Nottingham Trent University

The Importance of the Human Factor in any Cyber Security Strategy

Pri Alagoda – Chief Information Security Officer

EUNIS/EUA collaborative webinar on Information Security Strategy

6th May 2021

Pri Alagoda

CISO – Nottingham Trent University

25 Years Industry Experience, 14 in Information Security

Worked in 5 sectors:- Oil & Gas, Banking & Finance, Technology, Logistics, Academia

Advisory Board Member of the East Midlands Cyber Resilience Centre (EMCRC)

- CEH – Certified Ethical Hacker
- CISM – Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- CGEIT - Certified in the Governance of Enterprise IT
- ISO27001 - Certified Internal Auditor
- EU GDPR (F) - EU General Data Protection Regulation Foundation
- CDPSE - Certified Data Privacy Solutions Engineer
- MBCS - BCS Professional member

pri.alagoda@ntu.ac.uk

Why is the ‘Human Factor’ in Cyber so critical?

- Threats are evolving and Cyber Criminals are getting cleverer
- What do we know about what these attacks have in common?
- Targeted and more than likely originated via a phishing email
- BUT…
- All these institutions deployed numerous *technical* cyber security solutions
- No technical solutions in isolation are 100% effective
- Socially engineered threats bypass many cyber security systems
- CONCLUSION?

We need to understand the *'human factor'*

- ***The 'human factor' of cyber security represent the actions or events when human error results in a successful hack or data breach.***

We are only human, after all…*but*

- If hackers know that they can find a weak link
- Collectively we have a responsibility to make our defences stronger
- We shouldn't just rely solely on technical security measures
- Focus must be on both 'technical' & 'human' initiatives in equal measures
- A combined or *Layered* approach to security protection

~~***"The weakest chain in cyber security is the human being"***~~

Our approach…

- *Baseline our starting position*
- *Incorporated technology*
- *Individualised training programs*
- *Simulation based education*
- *Regular info-bytes & advisories*
- *Used multiple delivery channels*
- *Desktop Cyber Scenarios*
- *Align message to our strategy*
- *All year round approach*

NTU

Last thoughts…

- Make it feel like we are all on the same journey
- Engagement is key to creating a security culture
- Make Cyber Security awareness personal & relevant
- Give it a unique identity to your organisation
- Keep repeating the messages & encourage questions
- Awareness is our way of connecting with our audience

Nottingham Trent University

Thank you