Human Firewall:
Your People and Their Role

MOORE ClearComm

Today's Webinar

- Human Science and Cyber Crime
- Social Engineering
- Trust = Vulnerability
- Employee Engagement
- Building a Human Firewall
- Opportunity for Questions

3 Important Facts to Keep in Mind about Employee Awareness:

1) Just because I am **AWARE**, does not mean that I **CARE**
2) If you try to work against human nature, you will fail
3) What employees **DO** is more important than what they **KNOW**

Perry Carpenter (Chief Strategy Officer, KnowBe4)

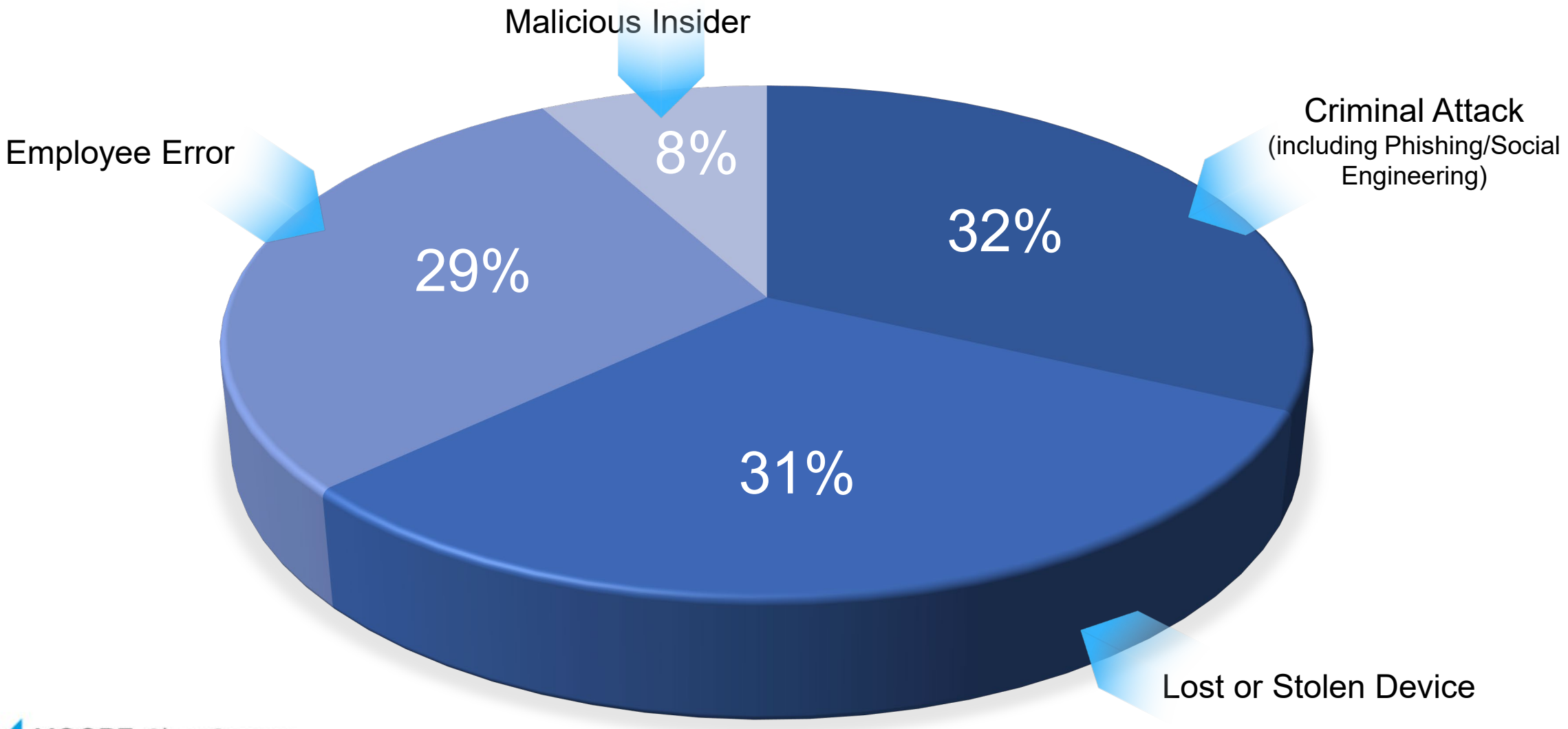
Today`s Panellists:

Bob Harper and Paras Shah

MOORE ClearComm

Human Science and Cyber Crime

Causes of “Human” Data Breaches (2023)



MOORE ClearComm

Causes of “Human” Data Breaches (2023)

- 91% of attacks by sophisticated cyber criminals start through email
- Emotional “lures” are entertainment, social, reward or recognition
- Only 3% of malware will attempt to exploit a technical flaw
- The other 97% targets users through Social Engineering
- Phishing will be the most likely method applied in these attacks
- Your employees are not your weakest link…
- …but they are the most likely point of attack

MOORE ClearComm

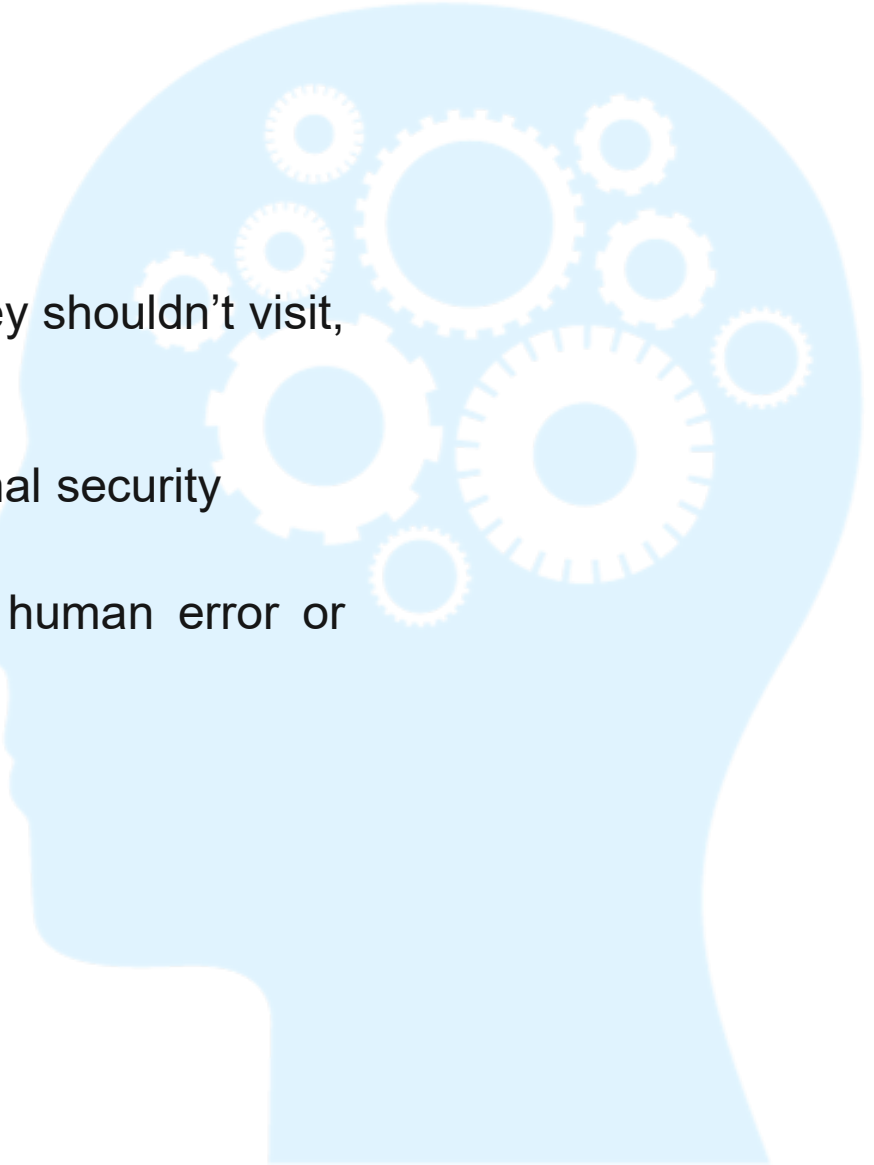
Social Engineering

Social Engineering Defined: IBM

- Sometimes referred to as ‘human hacking”
- Manipulates people into sharing information they shouldn’t share
- They download software they shouldn’t download, visit websites they shouldn’t visit, send money to criminals, or
- Make other mistakes that compromise their personal or organisational security
- Social engineering uses psychological manipulation and exploits human error or weakness

Rather than…

- Technical or digital system vulnerabilities



MOORE ClearComm

Phishing

- The most common type of social engineering attack that occurs today.
- Phishing is a cybercrime method that was first recorded in 1987
- Target(s) are contacted by email, telephone or text message, by someone posing as a legitimate institution
- They aim to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords
- Phishing is the most common type of cybercrime in 2024
- The FBI's Internet Crime Complaint Center reports more incidents of phishing than any other type of computer crime

Trust = Vulnerability

Trust = Vulnerability

- Social engineering is a malicious technique that relies on a single “key” for its success - **Trust**
- We are programmed to trust from a very young age
- “If a child successfully develops trust, they will feel safe and secure in the world” (Erik Erikson, Psychologist)
- According to Erikson`s theory, a parent figure shapes their child's perception and future relationships
- Children who learn to trust caregivers in infancy will be more likely to form trusting relationships with others throughout the course of their lives
- This manifests into adult life and the workplace
- Cyber criminals use this to their advantage

Three Truths about Human Nature (BJ Fogg)

We are Lazy

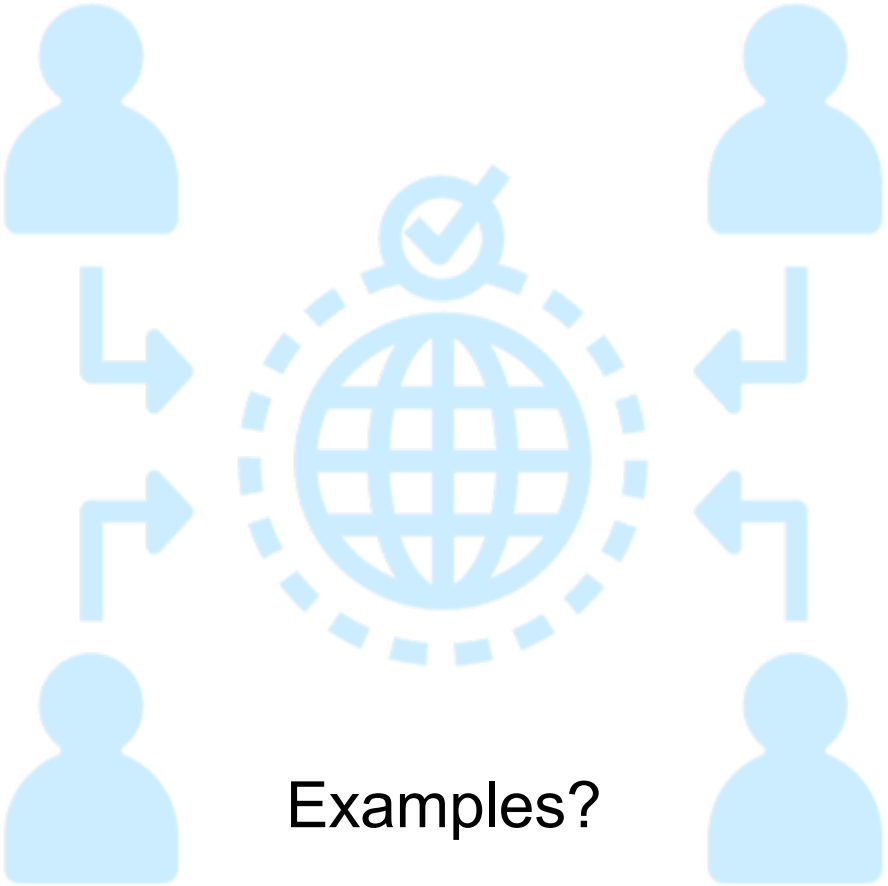
We are Creatures of Habit

We are Social

MOORE ClearComm

Red Team Case-Study: “Testing Trust”

- Red Teams: tasked with the objective of subjecting an organisation’s plans, programmes, ideas, assumptions and physical defences - to rigorous analysis and challenge
- Concept emerged in the early 1960s
- Technical red teaming = testing the logical network security of an organisation by attempting to compromise their digital assets
- Physical red teaming = testing the physical security controls of an organization`s assets, such as offices or data centers. Uses social engineering techniques and penetration testing tools attempting to access sensitive (or high-risk) areas



Examples?

Employee Engagement

Employee Engagement: Driving Secure Behaviours

Utrecht University definition: “a psychological state experienced by employees” based on:

- ✓ Vigour: energy, resilience and effort
- ✓ Dedication: enthusiasm, inspiration and pride
- ✓ Absorption: concentration and being engrossed in one’s work

MacLeod Review: “How to Enable Employee Engagement”:

Leadership that gives a “strong strategic narrative about the organisation”

Line Managers who motivate, empower and support their employees

Employee Voice throughout the organisation, to involve employees in decision making

Organisational Integrity with values reflected in actual organisational culture

Building a Human Firewall

Human Firewall

"A commitment of a group of employees to follow best practice, in order to prevent (and report) any data breaches or suspicious activity."

- ✓ A structured (ongoing) education for your people
- ✓ Focused on cyber threats and privacy risks
- ✓ Works like a technical firewall
- ✓ Designed to block outside threats and create a barrier
- ✓ Fosters an environment of mutual trust
- ✓ Shared goal: protect the organisation

MOORE ClearComm

Human Firewall: The Five Building Blocks

1) Cyber Security Culture: Starts at the Top
2) Encourage Employees to “Care” about Cyber Security
3) Build Constant Awareness & Knowledge*
4) Encourage Employees to Challenge & Question
5) Measure & Monitor Performance

Awareness alone will not drive Change.

Knowledge is not the same as Behaviour.

MOORE ClearComm

QUESTIONS

bob@agendali.com

paras.shah@mooreclear.com

richard.jackson@mooreclear.com

Our next webinar

“Cyber Essentials: Proving You Take Security Seriously”

Date: Thursday 29th February 2024
Time: 10.00am-11.00am

Moore ClearComm Speakers:

- Rich Jackson, Strategic Business Manager (Moore ClearComm
- Maritz Cloete Director of Cyber Services, Moore ClearComm
- Paras Shah, Cyber Security Consultant Moore ClearComm

Location: Zoom

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

MOORE ClearComm

Moore ClearComm
9 Appold Street
London
EC2A 2AP
t: +44 (0)20 45821983

www.mooreclear.com

Any assumptions, opinions and estimates expressed in the Information contained in this content constitute the judgment of Moore Kingston Smith LLP and/or its associated businesses as of the date thereof and are subject to change without notice. This Information does not constitute advice and professional advice should be taken before acting on any information herein. No liability for any direct, consequential, or other loss arising from reliance on the Information is accepted by Moore Kingston Smith LLP, or any of its associated businesses.

Moore Kingston Smith LLP is regulated by the Institute of Chartered Accountants in England & Wales. Certain activities of the LLP and/or its associated businesses are authorised and regulated by the Financial Conduct Authority or the Solicitors Regulation Authority. More details are available on our website at www.mooreks.co.uk © Moore Kingston Smith LLP.

MOORE ClearComm