Comments on AU Strategy

One of the issues with education in the cyber security sector is in understanding how the legacy infrastructure at the core of key businesses (e.g. IBM mainframes) and the operational technology (OT) environments should be managed. The really low level first principles seem to be missing. This means that whilst new graduates are useful in pen testing and securing simple ICT office environments with new Windows laptops and servers or current cloud the complexities of the real world non-standard and legacy environments is beyond them. I have made a career over 40 years in architecting for complex “real” environments that include legacy or OT and apart from people I or friends have mentored I worry that when my generation retire there will be a huge gap.

For OT environments, such as in healthcare where vendors control the device operating systems and patching, the government need to assist in pressurising vendors to ship more secure products and maintain them – and this may need renewed legislation through bodies such as the TGA/ADHA.

One size fits all ASD8, AISM doesn’t work in OT environments and this needs to be reflected in legislation. The main aim in healthcare – which can’t patch and uses passive detection and segmentation due to TGA compliance and the priority of not killing someone over confidentiality, integrity and availability, needed to be reflected.

There needs to be a rationalisation and clarification of the government requirements, regulatory regimes, and laws to make them less contradictory and clearer, with an understanding of context. We tried this with SOCI and it needs to improve in the same way. For example, several states have Police forces demanding access to all SIEM feeds for whole organisations but if the organisations also have contracts with the ADF this would constitute a data leak event. All laws need context and boundaries as to where they apply – so access should be “materially relevant and appropriate”.

SOCI needs to have more detail as to boundaries and dependencies. For example, for healthcare have hospitals in scope needs to explain what that includes as these have dependent diagnosis specialist pathology and imaging requirements, chemistry supply chains, power, etc requirements.

ASD/ACSC needs to have more specialist “sector streams” with contextual knowledge to advise organisations and collaborate with vendors and members of that sector. The organisations will have process “glue” knowledge that vendors and internal people won’t necessarily know. So many types of systems have to be glued together to make an organisation work in a given sector and these follow patterns – which consultancies have documented – and the government need to understand these when securing.

The country also needs regular “wargame” simulations and audits to “join up” the ACSC Cyber Incident Response Plans.

For some data the county – in the form of the federal government - needs to take complete ownership on hosting and controlling data in the GovDCs; i.e. MyHealthRecord needs the complete medical records and eReferrals. My experience of offshoring in government has allowed the data sovereignty principle in APP8 to be ignored, so controlling centrally and sharing through proper controlled environments where AISM and PSPF are enforced protects everyone.

Those of us with experience need to mentor the next generation in cyber security in the real world. I and my colleagues have volunteered as reservists and we need to assist the government in uplifting the infrastructure.

The move to the cloud needs to be decentralised. Australia has led the world in hosting remote cloud environments, such as the AWS Outpost in Perth and this needs to be built upon. Perth is the most remote city from the rest of the world so key infrastructure on the west of the nation and distributed needs to be built with a central high speed core. This improves resilience as well as performance as functions can be performed locally.

Cyber security research with genuine innovation requires acceptance that out of ten ideas maybe one only is successful. It is possible to build systems resilient to ransomware that emulate a local file system, for example – but if this is to be successful investment is required to build this and prove it in real life. The government is not well placed in writing new standards or developing innovative solutions so this should be an area the industry experts collaborate.

Systems need to be designed to adapt under attack and for this CI/CD and automation using intelligence feeds is required. This is in common use in the finance infrastructure already so is clearly possible. This “pattern” should be shared and built upon, with other successful patterns.