The Irish Accounting & Tax Summit 2020

Session 9

Your Biggest GDPR Risks - IT or People?

Presenter:
Richard Jackson - Pulse Cyber Security
& Des O'Neill - OmniPro

OmniPro Education & Training
Main Street, Ferns, Enniscorthy, Co. Wexford
053 9100000
www.omnipro.ie info@omnipro.ie

Your Biggest GDPR Risk: IT or People?

Introduction

Richard Jackson
Head of Operations (Pulse Cyber Security)

EU Certified GDPR Practitioner
CISMP (Certified Information Security Management Principles)
IIBA Business Analyst
ILM Project Manager
ILM Lean Management

www.pulsecyber.co.uk

pulse cyber security

Schedule

1) The GDPR: Current State
2) Human Science & Cyber Crime
3) Social Engineering
4) Trust is Vulnerability
5) Heuristic vs Critical Thinking
6) The Human Firewall

www.pulsecyber.co.uk

Europe & the GDPR Landscape

- 230 Fines Issued across Europe since May 2018
- Ireland & UK Combined: 2 Fines
- Ireland (DPC) under pressure from other nation states, with significant fines and orders for change against both Facebook and Twitter expected by early summer
- Focus on “Education and Awareness” from the ICO and DPC
- UK heavily impacted by over-reporting of breaches (x3)

Europe & the GDPR Landscape

Ireland:	1	Greece:	8
Belgium:	6	Hungary:	23
Bulgaria:	19	Iceland:	2
Croatia:	1	Italy:	11
Cyprus:	8	Latvia:	2
Czech Rep:	11	Lithuania:	1
Denmark:	4	Norway:	4
France :	5	Poland:	7
Germany:	25	Portugal:	4
UK:	1	Romania:	26
Slovakia:	6	Spain:	80
Sweden:	3	Netherlands:	4

www.pulsecyber.co.uk

pulse cyber security

Europe & the GDPR Landscape

Total Fines: €466,677,568

May 2018 to Sept 2019 (16 months): 83

Oct 2019 to Mar 2020 (6 months): 147

Trend Pattern:

- 64% of all GDPR fines in the last 6 months

Number of fines per month (non-cumulative)

www.pulsecyber.co.uk

pulse cyber security

UK & Ireland

Doorstep Dispenseree (Health & Social Care)

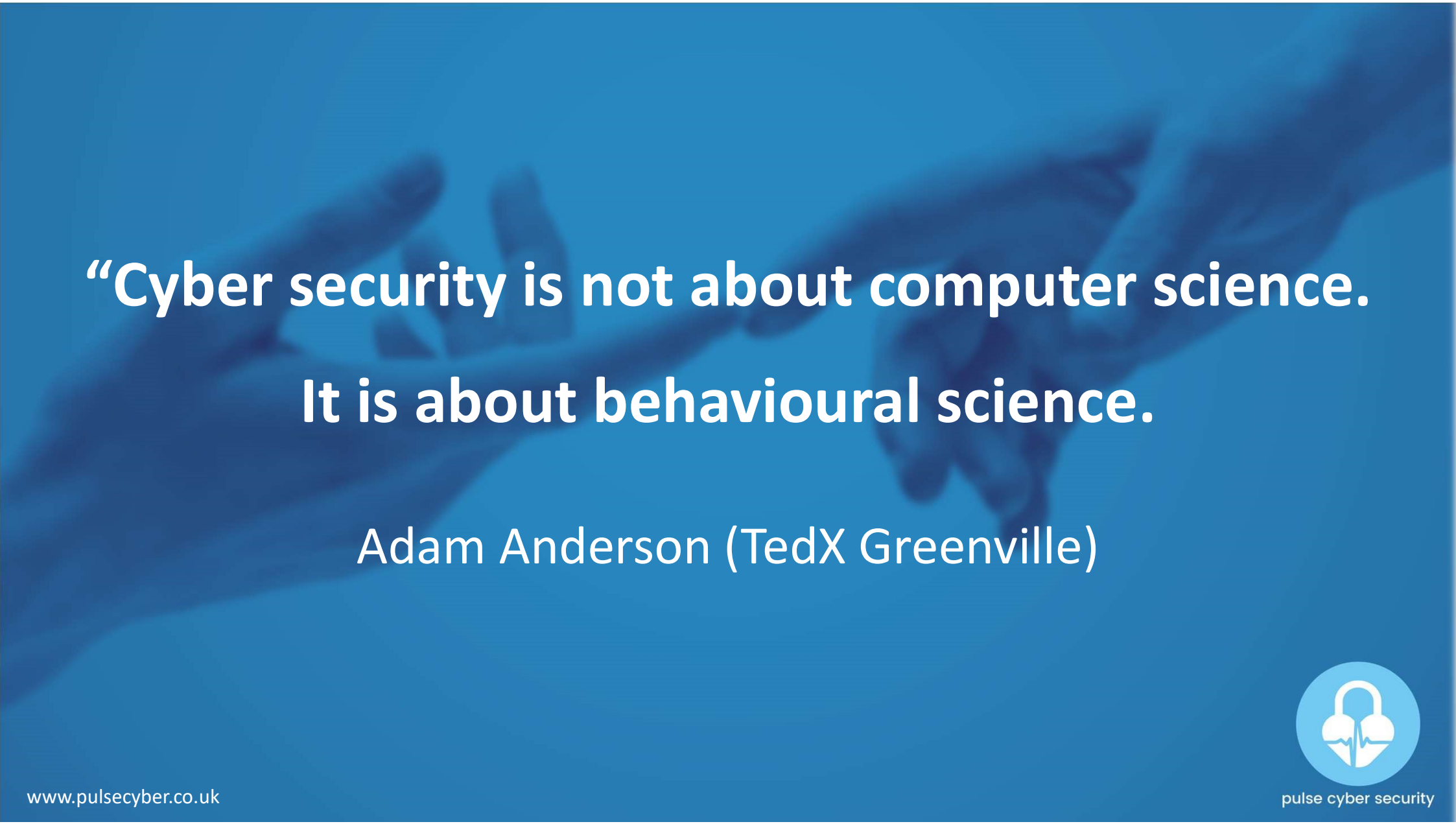
Fine: £275,000

Tusla - Child & Family Agency (Health & Social Care)

Fine: €75,000

www.pulsecyber.co.uk

pulse cyber security

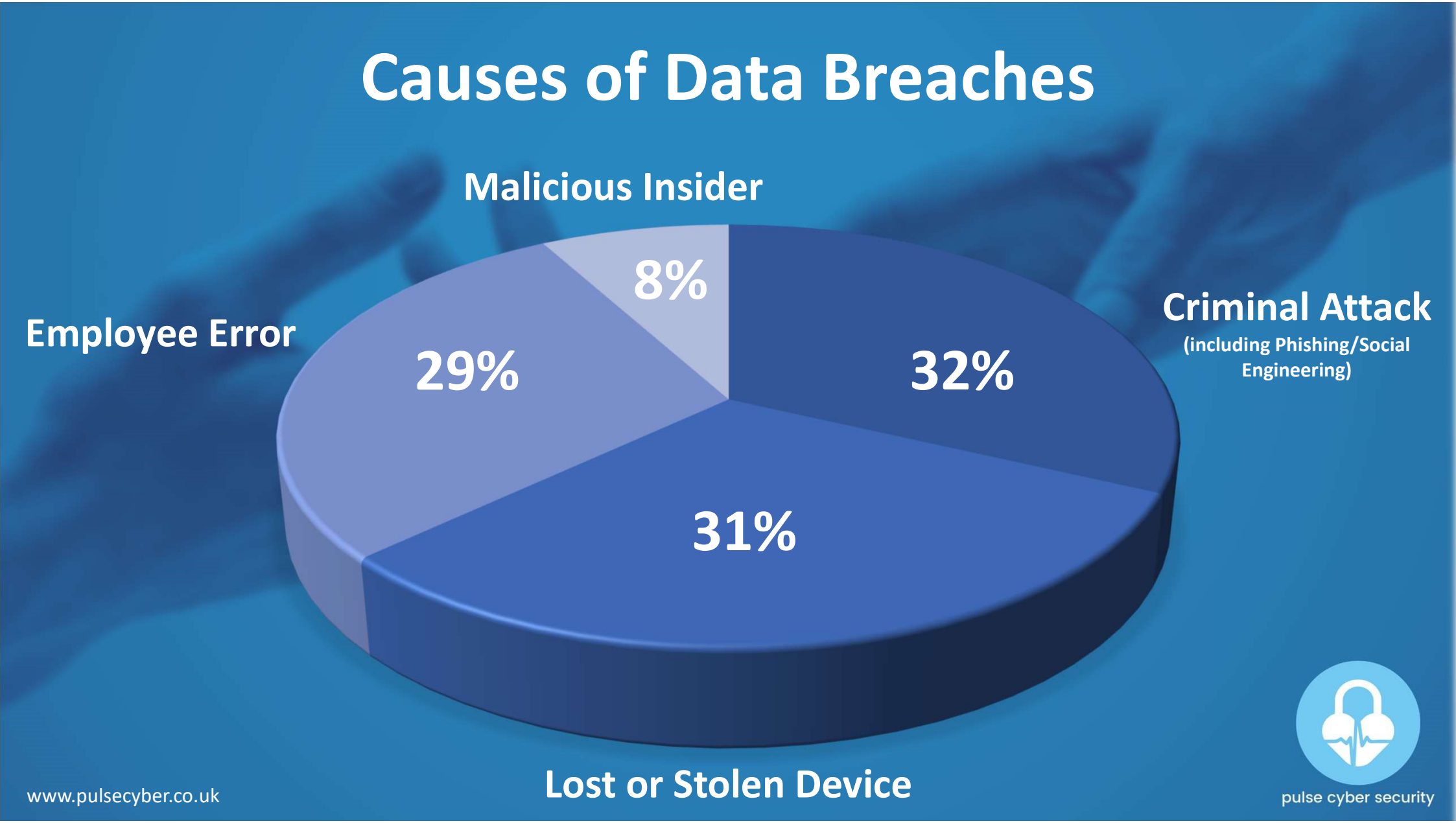

“Cyber security is not about computer science.
It is about behavioural science.
Adam Anderson (TedX Greenville)
www.pulsecyber.co.uk
pulse cyber security

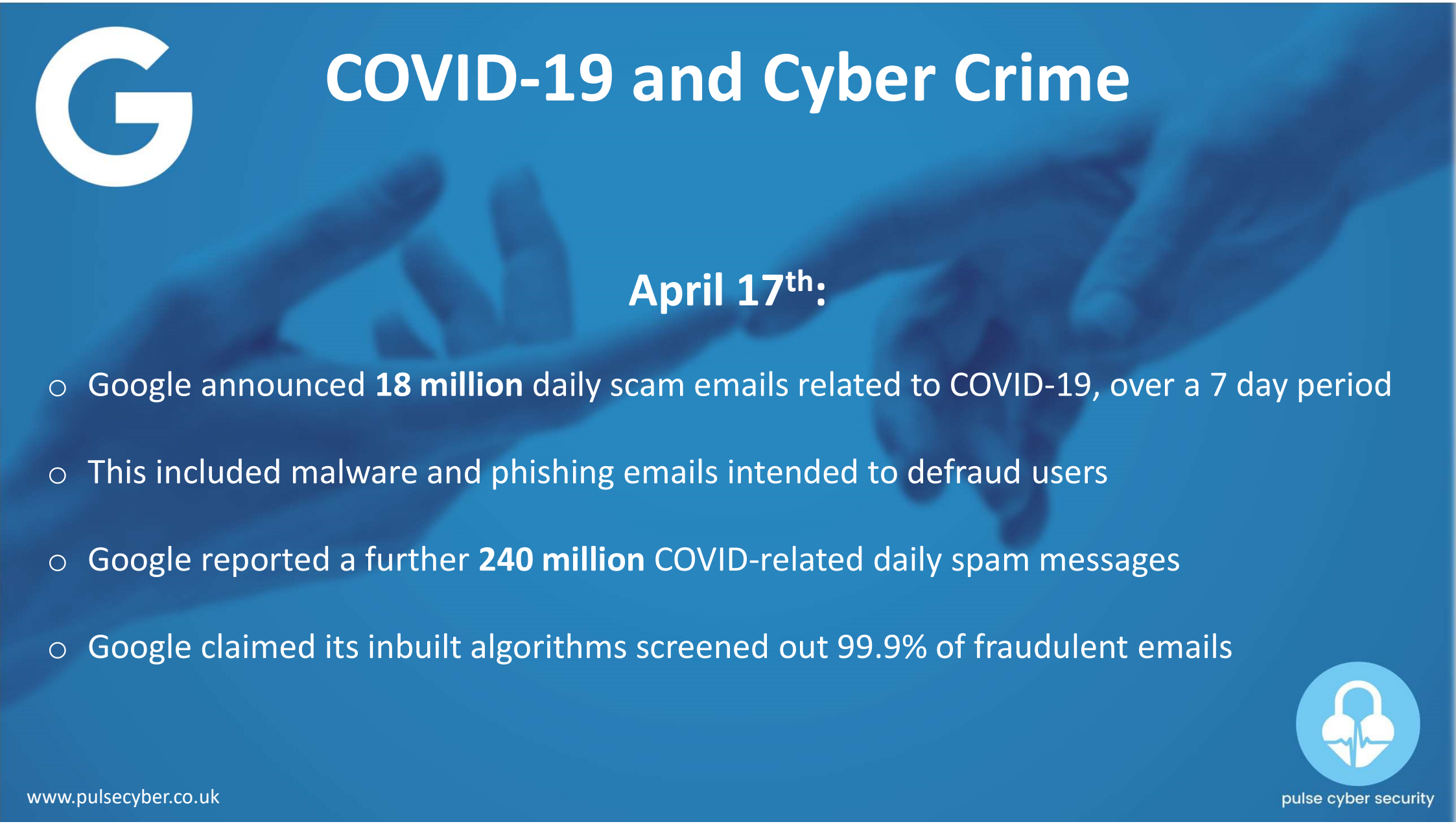
Prescribing the Wrong Treatment

- In cyber security, globally, we have a scenario where the standard solution to cyber crime is wrong
- Technology or computer science is not the (primary) cure to cyber crime
- People are
- If a doctor gives their unhealthy patient a list of medication it merely masks the symptoms to improve quality of life
- In many cases, changes of lifestyle can actually improve the health of the patient or (sometimes) make the symptoms go away altogether

www.pulsecyber.co.uk

pulse cyber security


Causes of Data Breaches
Malicious Insider
8%
Employee Error
29%
Criminal Attack
(including Phishing/Social Engineering)
32%
31%
Lost or Stolen Device
www.pulsecyber.co.uk
pulse cyber security



COVID-19 and Cyber Crime

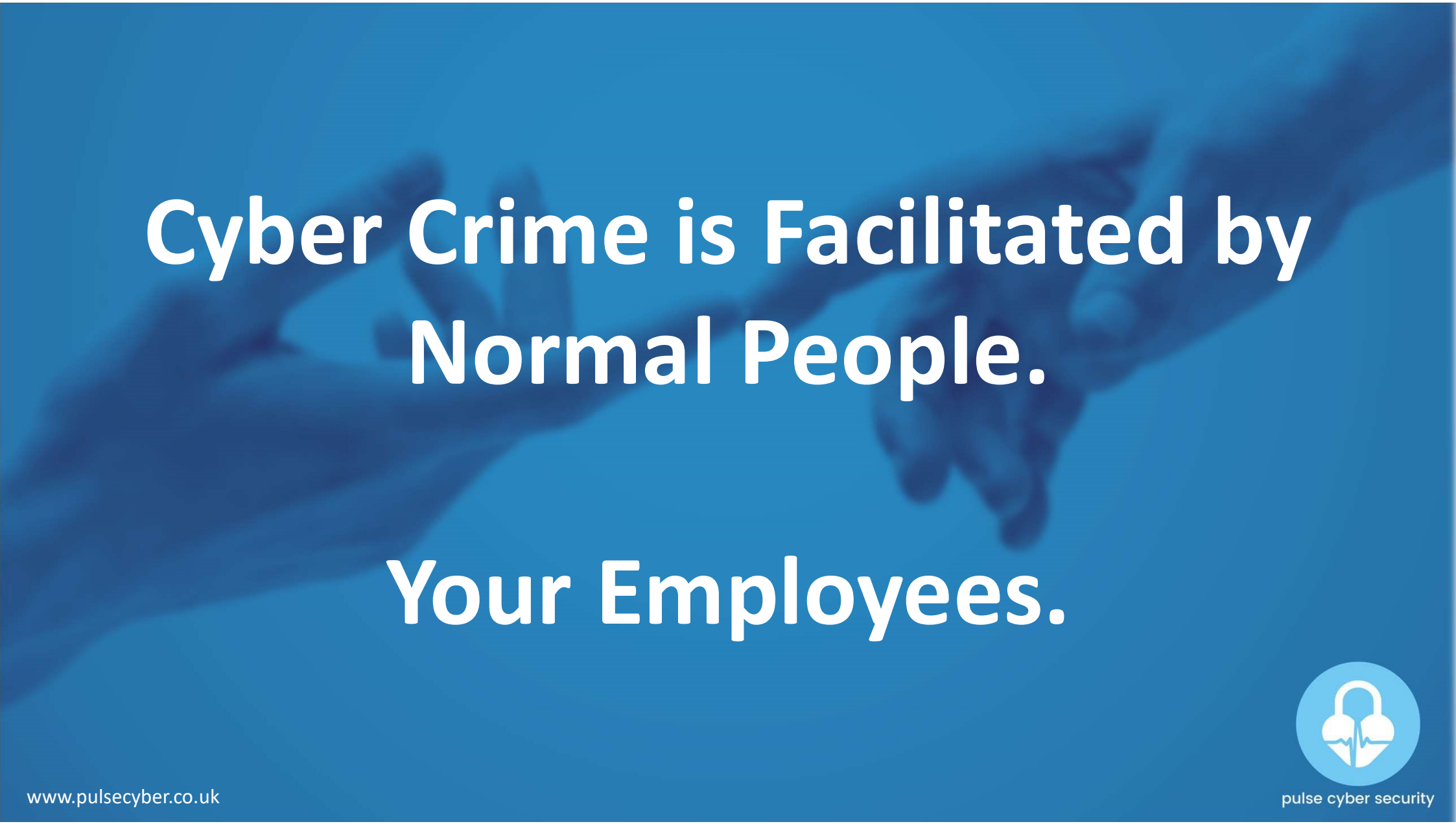
COVID-19
CYBER THREAT COALITION

April 15th:

- "Criminal groups and nation state actors are exploiting the COVID-19 pandemic to target healthcare systems and critical IT infrastructure all over the world"
- "Hundreds of thousands" of Fake Domains were set up mid-Feb to mid-March
- Approximately 5,000 domains were being registered DAILY
- Included World Health Organisation (WHO) & Nation States

www.pulsecyber.co.uk

pulse cyber security


Cyber Crime is Facilitated by Normal People.
Your Employees.
www.pulsecyber.co.uk
pulse cyber security

Cyber Crime Evolves Constantly

- Large amount of data that today is freely available in the social networks (Facebook etc)
- Easily machine-readable
- Advent of social networks & the new trends in sharing information changed the landscape
- The involvement of unforeseen experts in the planning of the attacks, such as:

Psychologists
Marketing
The Human Sciences

www.pulsecyber.co.uk

pulse cyber security

Research & Data (2019)

- 91% of attacks by sophisticated cyber criminals start through email (Mimecast)
- Emotional “lures” are entertainment, social, reward or recognition (PhishMe)
- Only 3% of malware tries to exploit an exclusively technical flaw (KnowBe4)
- The other 97% instead targets users through Social Engineering (KnowBe4)
- 15% of people successfully scammed, will be targeted again within the year (NerdSupport)
- £27,000 is the average cost for a UK business, as a result of email compromise (Neuways)

www.pulsecyber.co.uk

pulse cyber security

5 Key Risks of Home Working

1) Insecure Personal Devices

Home office networks are 3.5 times more likely than corporate networks to be infected by malware

2) Surge in COVID-19 related cyber attacks

Security researchers have identified an increase in business email compromise (BEC) and staff impersonation fraud, targeting IT teams, claiming they are having issues signing in remotely

3) Increased criminal activity targeted at VPN`s

Cyber criminals are targeting these services for vulnerabilities as a route to obtain entry into corporate networks

www.pulsecyber.co.uk

pulse cyber security

5 Key Risks of Home Working

4) Reliance on cloud-based tools

Not all cloud-based tools are secure, especially when security benefits such as password-entry are bypassed or switched off.

5) Lack of remote-working policies and procedures

Very few accountancy firms have a (tested) Business Continuity Plan.

With little time to develop appropriate working from home policies and procedures, many have been forced to deploy remote working arrangements without the necessary considerations for data security and privacy risks.

Compromised back-up processes, a lack of effective vulnerability scanning, patching and access control measures, and an overall reduction in information security control due to staff availability and/ or responsiveness.

www.pulsecyber.co.uk

pulse cyber security

Your People are the Key

- Human error is the number one cause of data breaches & data loss
- Responsible for **60 to 80%** of incidents
- By 2021, cyber crimes will cost **€5.5 trillion** worldwide
- Cybersecurity spending is on the rise; reaching **€115 billion** in 2019 (**€157 billion** by 2022)
- Only **52%** of employees receive GDPR or cyber security training once a year
- More than **50%** of businesses don't have the budget to recover from an aggressive attack

www.pulsecyber.co.uk

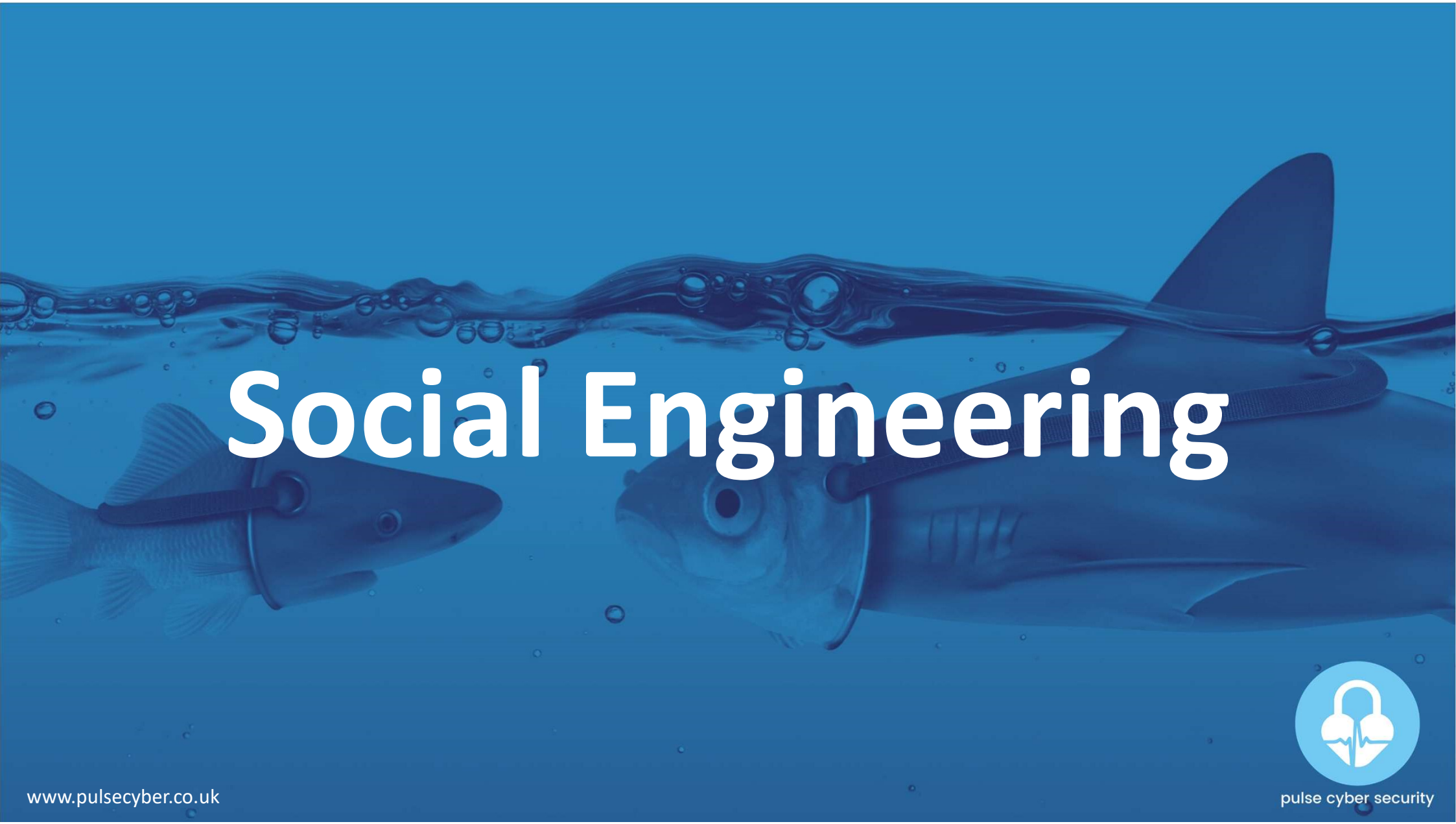
pulse cyber security

Kaspersky Research (2019)

- **33%** of incidents affecting infrastructure hosted by a third party were caused by phishing or other social engineering techniques
- **88%** of SME that experienced a data breach, said social engineering was part of the attack
- **90%** of business data breaches in the cloud happen due to social engineering attacks, which target customers' employees and **not** because of problems caused by their cloud providers

www.pulsecyber.co.uk

pulse cyber security



Definition

"The art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data."

Josh Fruhlinger
(CSO Online)

www.pulsecyber.co.uk

Phishing

Phishing is the most common type of social engineering attack that occurs today.

At a high level, most phishing scams endeavour to accomplish three things:

- Obtain personal information such as names, addresses and Social Security Numbers
- Use shortened or misleading links that redirect users to suspicious websites that host phishing landing pages
- Incorporate threats, fear and a sense of urgency in an attempt to manipulate the user into responding quickly

www.pulsecyber.co.uk

pulse cyber security

10 Social Engineering Tactics

- **Phishing:** tactics include deceptive emails, websites, and text messages to steal information
- **Spear Phishing:** email is used to carry out targeted attacks against individuals or businesses
- **Baiting:** an online and physical social engineering attack that promises the victim a reward
- **Whaling:** a highly targeted phishing attack - aimed at senior executives ("CEO Fraud")
- **Malware:** victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed

www.pulsecyber.co.uk

pulse cyber security

10 Social Engineering Tactics

- **Pretexting:** uses false identity to trick victims into giving up information
- **Quid Pro Quo:** relies on an exchange of information or service to convince the victim to act
- **Tailgating:** relies on human trust to give the criminal physical access to a secure building or area
- **Vishing:** urgent voice mails convince victims they need to act quickly to protect themselves from arrest or other risk
- **Water-Holing:** an advanced social engineering attack that infects both a website and its visitors with malware (lies in wait)

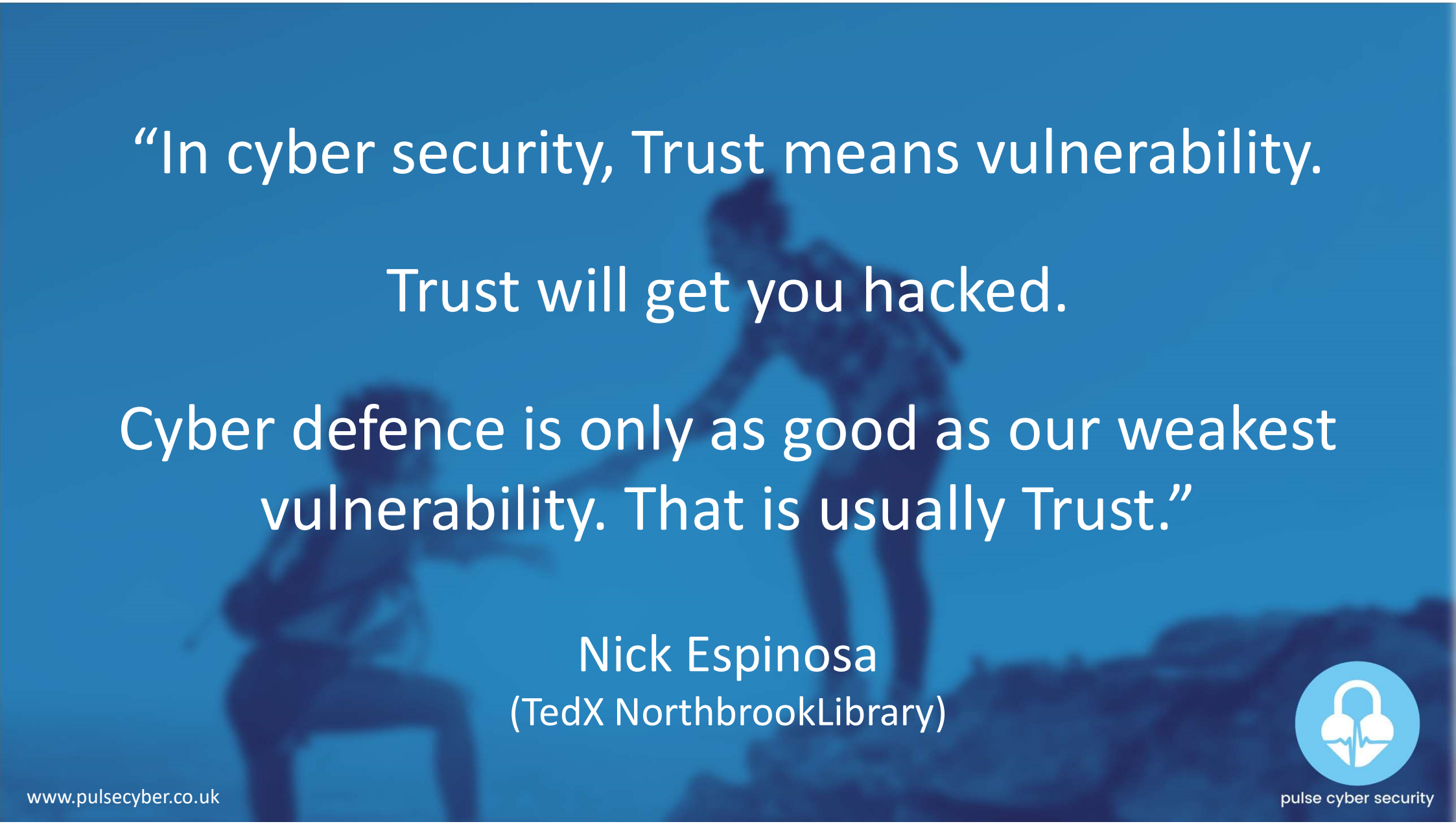
www.pulsecyber.co.uk

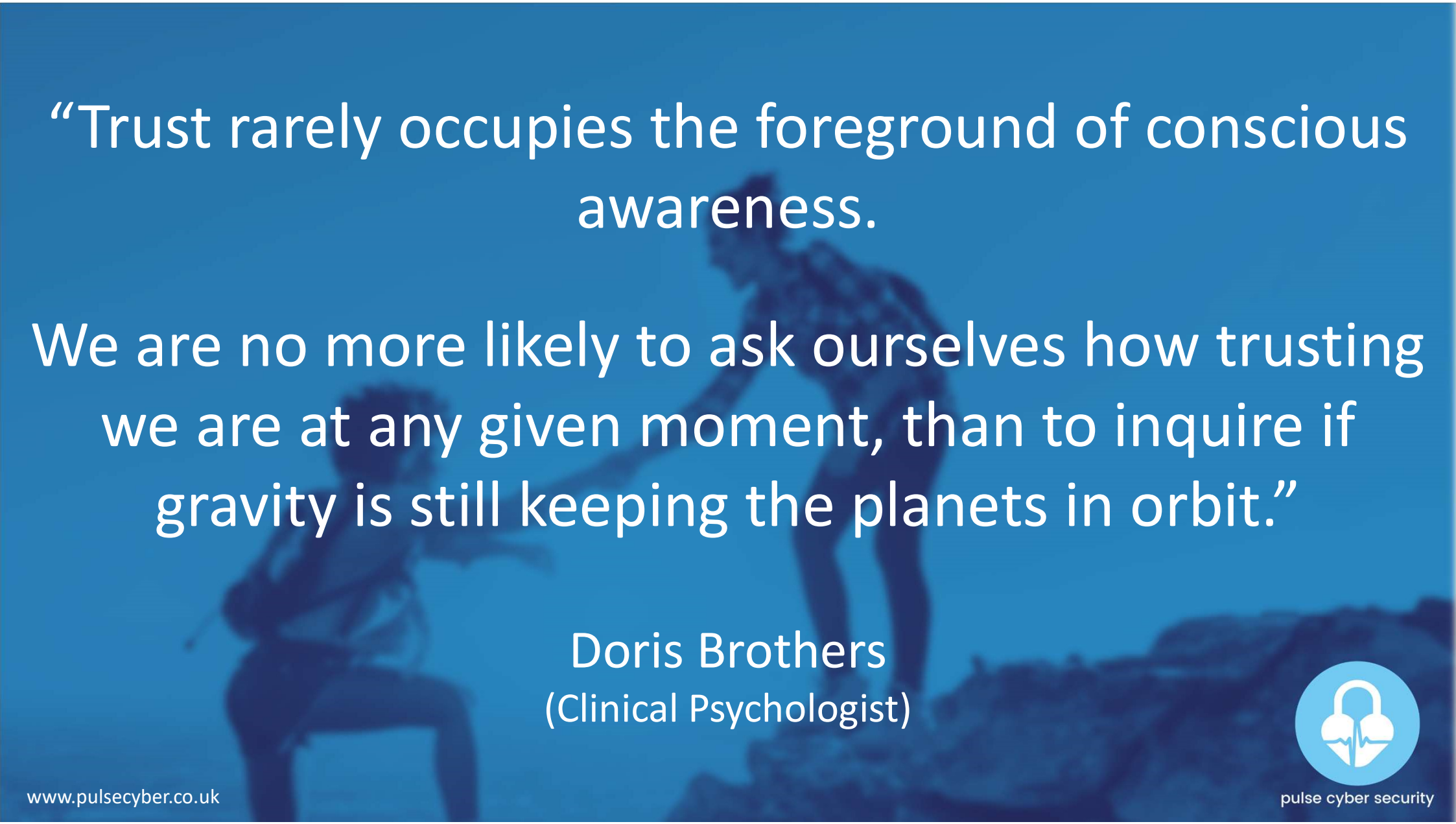
pulse cyber security

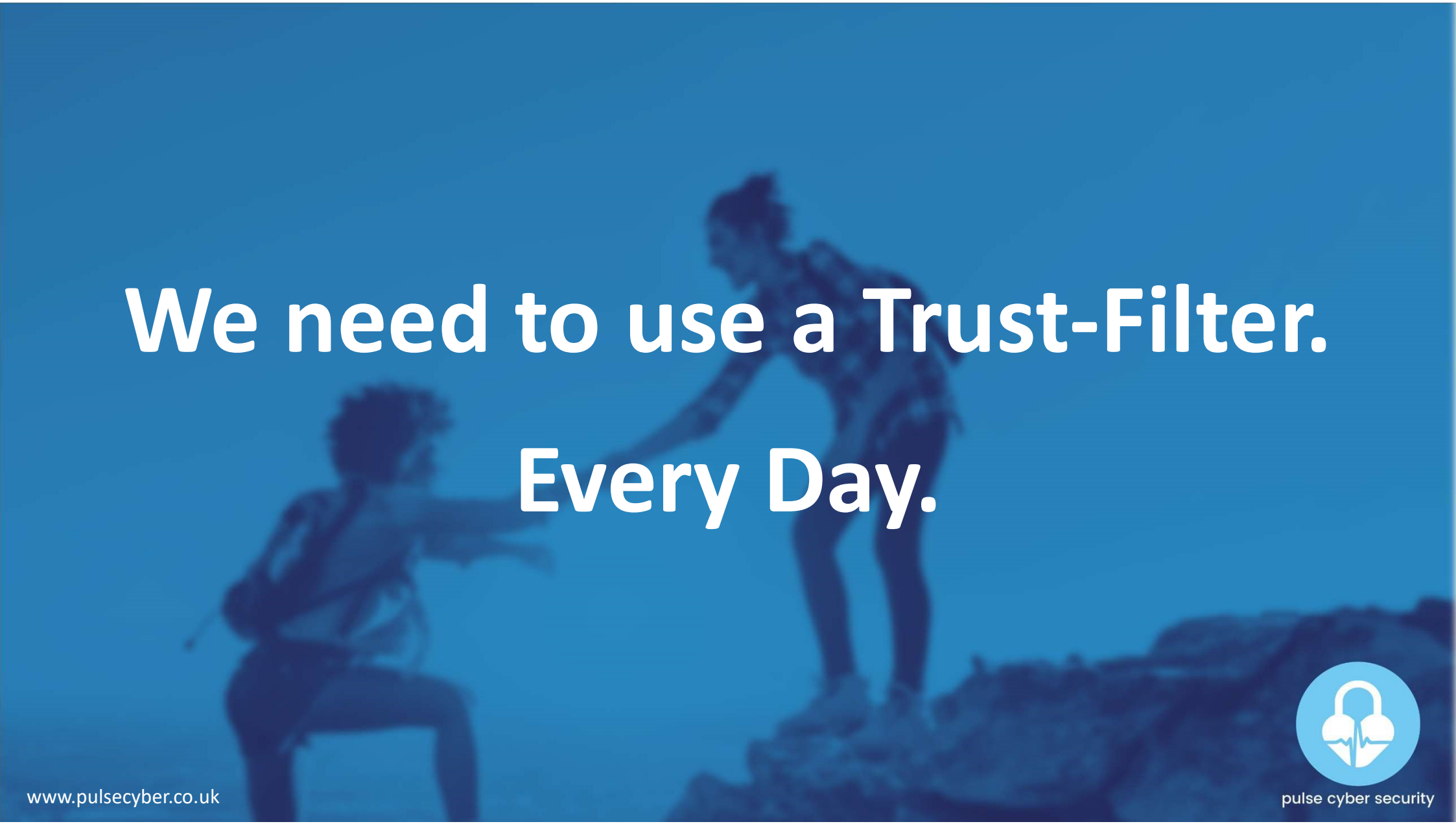
The Pulse Pyramid:

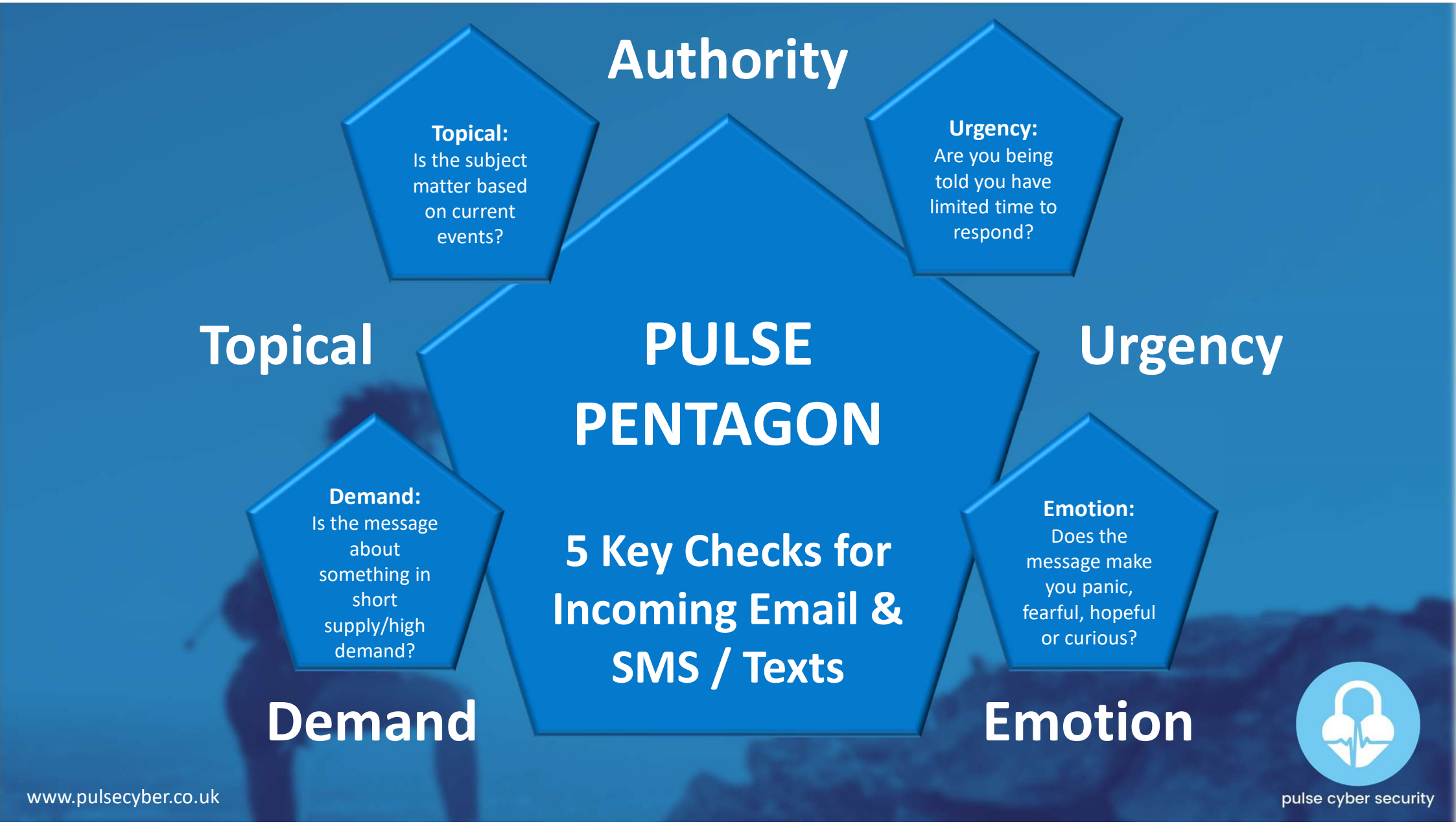
"A clever person solves a problem,
a wise person avoids it."

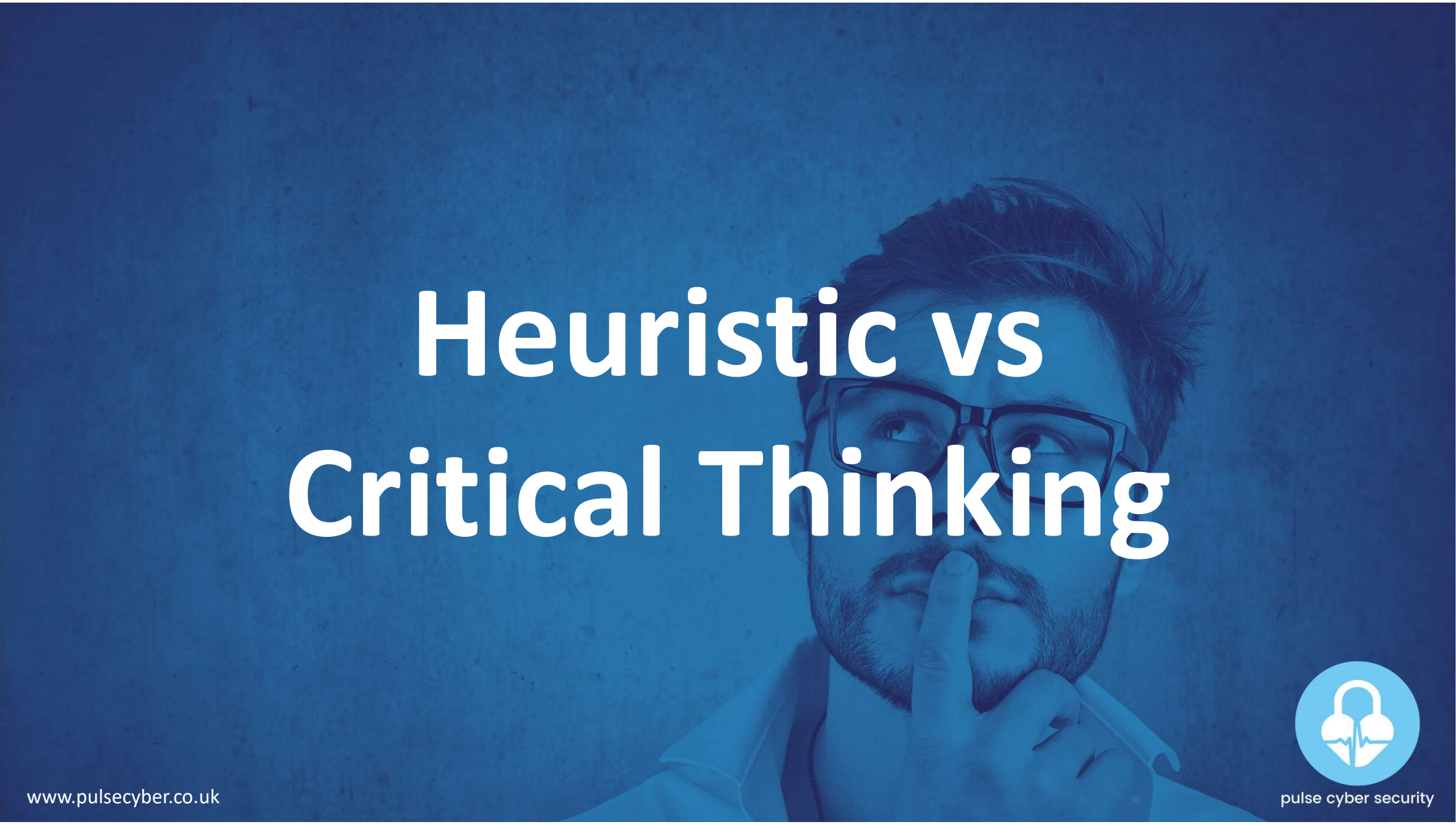
Albert Einstein

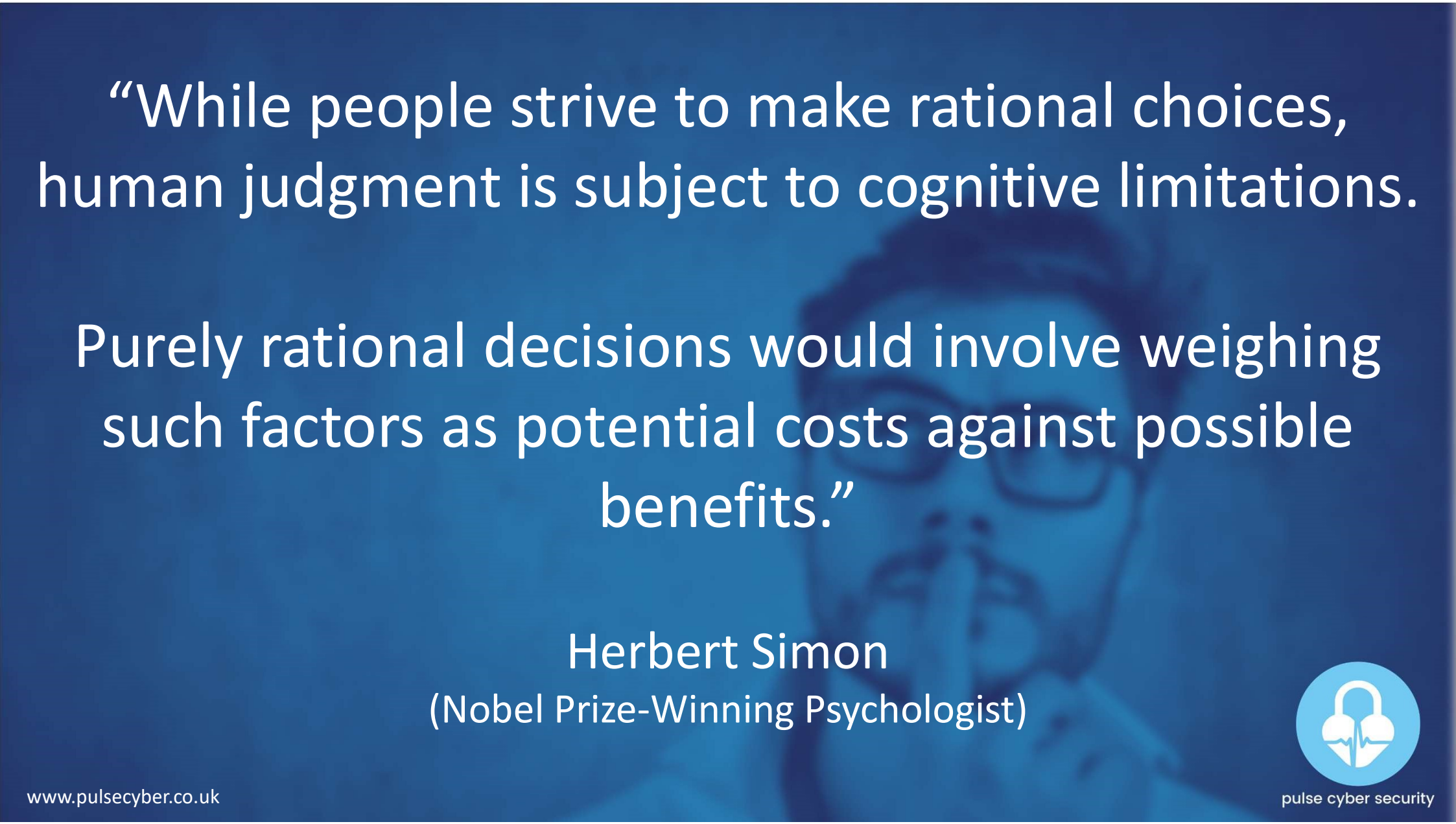

“In cyber security, Trust means vulnerability.
Trust will get you hacked.
Cyber defence is only as good as our weakest vulnerability. That is usually Trust.”
Nick Espinosa
(TedX NorthbrookLibrary)
www.pulsecyber.co.uk
pulse cyber security


“Trust rarely occupies the foreground of conscious awareness.
We are no more likely to ask ourselves how trusting we are at any given moment, than to inquire if gravity is still keeping the planets in orbit.”
Doris Brothers
(Clinical Psychologist)
www.pulsecyber.co.uk
pulse cyber security



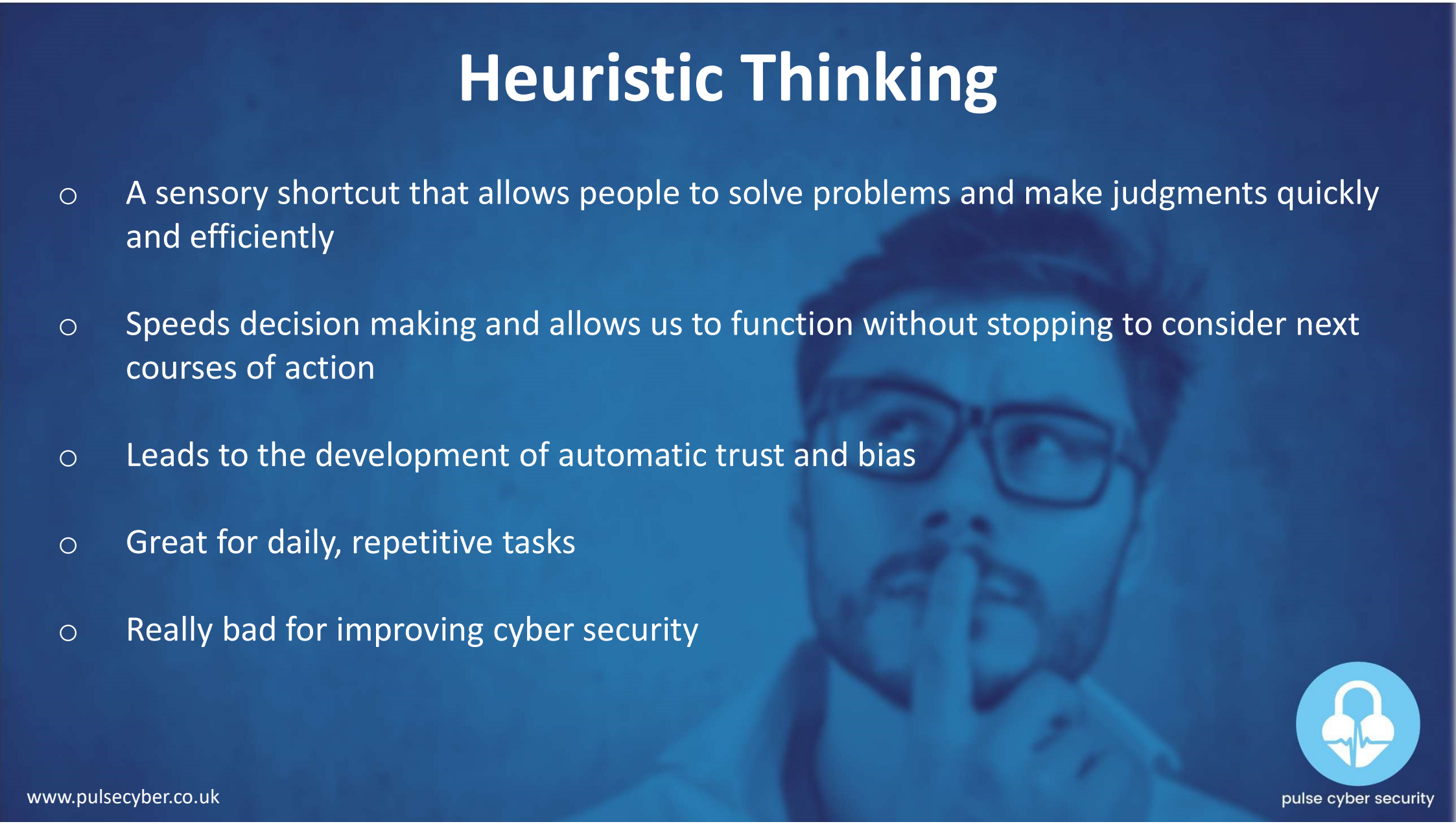

Authority
Topical:
Is the subject matter based on current events?
Urgency:
Are you being told you have limited time to respond?
Topical
PULSE PENTAGON
Urgency
Demand:
Is the message about something in short supply/high demand?
5 Key Checks for Incoming Email & SMS / Texts
Emotion:
Does the message make you panic, fearful, hopeful or curious?
Demand
Emotion
www.pulsecyber.co.uk
pulse cyber security


Heuristic vs
Critical Thinking
www.pulsecyber.co.uk
pulse cyber security


“While people strive to make rational choices, human judgment is subject to cognitive limitations.
Purely rational decisions would involve weighing such factors as potential costs against possible benefits.”
Herbert Simon
(Nobel Prize-Winning Psychologist)
www.pulsecyber.co.uk
pulse cyber security

Heuristic Thinking

- A sensory shortcut that allows people to solve problems and make judgments quickly and efficiently
- Speeds decision making and allows us to function without stopping to consider next courses of action
- Leads to the development of automatic trust and bias
- Great for daily, repetitive tasks
- Really bad for improving cyber security

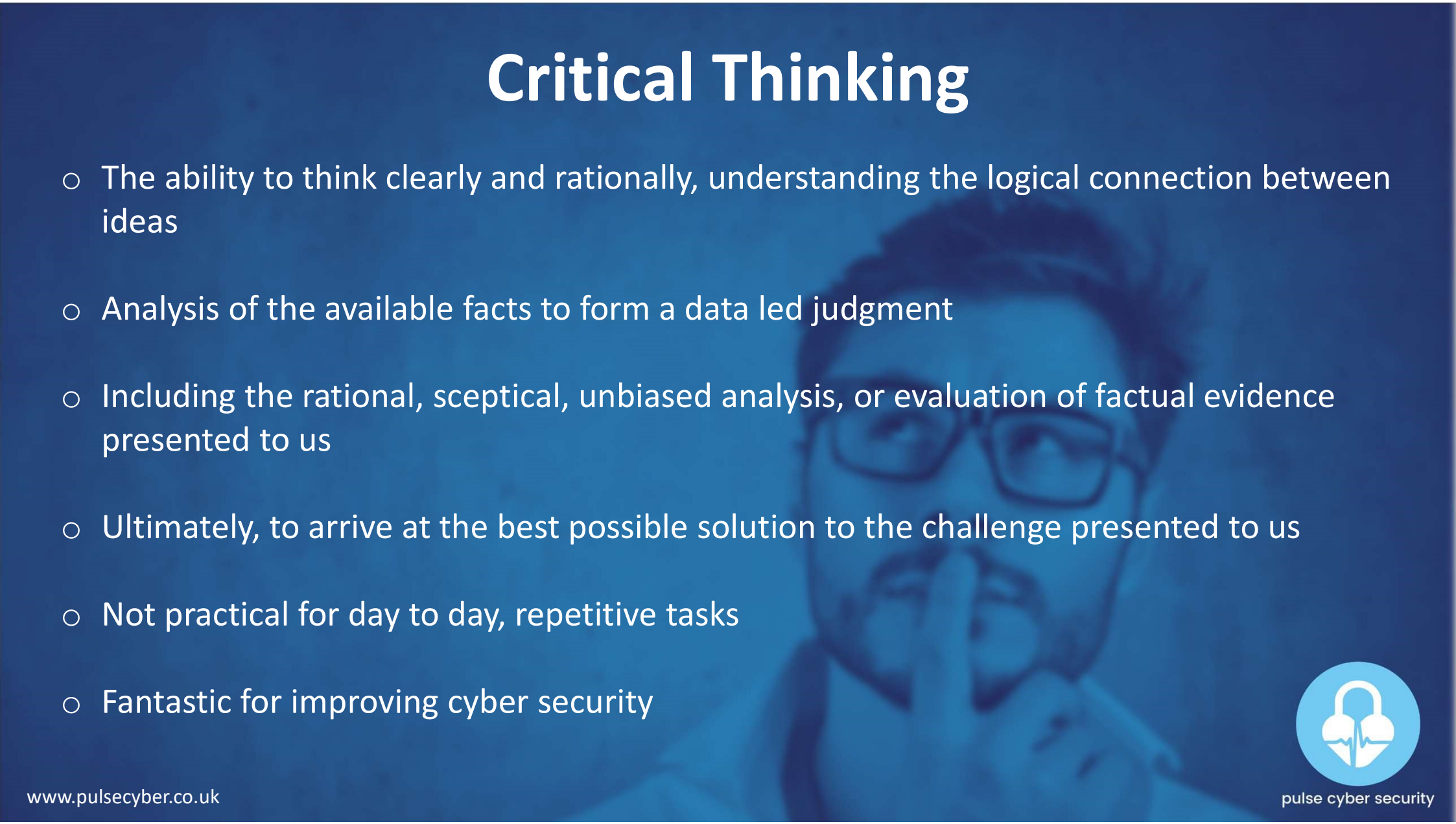


www.pulsecyber.co.uk

pulse cyber security

Critical Thinking

- The ability to think clearly and rationally, understanding the logical connection between ideas
- Analysis of the available facts to form a data led judgment
- Including the rational, sceptical, unbiased analysis, or evaluation of factual evidence presented to us
- Ultimately, to arrive at the best possible solution to the challenge presented to us
- Not practical for day to day, repetitive tasks
- Fantastic for improving cyber security



www.pulsecyber.co.uk

pulse cyber security

pulse cyber security

Questions

hello@pulsecyber.co.uk

www.pulsecyber.co.uk

@PulseCyberSec