2023-2030 Australian Cyber Security Strategy Discussion Paper

It is suggested that there are currently, about 134 690 cyber security workers in Australia. Forecasts from various sources suggest that by 2030, that workforce would need to jump almost 10-fold to around 1.2 million tech professionals. In 2020, it is estimated that Australia had a cyber security workforce of just over 108 000. An increase of 25% in 2 years. Along that trajectory, we are set to find ourselves around 900 000 fulfilled job roles shy of achieving our goals. Mindful, that the scenario is not as simple as I have illustrated, it does depict, and makes clear that we are set to (and already do) face a substantial skills shortage. For example, the evolution of the threat actor community and profession is force multiplying much faster than we are able to counteract the problem. Furthermore, due to the sharp rise in the sharing of information about cyber breaches, those professionals that are already in the sector are starting to suffer burnout, fatigue, adding additional stress levels that impact on their personal lives, and are unfortunately leaving the industry for a more balanced and sustainable lifestyle. A brain drain of sorts. The analogy that comes to mind, is that we are running the bath water, with the plug out. This gives rise to the question. Why the sharp increase in the demand for cyber security professionals? The answer may seem obvious, but is it really?

In answering this question, we also need to be asking ourselves questions like, what do we expect all of these skilled professionals to do? or What role will they play in our defence strategy? Presumably, a large proportion of the jobs required will be those of a technical nature, requiring individuals with a technical mindset to fulfill them. This by the very nature of the appeal to train more people in cyber, excludes the vast majority of the Australian population. Furthermore, we need to ask ourselves, not only who is going to train this workforce, but who is going equip this new workforce with the practical skills to take up arms and join the cyber war from day one. Organisations in general, don’t have the time, resource, or capacity to spend time developing skills in trainees, and academia without skills is merely stored knowledge with the inability to practically apply it.

In attempting to create a solution to our proverbial double edge sword, we first need to understand what the problem is, that we are really trying to solve. Is it a technical problem, a people problem, a business problem, a legislative or compliance driven problem, a process problem, or – ALL OF THE ABOVE. In my opinion the drive to make Australia the safest cybersecure country on the world by 2030 can only be achieved by integrating the skillsets of People, Process and Technology. The narrative rings loud and clear “Cybersecurity is a team sport”. But what does that mean? Is a simple “don’t click on that link” campaign or even ongoing campaigns sufficient to upskill the workforce at large? No, it’s not. A culture of good cyber hygiene and practice needs to exist in every organisation, big and small.

A detailed solution of how to achieve that goes beyond the scope of this paper, however achieving ambitious goals as set out by our government calls for a drastic change in the way we currently operate. For example, just as its mandatory for every person wishing to drive a car in Australia to undergo a period of learning and training, so to does it need to become mandatory for every individual in Australia to undertake a form of training relevant to their personal and professional lives. There are many ways to monitor this, ie through Telco's Internet Service Providers, companies etc. This can be in the form of a 2 hour online self-paced course for an individual to be renewed annually or form part of an onboarding procedure for every organisation that hires a new employee, regardless of their role. Again, to be renewed when appropriate. Certifications would be centrally monitored by state government which feeds into a federal system. Content that may be included in such certifications are understanding the ASCS Essential 8, practical ways to apply that knowledge to the individual or organisation and very importantly connecting the individual to the relevance of gaining that knowledge to their particular circumstance.

For a start, critical infrastructure organisations, filtering through to all organisations, should also be required to undertake mandatory prescriptive cyber culture upliftment programs, which provide measurable results, on a continual licence or accreditation based model, that needs to be renewed.

These concepts are not new. For example, the medical fraternity requires professionals to continually upskill and stay abreast with latest trends in the medical field, to remain licenced.

By addressing the people aspect in conjunction with the technical and process element, far reduces the need to upskill or reskill as many cyber professionals as is currently projected. We have a population of more than 25 million people with 99% connected to the internet. That is potentially a cyber security defence strategy of in excess of 25 million by 2030, of varying degrees of capability not 1.2 million.