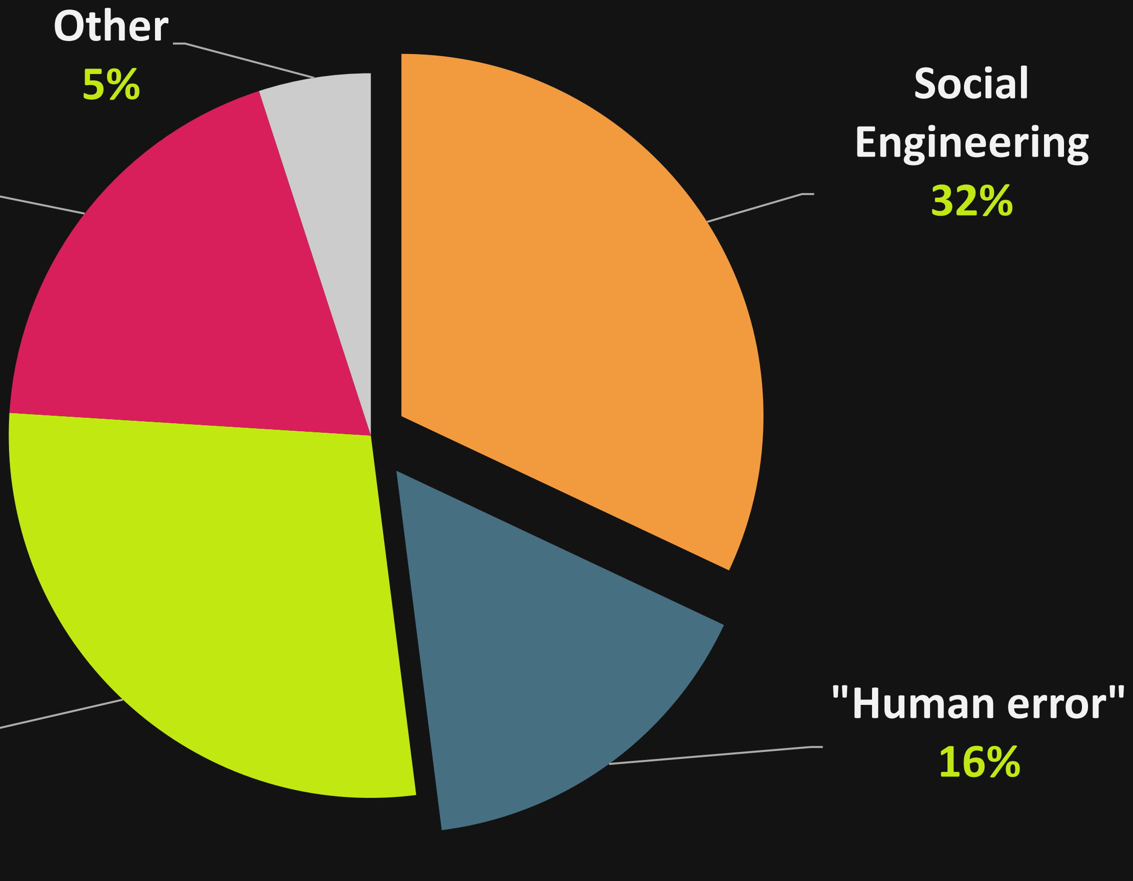
- DATA BREACH
- THE GREAT RESIGNATION
- OBTAINING TALENTS
- BURNOUT
- LACK OF INVENTORY
- FAILURE TO INNOVATE

Linked to OC :

- DATA BREACH
- THE GREAT RESIGNATION
- OBTAINING TALENTS
- BURNOUT
- LACK OF INVENTORY
- FAILURE TO INNOVATE

DATA BREACH

Root causes of data leakage*



*according to Verizon's Data Breach Incident Report 2021

DATA BREACH

Causes

- Web Application Attack
- Social Engineering > Phishing
- System Intrusion
- Human Errors

Some influencing factors

- DevOps practices (Knowledge, practices)
- Time pressure
- System configuration & patching
- User interfaces

Preventing Data Breach

- DevSecOps training, OWASP, Secure coding contests, Code review
- Prod, Pre-Prod, User Test and Test environments are created
- Pentests are performed on Pre-Prod environment for each major version
- …

Still…

YOU’VE BEEN BREACHED

Because a Dev fixed a bug in production and created a new vulnerability

Preventing Phishing

- Regular training on phishing detection, URLs, Domain names

- Monthly phishing exercises

- A warning banner is added to external emails, SPF and anti-spoofing are enabled

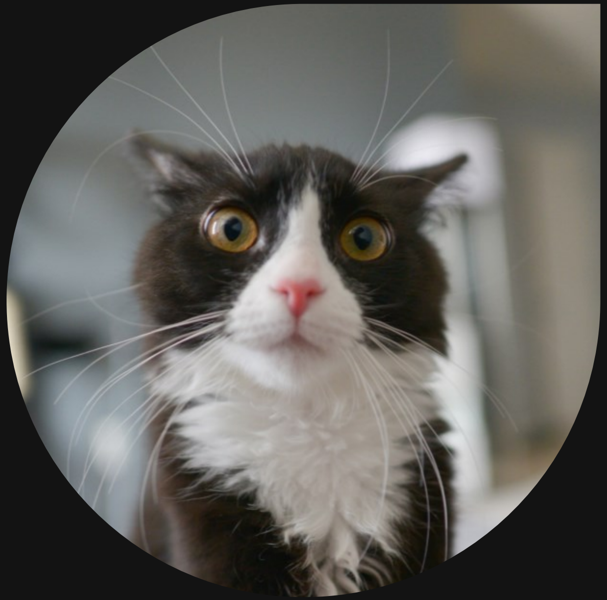
- …

Still…

YOU’VE BEEN PHISHED

Because a SysOps deactivated the anti-spoofing to allow a SaaS to send message using your organisation’s domain name and they could not find another solution on time before the project deadline.

What's wrong?



Your CULTURE plays against your team

ORGANISATION'S CULTURE / VALUES

From Belgium's Top Companies

- Passion / ambition / curiosity
- Performance / Empowerment / Accountability / Responsiveness
- Dare / Deliver / Share / Care
- Feel protected and valued / Unleash your ideas / Sustainable mindset / Bring your full self at work /

Official values / Culture vs. Actual Culture

apalala

Official values / Culture

- Client focused
- Accountability
- Respect each others ideas
- Deliver added value

Actual Culture

- Margin focused
- Hiding mistakes
- Working in silos
- Deliver on time and budget even if added value is not achieved

Why do we have differences?

- Money: KPIs and Bonuses work against culture
- Inconsistency & paradoxical communication:
  Do what I say, not what I do OR Yes, but No!
- Egos & Internal Politics: Power struggles tear down the organization
- Lack of plan to create the culture (= No Culture)

What is a culture valuing security?

apalala

Observable

- People challenging insecure behaviors
- Helping colleagues
- Asking the security team questions
- Identifying and requesting missing cybersecurity training
- Involving security early on in projects
- People reporting incidents, even if they cause them
- Phishing reporting rates is high
- Locking screens
- Shredding paperwork
- …

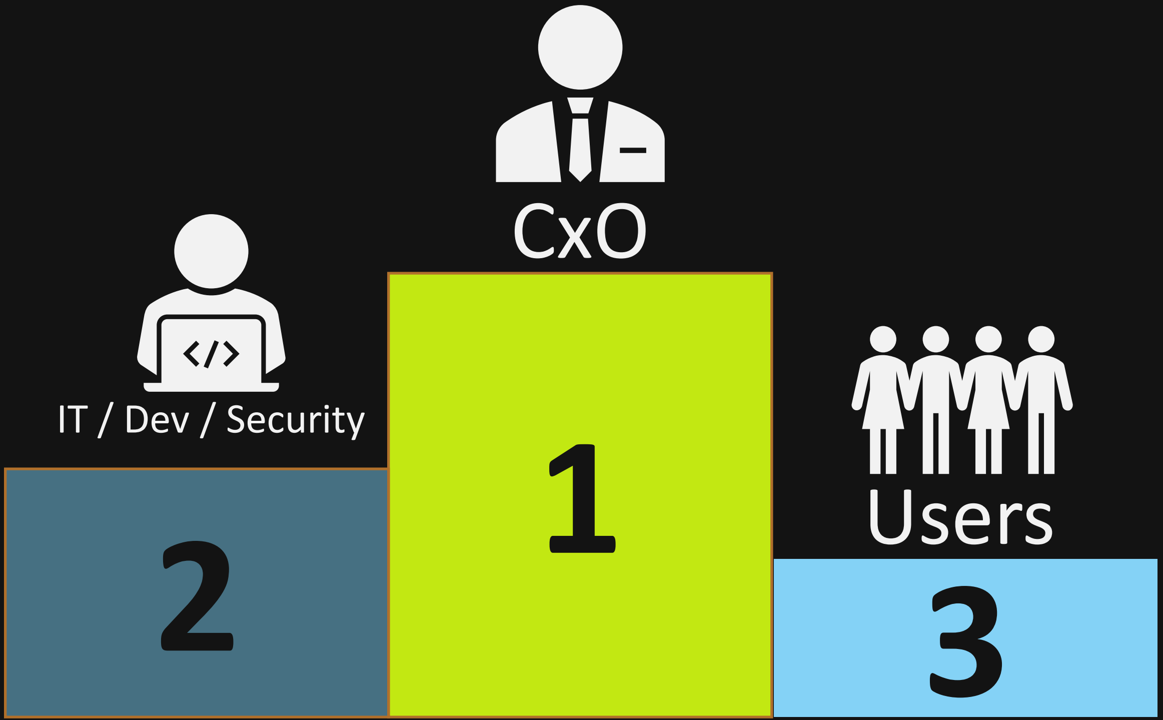
Non-Observable

- Feeling comfortable asking questions
- Knowing where to go for help
- Feeling responsible for the organization's cybersecurity
- Describing cybersecurity as part of their job description
- Belief that cybersecurity is important for the organization's success
- Understanding that the organization's security is more important than their own individual performance

How do we change the organization's culture?

- Convince Senior Management
- Define your security culture using your current organisational culture
- Be realistic, an evolution is better than a revolution
- Work with your colleagues from HR and Internal Communication
- Ensure alignment & consistency

Where to start?



Define Objectives

apalala

CxO

Leading by example

Budget & Priorities

Policies and rules

IT & Security

Understand the risks

Follow the rules

Be part of the solution, not the problem

Users

Understand the risks

Follow the rules

Be vigilant

Identify risks & Report incidents

A few Tips

- Connect with people & listen carefully
- Be humble and empathetic, suspend your ego
- Find common grounds, common values
- Let people define the security culture (Bottom-up)

If they are responsible for security, they should have a say about it

L O P Z D
F P O T E C

THANK YOU