*Jacqueline Jayne*
*Australia's 2020 Cyber Security Strategy - Submission form*

## 14 - How can Australian Governments and private entities build a market of high-quality CyberSecurity Professionals in Australia?

- Think differently
- Provide clarity on all the different roles that sit in the cyber space as they are not all technical.
- Promote cyber as a standalone – not just as STEM as there are roles with cyber that do not require S,T,E or M - Consider STEM(C) .
- Engage Human Resource within organisations and consultancy firms as they already have good business partner relationships. They should have an understanding on the culture of their business. From here discover those with the aptitude and curiosity to add cybersecurity to their knowledge base.
- Communication, Change Management, Marketing, Sales, Influence, Stakeholder Management, Data Visualisation, Creativity are just some of the skills required.
- Consider upskilling the aged care professionals as they have the most contact with the elderly
- Add a module of cybersecurity to the school curriculum and to all higher education. Like with math, there will be different levels each year as the complexities of technology increase so does the complexities of cyber.

## 24 – What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

**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 this personal for any real change to occur and a truly national culture of cybersecurity awareness and action to embed. Think 'drink and drive you're a bloody idiot', 'slip slop slap' etc.
- Behaviour change is akin to integrity, where you do the right thing when no one is watching.

**This following information is an evidence-based cybersecurity education and awareness program that was successfully executed in an Australian Organisation in the domestic environment and continues today.**

**The program created a strong culture of cybersecurity awareness with observable and measurable behaviour change.**

**The program is also scalable based on the elements referred to below.**

## Program Development

In many instances, a program such as this commence as a result of a board directive or identified need to 'do something' in upskilling people in cybersecurity. Whilst the preparation is multi-tiered, the result is a robust framework for a successful cybersecurity education and awareness program.

Remember that training people once a year will not work. The goal is to create a human firewall with your people ready for battle and armed with the appropriate tools and knowledge to protect your organisation from cyberattacks.

Your people are your last line of defense and creating human firewalls takes time.

In step 1 below, research and preparation will require time (1-3 months) with considerable stakeholder engagement and collaboration. The end goal is to obtain (if applicable) Board and Executive sign off. Without an agreed to plan, the program will not succeed.

**Who leads a cybersecurity education and awareness program?**
A successful program requires people (HR) and tech (IT) working together. If we consider the skills of each department, it is unfair to expect someone in IT to create a communications plan and it is unfair to expect someone in HR to understand the cyberthreat landscape.

- HR (generally) will have created a business partnering relationship with business units and have a clear view of the culture of the business – it's DNA so to speak. Change Management principals are also required which traditionally sit with HR.
- IT (generally) have a lot of knowledge in the cyber space, the technical jargon and compliance requirements. They get frustrated and don't quite 'get it' when the people still click on links and fall for these scams.

### Step 1: Research and Preparation

Create a Program Team (one person in HR (L&D or OD) to take the lead, an Executive Sponsor and an IT person(s). Step 1 could be treated as a project and transitioned to BAU after launch.

**Program**

- What is the program intent? (change or create a culture of cybersecurity awareness etc.)
- What are the programs objectives? (educate, change the culture, stop people clicking, comply with regulatory requirements etc.)
- What are the programs measures? (observable behaviour, simulated phishing reports, audits, completed training, assessments etc.)
- What are the key messages? (cyber is everyone's responsibility etc.)
- How will you know your program has worked? (measurements such as knowledge has increased, less people are clicking, people care about protecting the data etc.)
- If applicable, look for an alignment to your business strategy, risk policies and related compliance and regulatory requirements (PCI-DSS, NDB Scheme etc.)

- What kind of reports will you prepare?
- What impact with a program like this have on your organisation from a resource and time point of view?
- Research best practice for a cybersecurity training and simulated social engineering platforms to underpin your program.
- Include a baseline simulated phishing exercise and a cybersecurity knowledge check.
- Will there be a need for budgetary items (resourcing, licensing costs, marketing engagement materials, target free time for training, rostering needs etc.)
- Create a communication plan (type, frequency, intent, content, templates, emails, reporting, intranet, visual aids, etc.)
- Develop a program timeline (demonstrate all the steps involved and highlight milestones linked to measurements for success)
- Engage Sales and Marketing (look and feel, design a logo, phrases, imagery, position statement etc.)
- Ongoing Training and Education (engaging and relevant videos, eLearning, posters, infographics, games, informal F2F sessions throughout the year etc.)
- What does a month look like for staff?
    - Monthly Training – between 5 and 15 minutes
    - Ongoing simulated social engineering (SSE) – phishing, smishing, vishing, USB, tailgating, dumpster diving etc.
    - Reporting monthly with previous monthly training and SSE results
    - Gamification – teams against teams and leaderboard
    - Reward the desired behaviour – reinforcement

**People**

- What are the expectations for staff (compulsory monthly training, reporting of suspicious emails, participation with simulated social engineering, observable change in behaviours etc.)
- Leaders Expectations (leading by example, supporting program expectation for their teams etc.
- Consider Roles and Responsibilities in the organisation related to cybersecurity (this assists with identifying low, medium and high-risk roles when it comes to cyber)
- Will you include any elements of the program into key performance indicators for performance reviews?
- Will you add a cybersecurity education module for your new starters?

**Engagement (activities to support awareness)**

- Implement a formal team of CyberSecurity Safety Officers CSSOs (think along the lines of First Aid Officer, WHS Representative, Mental Health Officer etc.)
- WIIFM (the aim is to create a program that moves people to act so link CyberSecurity to activities outside of work, family, kids, travel, elderly etc.)
- Develop a rewards scheme for observable behaviour change (gamification, leaderboards, awards, make it fun etc.)

**Other Considerations**

- Do not ever punish human error (use it as a learning opportunity)
- Develop a cyber related newsletter or page on an intranet
- Provide useful tools for employees to share with their families
- Demonstrate live hacks so the 'a-ha' moment takes place
- Provide radical transparency on any near misses or actual cyber-attacks in the organisation
- Look at the data you hold and research what the actual value of it would be
- Focus on the data you have on each employee – when they realise it's not only the customers data at risk the level of care increases

## Step 2: Program Sign Off

Once you have compiled all the above information, it's time to present it to the Executive team for discussion and sign off.

You are now ready to launch your program.

**Final Comment**

There is a lot of information here. I am more than happy to elaborate on anything if required.
Thank you for the opportunity to provide this submission.

**Jacqueline Jayne**
[redacted]
Security Awareness Advocate – APAC
KnowBe4
www.knowbe4.com