CISO's As Digital Leaders With Security Culture as Their Top Priority

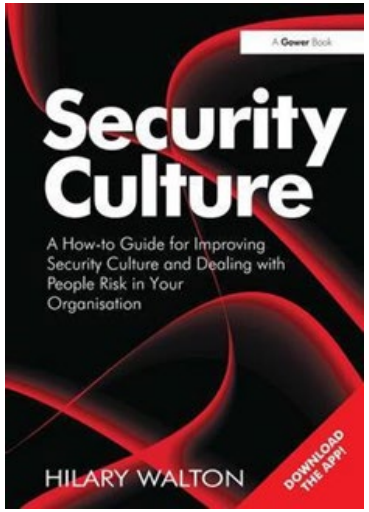
Hilary Walton @HilsWalton

CISO Kordia Group | Director | Psychology | Author & Podcaster | Passionate about Security and Digital Culture ideas

kordia®

Hilary Walton @HilsWalton

kordia



Institute of DIRECTORS NEW ZEALAND

Technology and processes alone won't hold back cybercriminals...

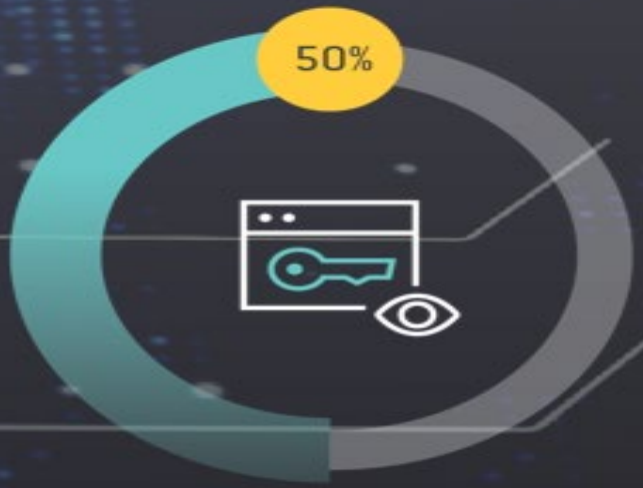
your EMPLOYEES are the first line of defence against cyber-attacks.

BUT

2 IN 5

do not have policies and training in place

TO HELP PREVENT CYBER BREACHES



AND

ONLY ½

are confident their employees understand the

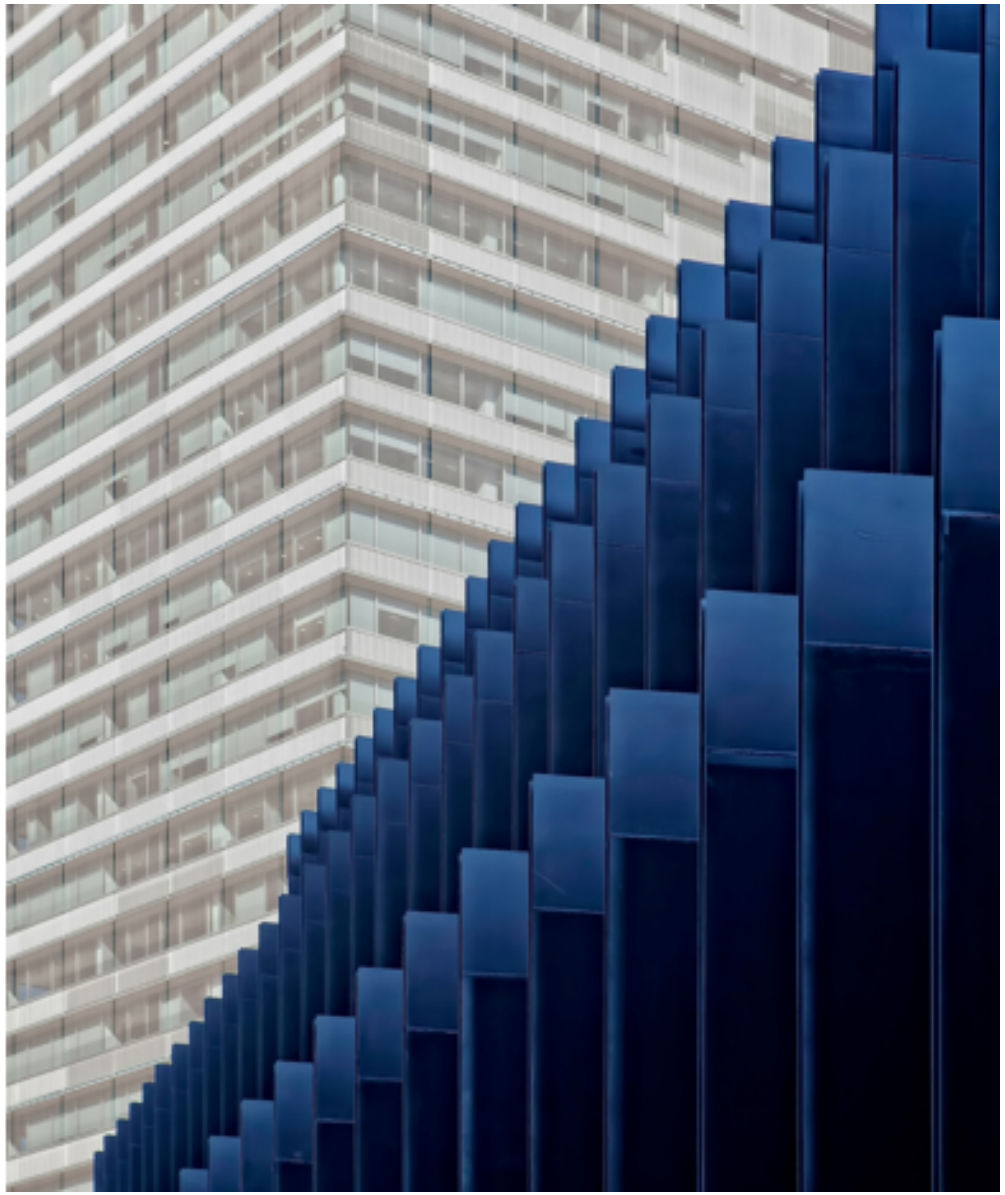
IMPORTANCE OF GOOD PASSWORD PRACTICE.

POWERED BY KORDIA

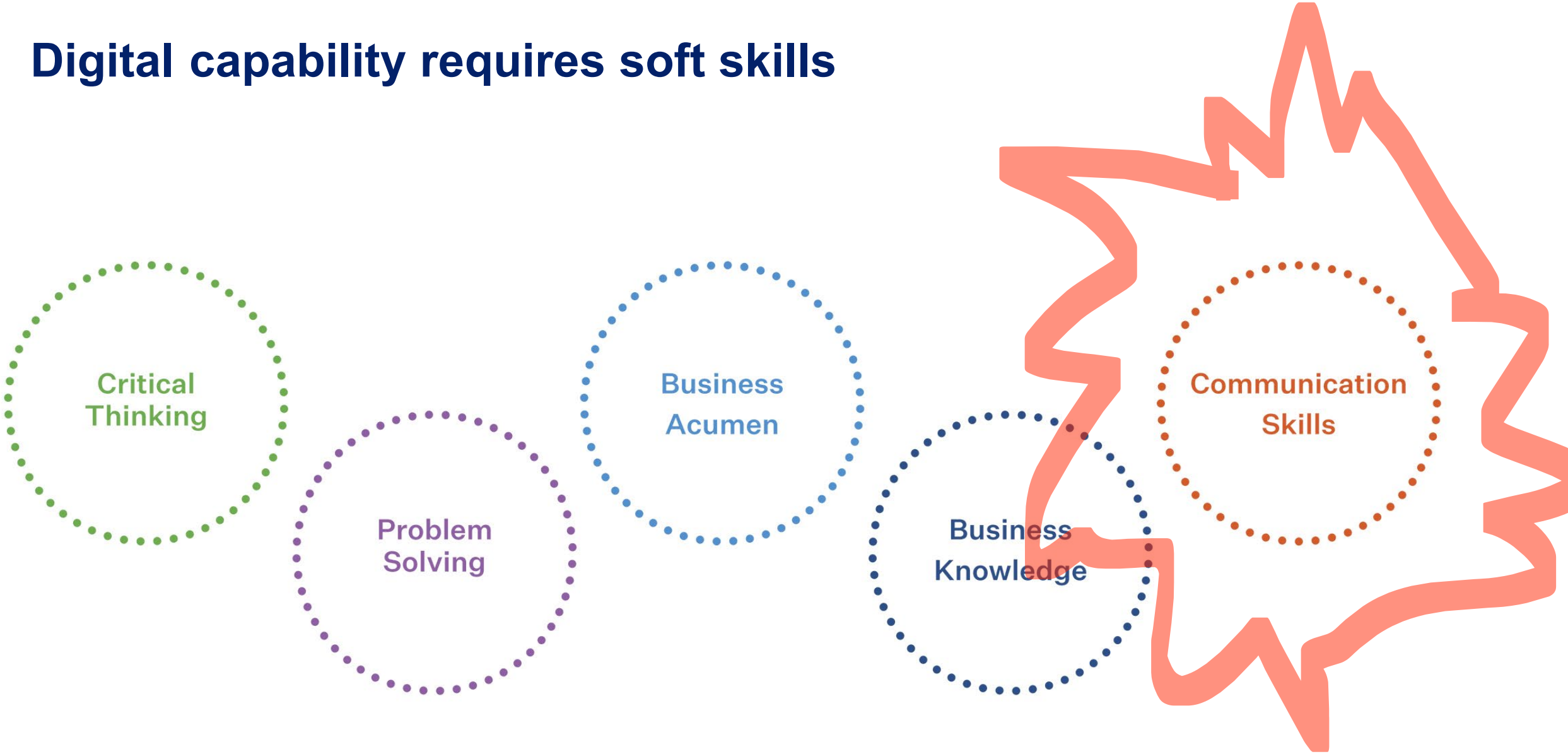
Its more than just awareness, we have to change culture and behaviour to reduce people risk

Leadership in the digital age

Leaders need to **empower** their teams to work with **autonomy** and freedom, and **to take decisions**. Organisations need to create leaders at all levels by building **participation** and **accountability**. They need to **learn from people** working on the ground, take inputs and **trust** them. Every member of the team should be **encouraged to contribute** ideas, insights and knowledge for achieving **shared goals.**



Digital capability requires soft skills



Digital requires new leadership and behaviours because . . . the **biggest cultural and business model shift** is happening right now . . . a shift to a more digital culture and ways of working.

What are some ways technology and the internet are changing the way we **think**, make **decisions**, **behave**, **interact** and **communicate**?

. . . Discuss ☺

Digital Shifts - Make no mistake!

2022

Your mobile phone is the TV

1950's

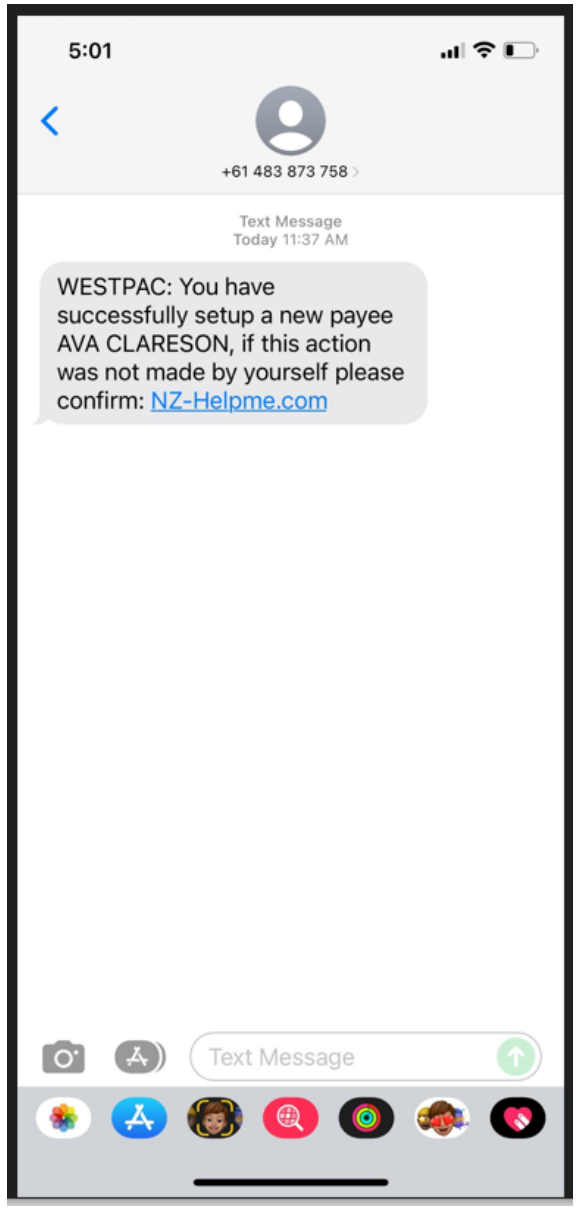
Your TV is the radio

Text-Phishing (SMISHING)

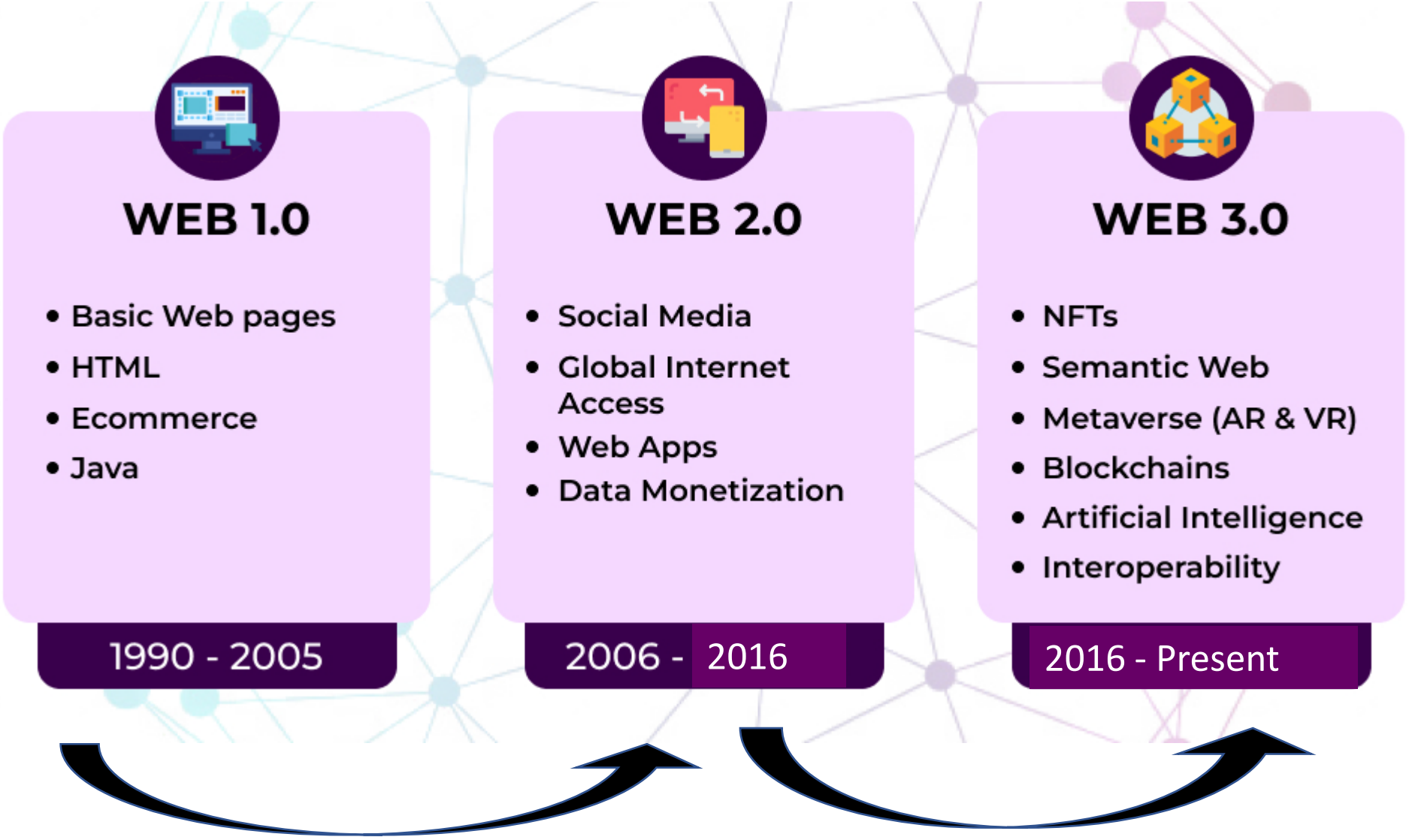
As a variant of phishing, victims are deceived into giving sensitive information to a disguised attacker.

SMS phishing can be assisted by malware or fraud websites. It occurs on many mobile text messaging platforms, including non-SMS channels like data-based mobile messaging apps.

- COVID-19 smishing
- Financial services smishing
- Gift smishing
- Invoice or order smishing
- Customer support smishing



Another Significant Digital Shift
- Amongst other things, this affects how you communicate security



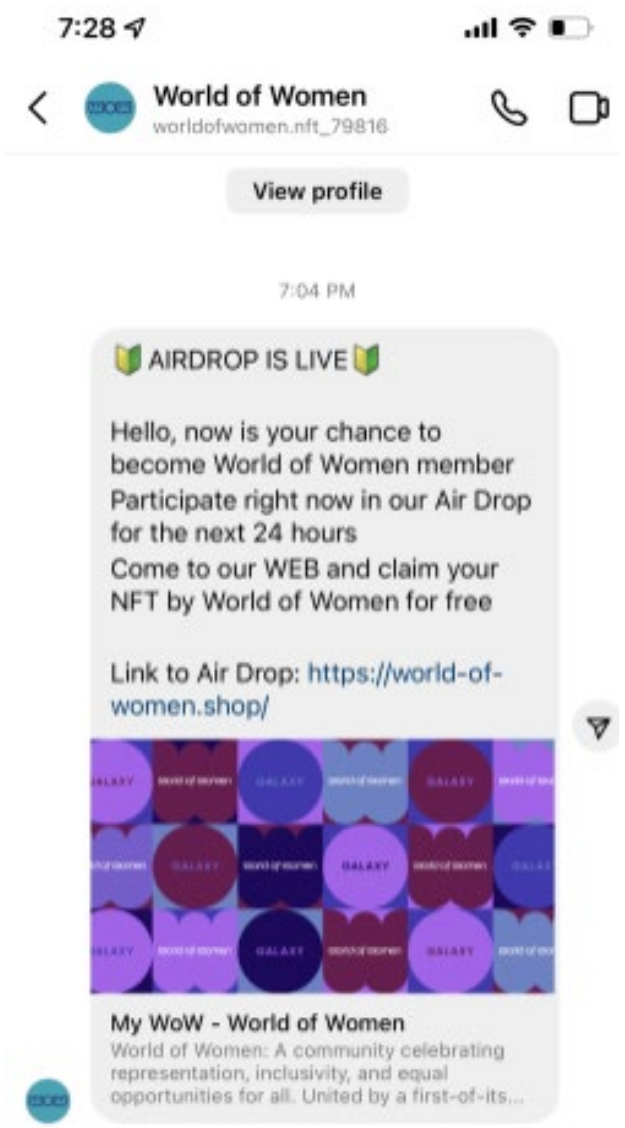
Web3, Crypto and Blockchain Phishing Scams

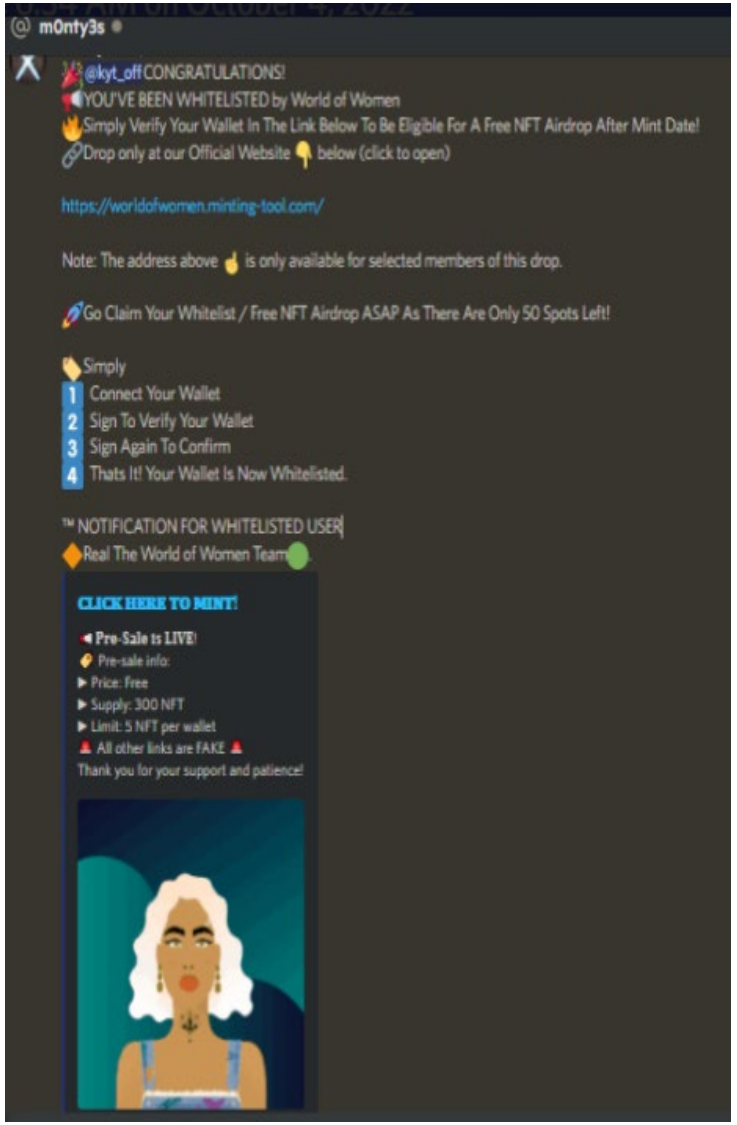
- New playground for opportunistic cybercriminals

People will always be vulnerable to manipulation.

Blockchain empowers criminals to remain anonymous and stolen funds are usually irretrievable.

- Malicious AirDrops
- Seed Phrase Phishing
- Ice Phishing - clickjacking
- Fraudulent emails, websites and social media accounts



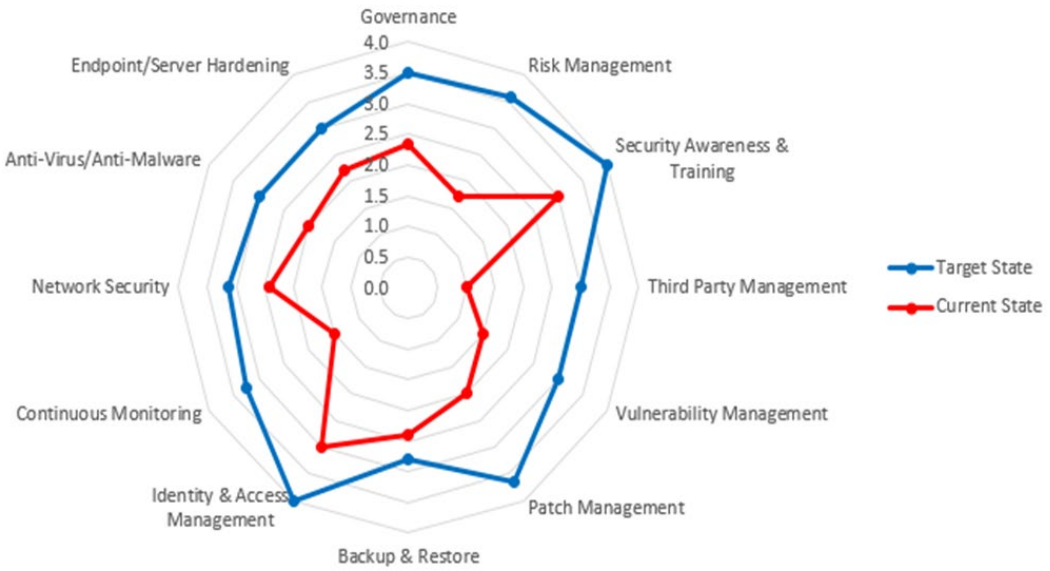


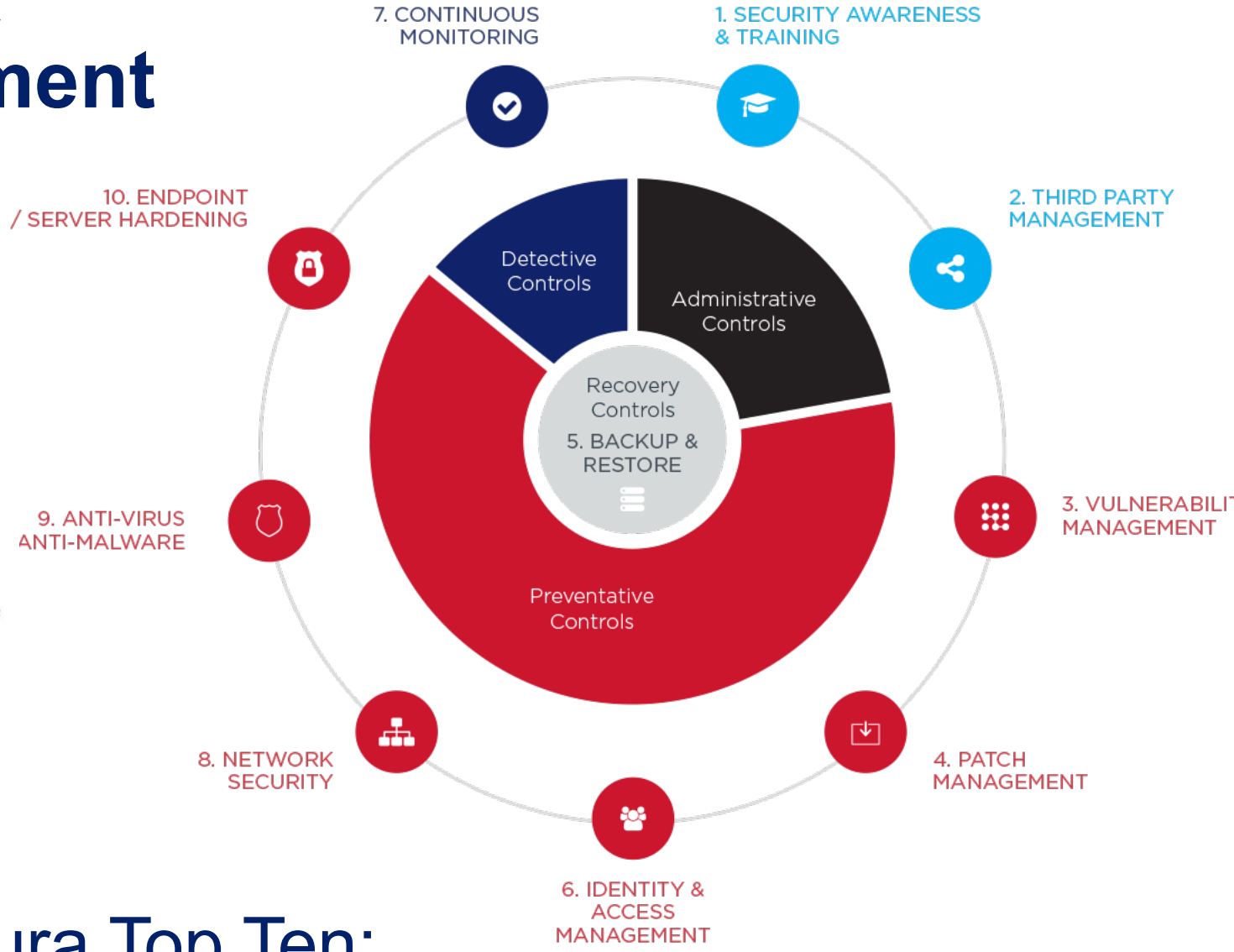
Digital is Everyday Life
– Being a Digital Native Does Not Mean You Are Cyber Smart

Four CISO Leadership & Communication Strategies to build security culture and behaviours

kordia®

#1 Treat Security as a Continuous Improvement Exercise.





Aura Top Ten:

Critical Controls & Mitigation Strategies

#2 Use Security Culture Change Management Mechanisms

1. Level of Management Commitment

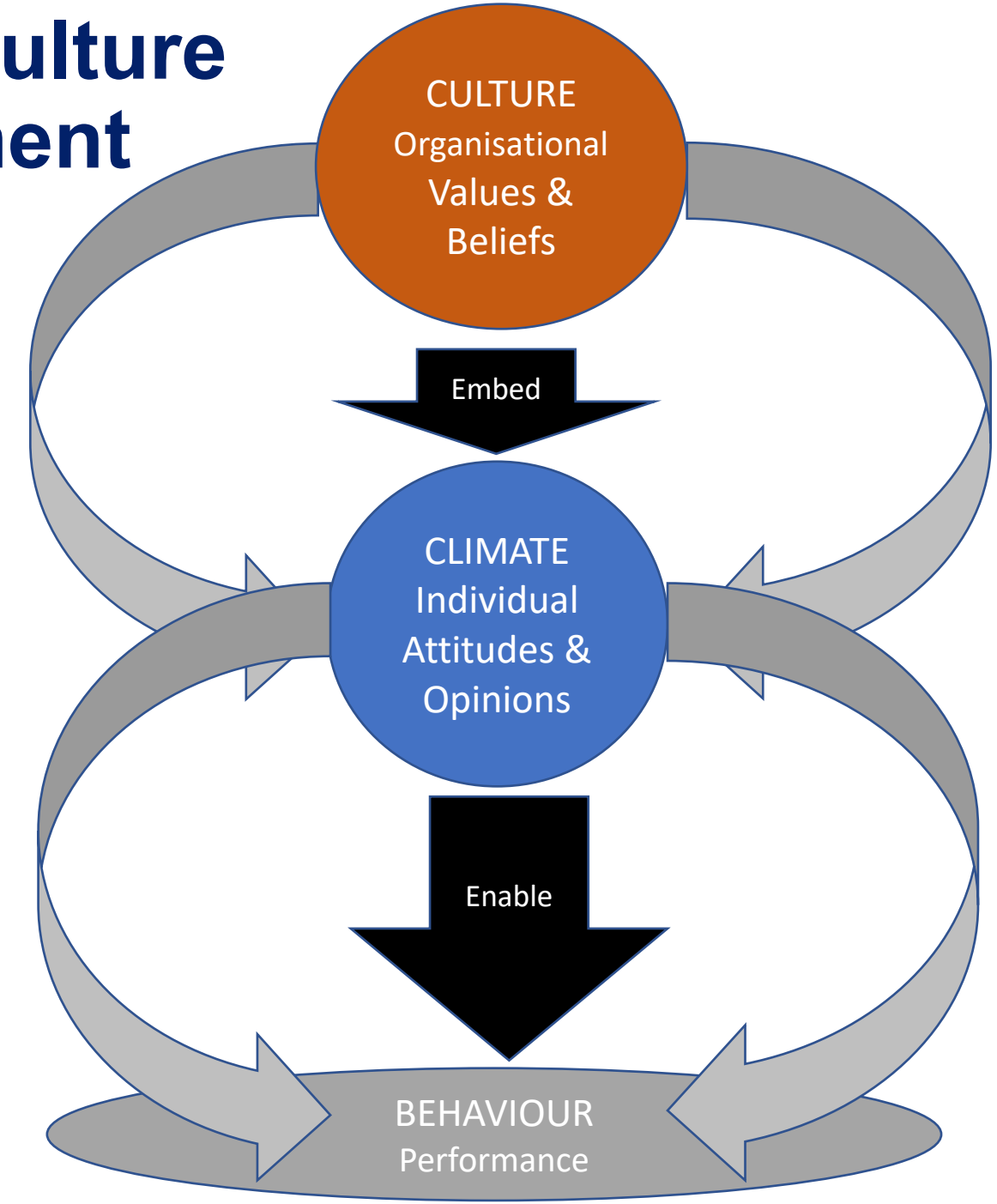
2. How incentivise & motivate Staff

3. How Manage Business Pressures

4. Fit-for-purpose Organisational Management Systems

5. Communication, education & awareness

6. Develop compliance & ownership



Adapted from the CAS Model of Culture Management and the Alnatheer Model of Security Culture

#3 Its Time for CISOs to Work Out Loud

#4 Build an community of security passionate people in your organisation

Benefits and Objectives:

- Creation of a community to enhance the provision of security capability.
- Enhanced security good practice across the business to impact our business and our customers.
- Communication and collaboration on security issues and activities
- Enhance the capability of our people

What's in it for them?

- Provide them with security insights, training, and knowledge sharing
- Keep them updated with current security news and activities
- Provide updates and key messages for them to share as they wish
- Allow them to share experiences and ask questions to the group.

Build a community, based on belonging and connection

Key Takeaways

- People are your first line of defence against cyber attacks, but they are still struggling to embrace good cyber security behaviours
- Its more than just awareness, we have to change culture and behaviour
- So much about people's behaviour is driven from those in leadership positions
- Digital leadership capability requires soft skills and importantly communication
- We need to empower people, build levels of participation and accountability. Our people need to learn from those around them, and every team should be encouraged to contribute ideas, insights and knowledge for achieving shared goals.
- Big digital shifts are happening right now - important to understand them from a people and customer perspective.
    1. Attention is firmly on mobile devices
    2. The internet is evolving from basic web pages, to interactive social media to the consumer blockchain and NFTs. This shift matters.
- As CISOs we can embrace digital shifts to become more effective leaders to communicate more effectively with our people and build strong security cultures. 4 strategies to do this are:
    1) Treat security as a continuous improvement exercise. Keep getting better every day.
    2) Use change management models to move the dial on your company security culture, not just InfoSec models
    3) It's time for CISOs to Work Out Loud, and
    4) Become community builders

How to connect

HILARY WALTON

Email: hilary.Walton@Kordia.co.nz

LinkedIn: linkedin.com/in/HilsWalton/

Twitter: @HilsWalton

TikTok: @HilsWalton

Instagram: @HilsWalton

Facebook facebook.com/HilsWalton

YouTube: Digital Culture Ideas with Hilary Walton

Podcast: Digital Culture Ideas with Hilary Walton

kordia®