How to create a Cybersecurity Education and Awareness Program to change behaviour

Jacqueline Jayne ‘JJ’

KnowBe4

BEFORE WE BEGIN THE WEBINAR

- **Presenter** will talk for about 40 minutes
- At the end of the presentation, we will **take questions**
- We will answer as many questions as time allows
- Use the **Q&A button** on the Zoom toolbar to submit your questions
- This session is being **recorded**
- **Recording** will be available to all registrants within 7 days

AISA presentations are intended for educational purposes only. Statements of fact and opinions expressed are those of the participants individually and, unless expressly stated to the contrary, are not the opinion or position of AISA, its sponsors, or its partners. AISA does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be recorded and published in various media, including print, audio and video formats without further notice.

AISA acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

AISA

About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

Australian Research

Office Workers

- 34% admit to using the same password for more than one account
- 14 % are using their work email address and their work phone personal activities
- 68% don’t believe using their work email for personal activity is a security risk
- 43% are not confident in identifying a real or fake email
- 46% are not confident in identifying a real or fake SMS
- 21% believe that Cybersecurity is the IT departments responsibility

KnowBe4
Human error. Conquered.

Australian Research

IT Decision Makers

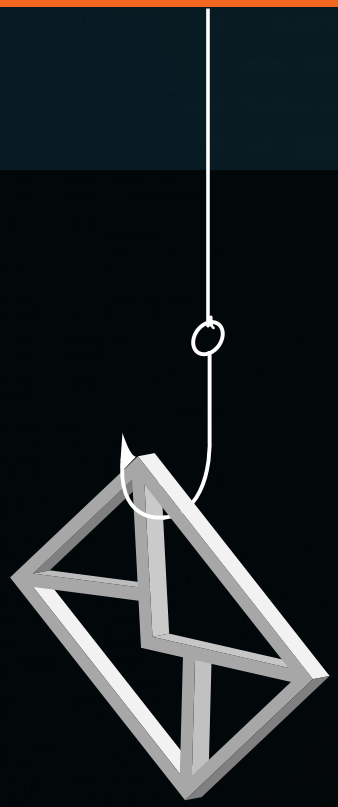
- 38% are concerned about phishing
- 42% are confident they would know the steps to take following a cyber incident or data breach
- 40% are confident their employees understand the business impact of a cyber attack
- 31% believe that it Cybersecurity is the IT department's responsibility

The majority cybersecurity breaches are a result of human error.

The ISHING Family

Vishing

Smishing



Phishing

QR Code Phishing

Spear Phishing

HUMAN ERROR IS NOT ALWAYS TECHNICAL IN NATURE

NON-TECHNICAL

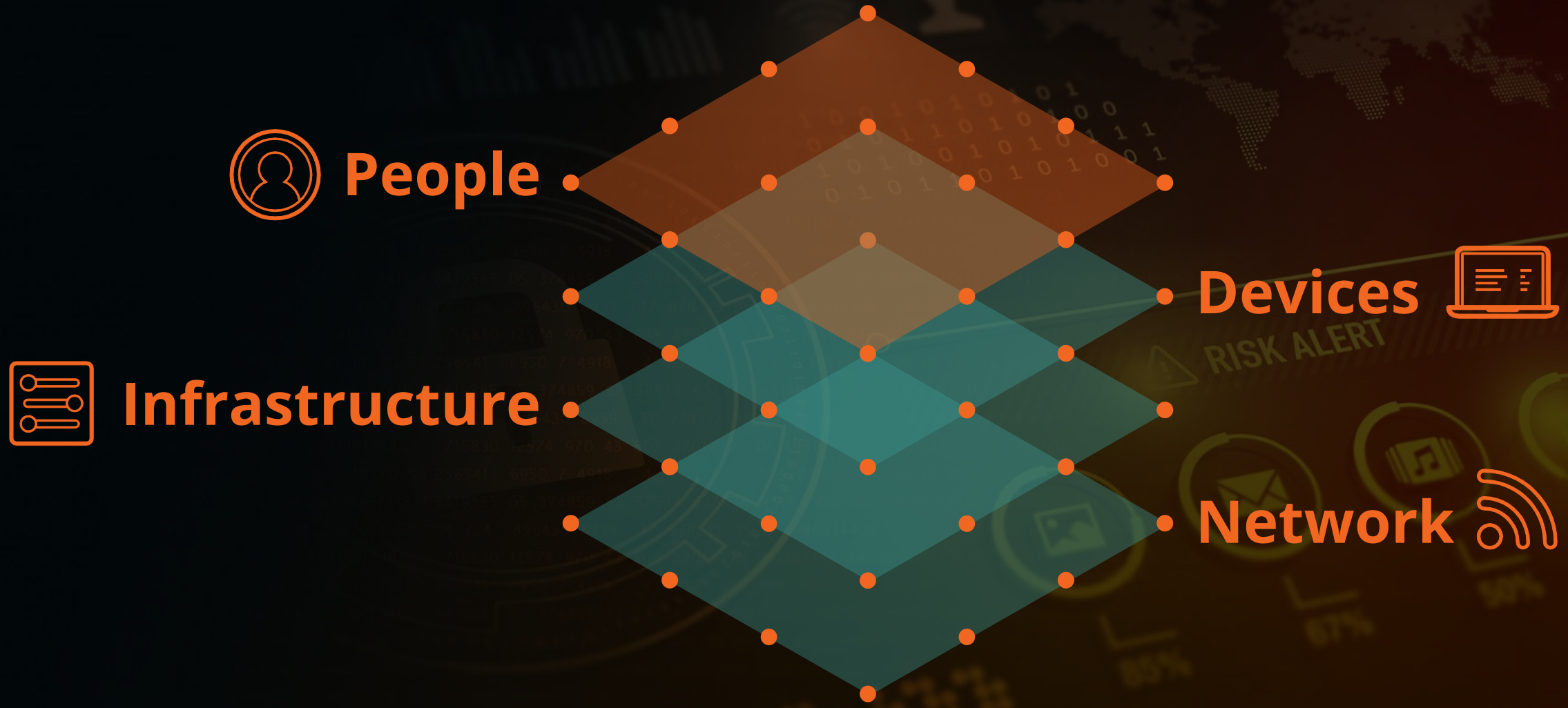
- Loss/Theft of Paperwork
- Loss/Theft of Devices
- Accidental credential disclosure (e.g. writing down passwords)
- Accidental disclosure of sensitive information via conversation
- Insecure data disposal
- Allowing tailgating into secure areas
- Sensitive information left on whiteboard
- Data mailed or faxed to incorrect recipient

SECURITY INCIDENT OR DATA BREACH

TECHNICAL

- Falling victim to phishing, vishing or smishing attacks
- Data accidentally sent to incorrect email recipient
- Failure to use BCC when sending email
- Poor password hygiene
- Insecure coding
- Malicious app download
- Misconfiguration of cloud storage
- Failure to redact data
- Oversharing on social media

Customers are Building a Modern Security Stack



That Starts with the Human

KnowBe4
Human error. Conquered.

Key Questions

1. How do we educate our people to understand their role in staying safe online.

2. Why can’t we just tell people what to do – make it compulsory.

3. Why is a combined approach to cybersecurity so important?

Observations

- Training people on cybersecurity once a year will not work
- Changing behaviour takes time and effort
- Knowledge or awareness is no longer enough
- There is a need to make cybersecurity personal to everyone for any real change to occur and for a culture of cybersecurity to develop
- Changing behaviour is akin to integrity, where people do the right thing even though no one is watching

Steps to Create a Cybersecurity Education and Awareness Program to Change Behaviour

1. **Research and Preparation**
   - Executive Buy In Part I
2. **Executive Buy In Part II**
3. **Launch and Manage**

1 Research and Preparation

Executive Buy In Part I

Project Plan ⇨ BAU

1. Team
2. Intent
3. Objectives
4. Success metrics
5. SAT platform
6. Key messages
7. Alignment with organisation
7. Reporting
7. Resources
8. Budgets
9. Employee monthly view
10. Simulated phishing templates
11. Best practice
12. Develop a timeline
13. Engage the organisation
14. Communication plan
15. Program expectations

What about the People?

- Expectations
- Roles and Responsibilities
- Identifying Risk
- Existing KPIs
- New Starters Program
- Cybersecurity Safety Officers (CSSOs)
- WIIFT (What's In It For Them)
- Rewards and Gamification

Engagement (activities to support awareness)

- Implement a formal team of Cybersecurity Safety Officers (CSSOs).
- Identifying the WIIFT (What's-In-It-For-Them)
- Develop a rewards program or gamification for observable behaviour change

Executive Buy In Part I

1. What does their ‘universe’ look like.
2. What information/data that is important to them.
3. What would it mean if that was stolen/breached.
4. Do their teams/people understand how to protect it.
5. What is the one biggest challenge they have when it comes to cybersecurity.

3 Executive Buy In Part II

Agreement and Sign off for:

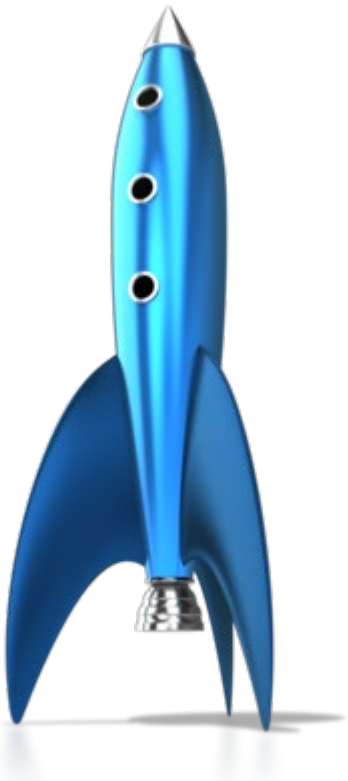
- SAT platform to underpin the program
- Look and feel (logo, language etc.)
- Communication plan
- Benchmark phishing email
- Knowledge and culture assessments
- Training minimum requirements
- Simulated phishing templates
- Reporting requirements
- Expectations
- Budget needs
- KPIs for the organisation
- Who is responsible for the ongoing program

4 Launch and Manage

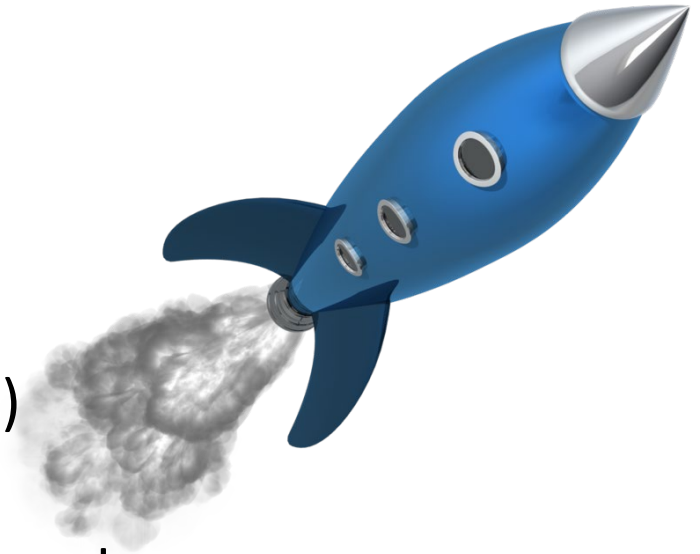
- Launching isn't what you might think.
- Formally engaging other areas of the organisation that will be supporting you.

In the first month:

- communicate the program out to the entire organisation
- benchmark results and what they mean – paint a picture
- upcoming knowledge and culture assessments and the WIIFT
- Expectations
- A calendar of upcoming events
- Provide enough information to ensure people know what, why, how, and when
- Include a link to the knowledge and culture assessments providing 2 weeks for people to complete them



4 Launch and Manage



- Communications to everyone (emails, notifications, updates, etc.)
- Sending out training
- Sending out simulated phishing and other social engineering elements
- Analysis of results
- Reporting to stakeholders and the entire organisation
- Preparing reports for compliance and regulatory requirements
- Organising in-person or virtual events
- Keeping up the hype for the program
- Cybersecurity Safety Officers (CSSOs)
- Gamification

Other Considerations for a Successful Program

- Never punish human error.
- Develop a cyber-related newsletter or page on your intranet.
- Demonstrate live hacks so the ‘a-ha’ moment takes place.
- Provide full transparency on any near misses or actual cyber-attacks on the organisation.
- Look at the data you hold and understand and communicate its real value.
- Focus on the data you have on each employee: when they realise it is not only customers data at risk their level of care increases.
- Provide useful resources for employees to use and also share.

Social Engineering Red Flags

FROM

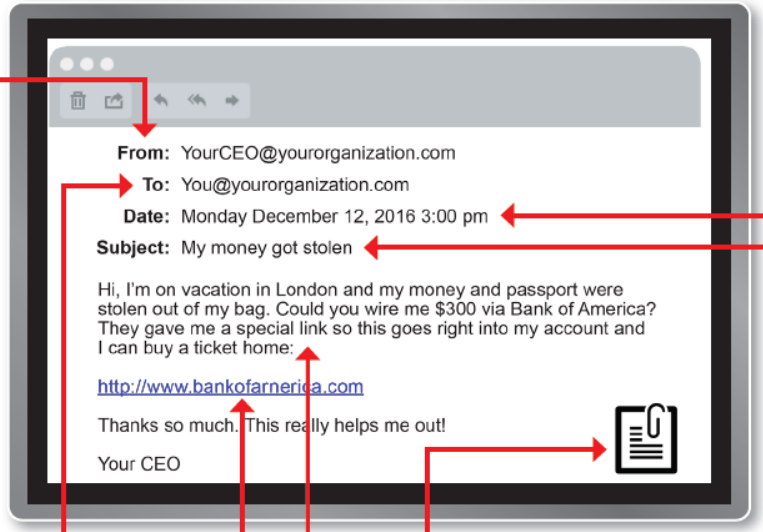
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

What you are embarking on is a whole organisation change management program that results in everyone making better decisions when it comes to security, ensuring all regulatory and compliance elements are achieved, the risk is reduced, your people are a formidable human firewall, and a culture of security is created.

Steps to create a Cybersecurity Education and Awareness Program to change Behaviour

1. **Research and Preparation**
   - Executive Buy In Part I
2. **Executive Buy In Part II**
3. **Launch and Manage**

KnowBe4
Human error. Conquered.

Thank You

Jacqueline Jayne
Security Awareness Advocate - APAC

Email: *jacquelinej@knowbe4.com*
Twitter: *@jakkijayne*
LinkedIn: */in/JacquelineJayne*
Clubhouse: *@jacquelinejayne*
Substack: *JacquelineJayne.substack.com*