Improving Cyber Security Culture: Part 01

A 10 Step Approach to Improve Cyber Security Culture

CultureAI's cyber security and behaviour science experts look at how organisations can evolve from raising security awareness to building resilient cyber security cultures, where employees help defend both the organisation and themselves.

www.culture.ai

Culture AI
Helping People Defend

About this Series

This guide is part 1 of CultureAI's **"Improving Cyber Security Culture"** series; a set of resources produced by our cyber security and behaviour science experts, to share our insights and experience with organisations looking to change employee security behaviour and improve security culture.

We intend for this series to serve as a practical guide for IT, IT Security and HR Managers with a stake in raising awareness and improving cyber security culture in their organisation.

In this series

- ● **Security Culture & Behaviour Change Theory**
- ○ Planning a Security Culture Improvement Programme
- ○ Communicating your Programme
- ○ Implementing Ongoing Culture Assessment & Monitoring
- ○ Executing your Programme with Maximum Results

We release the next guide in the series every Friday on our website, LinkedIn & Twitter feeds

www.culture.ai

@culture_ai

in cultureai

What is Cyber Security Culture?

The industry is flooded with pop-up awareness training providers throwing around the terms ‘awareness’, ‘behaviour’ and ‘culture’ almost interchangeably. Forgetting the marketing hype, what do these terms actually mean to organisations looking to reduce cyber security risk?

Security Awareness

Security awareness simply means, “**does an employee know how to behave securely?**” Raising awareness does not guarantee an improvement in behaviour or a reduction in risk.

Security awareness is a poor way to measure risk.

vs

Security Behaviour

Security behaviour is **how people actually behave** from a security perspective in real-life situations (eg. do they set strong passwords?). This is influenced by awareness, capability, attitude, cognitive process and social norms.

Measuring security behaviour is a great measure of risk for known behaviours.

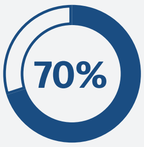
vs

Security Culture

Security culture is best thought of as the **sum total of all security behaviours throughout an organisation**. It’s an incredibly good predictor of cyber security risk as it is an accurate indicator of how employees will behave.

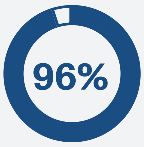
Measuring security culture is a great predictor of risk for unmeasured behaviours.

Most organisations still focus on awareness and fail to significantly reduce risk



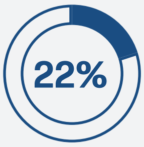
70% of organisations with security awareness training have had an incident caused by employee security behaviour.

Awareness training alone is not reducing risk effectively enough.



96% of social attacks, from phishing to tailgating, are not reported by employees, impeding detection.

There is an opportunity for organisations to improve their detection capability significantly by improving security culture.



22% of employees on average still click on phishing emails within organisations that believe they have a good security culture.

It’s important to assess the effectiveness of your awareness campaigns in reducing your risk from real-world threats.

How is Security Culture Improved?

In order to improve cyber security culture, organisations must identify and change the range of employee security behaviours that put their organisation at risk.

Unfortunately, changing behaviour isn't as simple as just deploying security awareness training to all employees - which is why most organisations fail to build resilient security cultures. The diagram below shows the main pillars of behaviour change, which should be addressed for each behaviour that presents a risk to the organisation and tailored to each employee.

To improve security culture organisations need to zoom out from just raising security awareness.

1

Identify and prioritise the behaviours that put your organisation at risk

2

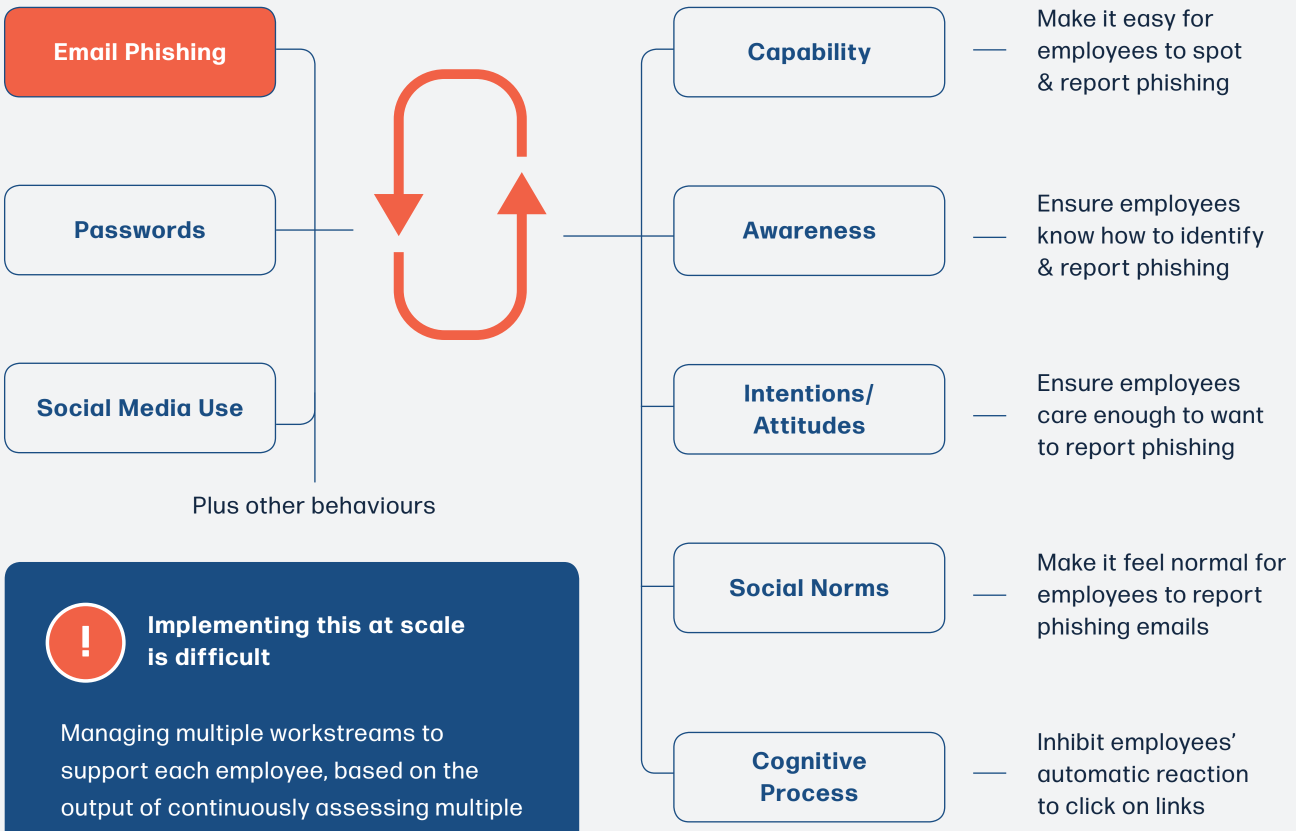
Continuously assess each behaviour at an employee level

3

Use behaviour change theory to understand the behaviours observed

4

Run workstreams for each employee to improve behaviour



Email Phishing

Passwords

Social Media Use

Plus other behaviours

Capability	Make it easy for employees to spot & report phishing
Awareness	Ensure employees know how to identify & report phishing
Intentions/ Attitudes	Ensure employees care enough to want to report phishing
Social Norms	Make it feel normal for employees to report phishing emails
Cognitive Process	Inhibit employees' automatic reaction to click on links

! **Implementing this at scale is difficult**

Managing multiple workstreams to support each employee, based on the output of continuously assessing multiple behaviours is not easy to manage.

CultureAI's platform allows you to run the process above on autopilot.

Where to start?

Start by planning a structured security culture programme with the clear objective of building a security culture where your employees help defend the organisation and themselves. The steps below describe the high level process we've found to work exceptionally well. Each week CultureAI will release a guide covering the steps in further detail.

Designing & Implementing a Security Culture Improvement Programme

Self Implemented or Autopilot

1.	**Engage Stakeholders**	Involve IT, IT Security, HR & Senior management
2.	**Identify Risks & Compliance Reqs**	Identify the behaviours that put your organisation at risk
3.	**Set Objectives & KPIs**	Set clear, measurable objectives to achieve for each behaviour
4.	**Evaluation & Benchmark**	Evaluate & benchmark current behaviours
5.	**Communicate**	Communicate your programme clearly to employees
6.	**Implement Monitoring**	Implement continuous assessment & analysis of employee behaviour
7.	**Improve Capability**	Deploy controls & assistive tools to help employees behave easily
8.	**Improve Awareness**	Improve employees' grasp of each behaviour, using their preferred learning method
9.	**Improve Intentions**	Get employees wanting to help defend the organisation
10.	**Improve Cognitive Process**	Ensure that employees' automatic actions are safe

Design & run on autopilot with CultureAI's platform.

Our team will set up your security culture programme, then give you access to our web-based platform.

The platform allows you to run every aspect of it on autopilot, with as much or as little control as you like, and view results in real-time.

Ready to get started?

www.culture.ai/start

contact@culture.ai

+44 (0) 800 368 7676

In the next part...

We'll start diving into detail, with a look at engaging stakeholders ahead of your security culture programme for best results.

www.culture.ai

cultureai

@culture_ai

Culture AI

Helping People Defend

CultureAI are a team of cyber security experts, penetration testers, behaviour scientists, machine learning and general technology geeks. Our team have worked with some of the worlds leading organisations to help them successfully build resilient cyber security cultures, where employees play a key role in defending their organisation. We're also a GCHQ certified training provider.

We built the world's first Security Culture Enablement Platform® to enable any organisation to transform security culture effectively. It does this by providing and automating all of the tools needed to change a range of behaviours, including security awareness training that intelligently adapts to each employee, within a single unified platform.

www.culture.ai   @culture_ai   in cultureai

CESG Certified Training

CYBER ESSENTIALS PLUS

CSA cloud security alliance℠

QMS ISO 9001 : 2015 REGISTERED Cert No. 310292019

QMS ISO 14001 : 2015 REGISTERED Cert No. 317432019

QMS ISO 27001 : 2013 REGISTERED Cert No. 310282019 www.culture.ai

contact@culture.ai

+44 (0) 800 368 7676

Culture AI
Helping People Defend