



BANK OF ENGLAND

Bank Security




Building a security conscious culture


CAA Aviation Cyber Forum
23rd April 2021

John Scott – Head of Security Education



Security Awareness

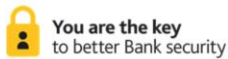
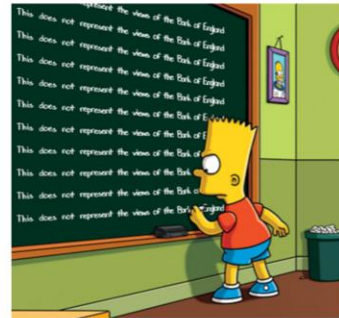


 **You are the key**
to better Bank security

Building a security conscious culture | 2

Introduction – why people make mistakes and what fixes them.

Who am I?



Building a security conscious culture | 3

Intro and disclaimer – all my own opinions and not those of the Bank of England or the SANS Institute.


I'm the Head of Security Education at the Bank of England, running their security awareness and cultural change programme for the last 5 years.

I'm also an Instructor for the SANS Institute, teaching on MGT433 – Managing Human Risk.

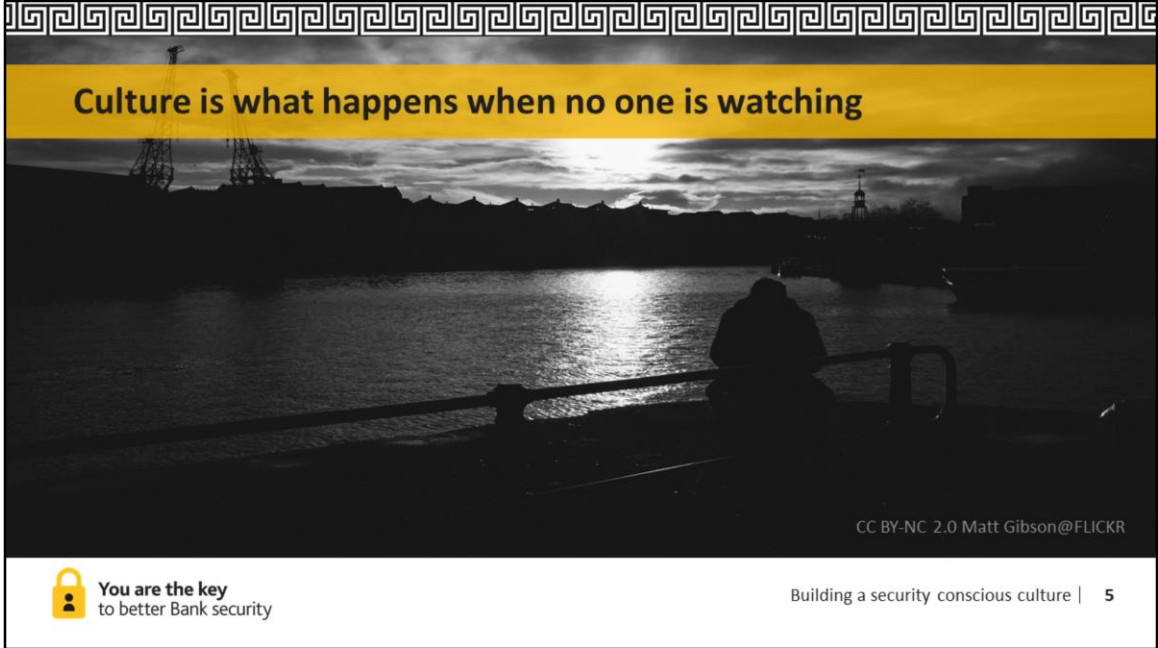
I'm on LinkedIn at <https://www.linkedin.com/in/johnfscott/>

“If we define a healthy cybersecurity culture as **clear policies about acceptable online behavior**, how would you characterize the health of your organization’s cybersecurity culture as measured by its collective online behavior?”

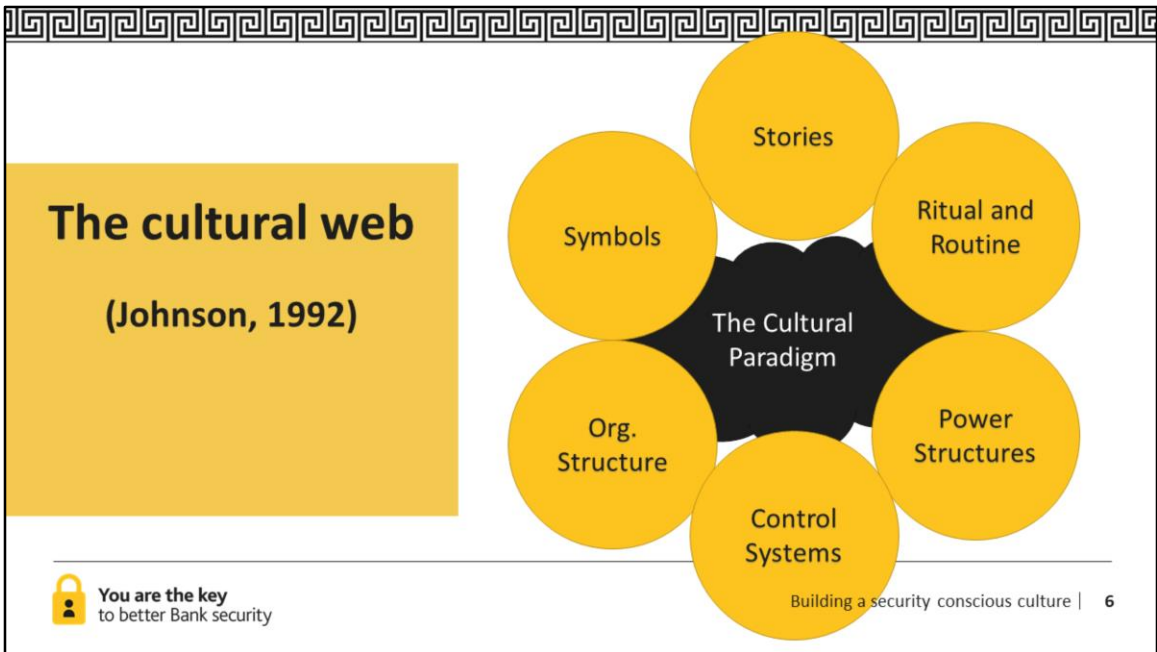


 **You are the key**
to better Bank security

We need to decide what we mean by culture – the above quote came from a technology conference, and is part of the way there, but only really touches on part of it.



I don't think there's such a thing as Security Culture – (or safety culture for that matter) – just cultures which value safety and security. Because culture is everything about your organisation. And it changes whether you want it to or not. All you can do is try to shape aspects of it by promoting, recognising and rewarding the behaviours that you want to see in your staff.



The Johnson and Scholes Cultural Web posits that you don't change culture, you change the things which change culture. And not all of those are in the remit of your awareness programme – if your senior executives won't wear their ID badges, for example, it's more difficult to enforce lower down. Whereas if everyone is empowered to challenge anyone who isn't wearing their badge, that's a better indicator of your culture.

https://www.mindtools.com/pages/article/newSTR_90.htm

Slips, lapses and mistakes

“Operators tend to be the inheritors of system defects created by poor design, incorrect installation, faulty maintenance and bad management decisions. Their part is usually that of adding the final garnish to a lethal brew whose ingredients have already been long in cooking.”

Human Error
James Reason 1990

Photo: TSgt Lealan Buehrer @USAF


 **You are the key**
to better Bank security

Building a security conscious culture | 7

Culture needs to address all three sorts of non-deliberate error, but needs to address them differently. Organisational cultures which value safety are used to no-blame post incident reviews. The same needs to happen with security.


Remember, a phishing email in my inbox has beaten all of the organisational technical controls.

Risk Assessment



JAWS

PROBOSCIS

 You are the key
to better Bank security

Building a security conscious culture | 8

One of the key differences between security and safety culture is how well people can assess risk. Mosquitos kill more people in a day than sharks have killed in 100 years, yet which do we think is higher risk? In security, especially Cyber Security, the consequence of a bad decision may not be visible for a long time, if ever.

Awareness, Behaviour then Culture

CC BY-NC-ND 2.0 Diamond Geysler@Flickr

 You are the key
to better Bank security

Building a security conscious culture | 9

Awareness, then behaviour, then culture ...

Awareness isn't enough – the person has to want to change their behaviour. It has to be to their benefit.

This chap won't change because his business model is custard pies in the face.

Ongoing engagement tactics



CC-BY-NC-ND 2.0 foreverdigital@FLICKR



You are the key
to better Bank security

Building a security conscious culture | 10

Remember the main thing about engagement – the other person has to say yes
Are we listening as much as we are talking? When does security get in the way of the organisation trying to do what it does? Can we make things easier for people rather than harder?

Respect your colleagues

Information Security Awareness

- Educate yourself and your users
- Test your users: exams and simulated attacks
- Create awareness around the office
- Reward good security
- **Every** employee is part of the security team

Photo credit John Scott



You are the key
to better Bank security

Building a security conscious culture | 11

Do your security team have a 'stupid users' attitude? Your users probably know that. And that undercuts all of your 'Security is for everyone' or 'Security is everyone's responsibility' messaging. Technology is rife with this. Your colleagues are domain experts in their fields, whatever that is. If they don't know about security, that makes them uninformed or uneducated, not stupid.

Gamification and phishing



Image credit Yaoren Wo



You are the key
to better Bank security


Building a security conscious culture | 12

Be very clear what your programme is for – we use phishing as an education tool, not a punishment tool. Education delivered right at the point of interaction – the moment the phishing email is clicked on, is very valuable.

Use the right language

CC-BY 2.0 emdot@FLICKR

CC BY-SA 3.0 Kim Traynor@Wikimedia

 **You are the key**
to better Bank security

Building a security conscious culture | 13

People don't relate to language they don't understand – so why talk about your staff being your 'human firewall' or 'sensor net' when you could talk about telling facilities when the loo is broken? This doesn't mean talking down to them, just using non-technical language and metaphors that make sense and resonate with them.

Modelling good behaviours

Clear Desk Inspection

- ✓ Desk pedestal locked
- ✓ Sensitive hardcopy material secured
- ✓ Computer secured

Thank you.
You've helped keep the Bank's information secure.

INFORMATION SECURITY
YOU are our first line of defence

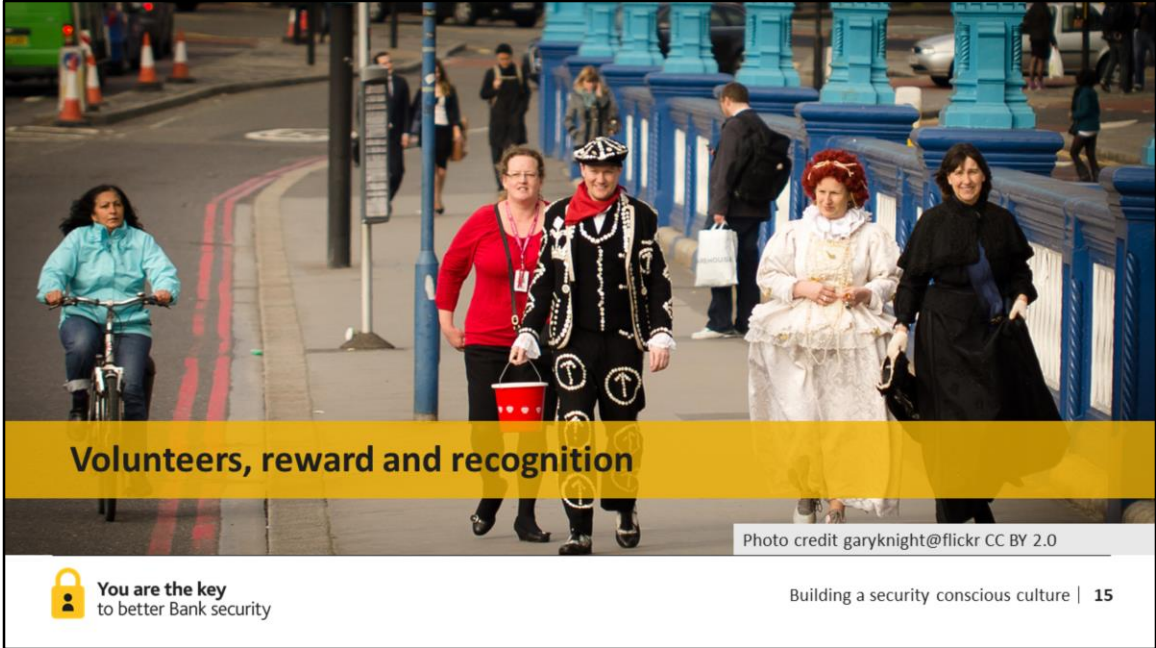
Photo credit John Scott

You are the key
to better Bank security

Building a security conscious culture | 14


We often call out bad behaviours – how often do we recognise good behaviours? If you have a 5% click rate in a phishing simulation – you have a 95% non-click rate. And what's your reporting rate?

Call out the good behaviours to show everyone what to aspire to.



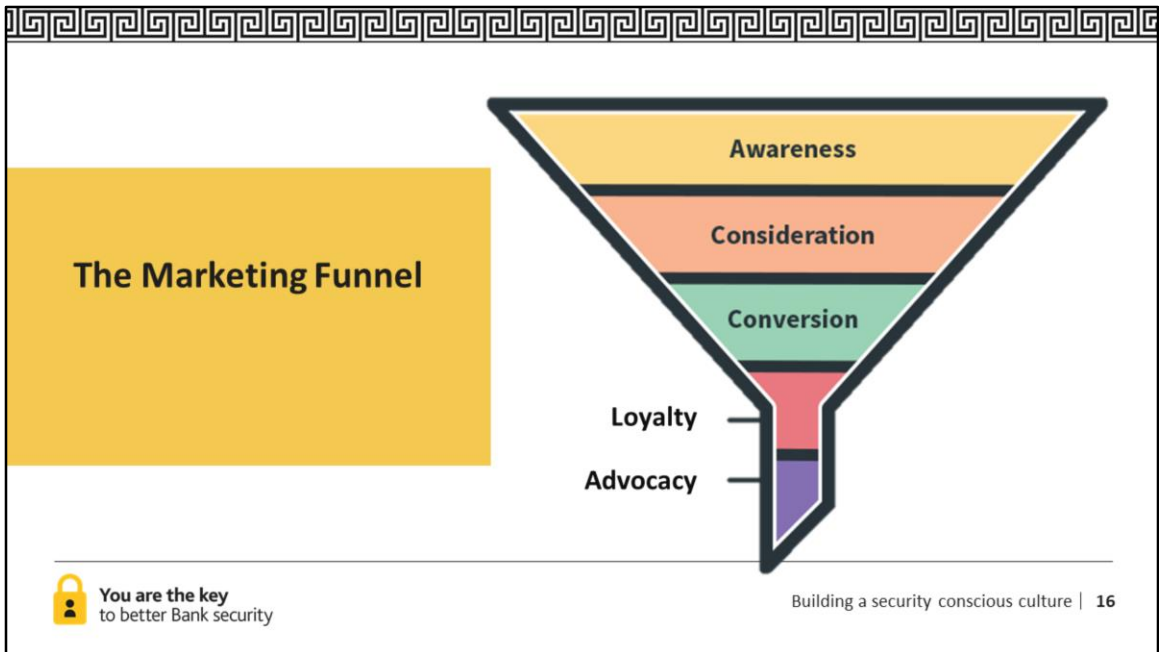
Volunteers, reward and recognition

Photo credit garyknight@flickr CC BY 2.0

 **You are the key**
to better Bank security

Building a security conscious culture | 15

If you have people on your teams willing to go that extra mile – what do you do about it? Recognition is key – mention it to their line management even if you can't afford (or don't want) to give people rewards.



Learn from the experts in behaviour change – marketers. You want your customers to understand ‘whats in it for them’ and to become not only repeat customers, but advocates for your brand.



Remember this isn't a race with an end point – it's an ongoing journey to change cultures. It's great to have a focus on security that the whole organisation focuses on for a year, but you don't want seniors saying 'didn't we do culture last year?' – this has to be seen as something that happens every day.

Three take-aways

1. The most visible sign of cultural change is widespread behavioural change
2. Fix what you can fix with the appropriate tools – procedures and technology for slips and lapses, awareness and education for mistakes
3. Culture change is slow but inevitable – you can shape the direction, but not steer it

