Building a Security Conscious Culture

Melanie Oldham
Founder & CEO
Melanie Oldham
The Boss & Founder of Bob’s Business
10+ years experience in Infosec
Passionate about digital adoption
Advocate of cybersecurity as an enabler
Chair of Yorkshire Cyber Security Cluster

www.linkedin.com/in/melanieoldham
Why don’t employees exhibit responsible behaviour?

Malicious intent?
People driven by emotion

**Criminals** by greed, anger, jealousy, power

**Employees** want to please, do a good job, be helpful, work hard
If people want to please, where does it go wrong?

Organisational challenges

• Increasing awareness & understanding
• Removing communication barriers
• Getting people to care about security
Common pitfalls

Believing ISA is an ISO/ IT function
Failing to get personal
Underestimating the power of the people
Assuming fear is an enabler
Poor planning & communications
So...

How do you build front line defenders?
Engage the disengaged & change behaviour?
Communication is Key

To achieve positive change you need to deliver in a way employees can understand and relate to:

- More listening
- Take more in
- Increased engagement
Vilifying the user

Fear is not an enabler

Damages communication - Them & US

No trust, not conducive to developing positive, communicative culture

Focus isn’t on education, but on punishment

Reward & Recognition
Creating the right environment

- Trusted environment
- Encourages learning and reporting
- Positive reinforcement
- Sharing of experiences
Keep it simple!

- No unnecessary information or jargon
- Concise practical advice
- Two way conversation
- Simple reporting
- Ease of access
Internal marketing!

Create a brand
Plan objectives
Dispelled some myths
Tone – positive, open, and engaging

Positive Attention!
Communicate!
Continual reinforcement
Make it relevant!

- Make it personal
- Make it emotional
- Align with people’s values
Power of the people

People assume the actions of others in an attempt to reflect correct behaviour for a given situation

Need to understand they are an integral part of our cyber defences.
Collaborative approach

**HR** - Remove sensitivities around awareness campaigns

**IT** - Identify trends and approachability, referral process

**Marketing** - Encourage communication, sell cyber security and good email practices

**Everyone** - Complete training and adopt best practices
Case study: HMRC

43% - 16% susceptibility to phishing risks

Transparent comms - Collaborative approach
HR - Support, sensitivities,
Yammer - Peer to peer influencing
Case studies - Making it personal
Positive reinforcement - Marketing
Thank you for listening!

Check us out at:

https://BobsBusiness.co.uk