Dear Sir / Madam,

There will no dobut be considerable and detailed input from the public and organisations around your request for submission for Australia's 2020 Cyber Security Strategy.

I wish to only highlight the point that is already accepted by most in the community, which is that resillience is the most important aspect of any cyber security strategy.

Resilience comes in various facets though, and nothing is more resilient than a truly "distributed" system that does not have external dependancies for it's core function.

Whether it be our critical infrastructure, or an end-user technology the vast majority has become dependant on, I believe the government must enforce a standard whereby reliance on a central service must be minimised.

Much like the GDPR, which enforces that a product must continue to function if some information not critical in the delivery of it's value proposition is refused by the user; similarly, I believe the government must enforce that a function that does not absolutely require connectivity, should work without connectivity.

The above will be a worrisome statement for SaaS providers that wish to monolopise the market. The likes of facebook, google, uber, etc; will be (and should be) required to produce offline capabilities as standalone applications for their products that can synchronise data if need be, but must continue to function for all features that don't mandatorily require connectivity. It might be argued that in some cases, they already have such features (such as gmail-offline), but they are sorry excuses the companies have built. The government should enforce a standard that mandates that business logic must be executed on the client side (not server side) if possible to do so.

My next point is about preferentially chosing open source over proprietary software. Furthermore, FOSS (Free Open Source Software) must be used in preference to just OSS (Open Source Software). It is about time we moved on from the rationale beind old idoms like "Nobody Ever Got Fired for Buying IBM" - the saying might have changed, but the thought pattern behind decisions (especially in government departments) has not. It appears most decisions are based on either FUD (fear, uncertainty and doubt) and people go with technology where they can point the finger of blame squarely at someone else, or they take the easy short term path where the only skills required are being able to press the "next, next and submit" buttons.

Proprietary technology does not advance the goals of transparency and does not promote responsibility or give us power to "fix issues ourselves (as FOSS does) rather than just point a finger of blame at the vendor and shrug our shoulders as nothing more can practically be done". It has been very disheartning to see that many public schools now post event information only on facebook, and mandate the use of proprietary google tools by students. It is also dispicable to see that schools are encouraging students to buy "Windows laptops or apple laptops as the network and tools used might not be supported on linux". The point relates to cyber security as the ability to inspect the source code for the systems we depend on should be a fundamental right. Such inspection leads to detection of vulnerabilities that can be fixed resulting in a more secure, stable system; as well as encourages those writing the software not to try to put backdoors as they will get caught out.

Lastly, I believe it is an absolute necessity for the federal government to take up the development of a search engine. Just as regulation governned the media industry to ensure a level of standard; with

“user generated content” now as the primary source people consume on any topic, the ability to ensure transparency around it’s discoverability should have a regulated standard.

Much like the existence of government sponsored media, to ensure a level of unbiased news (although debatable whether that is still reality; the fact remains, unbiased news is important and if that is not the case, then things should be altered to make it the case); the government must ensure that a search engine is developed where:
* The algorithm is published for anyone to see
* A reference implementation is done for anyone to use
* The source is made available for anyone to copy and use as they see fit

The development of the above is paramount to cyber-security as the power bases have shifted too far whereby “Big Tech” companies now control what people can discover, and proactively manipulate the masses towards the benefit of their own organisations (including the swaying of sentiment at critical times such as when an election is imminent).

In summary:

We need decentralisation of products; centralisation has led to an imbalance of power such as:

* Facebook being able to psychologically manipulate individuals and the masses
* Google slurping data on everyone and everything to also manipulate the individuals and masses, albeit a little more subtly than Facebook (but at the same time, it’s orders of magnitude more capable of doing so)
* Uber effectively rendering occupations untennable by individuals … where there were hundreds to thousands of taxi firms, there is now effectively one (Uber), and if it arbritarily decides you are not going good enough for their platform – you will likely never drive a taxi again.

Such centralisation reduces resilience which is the most important aspect of reducing our cyber-threat.

We need to pick Free Open Source Software instead of Propritary software as it is more secure, and by it’s very nature, it is also not transparent for anyone to inspect (and contribute to) to help secure it further.

We must develop a search engine that publically discloses it’s algorithm, so that people have an alternative to foreign owned “Big Tech” companies who have the ability to manipulate the masses and vested interests in everything from influencing the public to make a particular party win at elections, to moving the masses to support or protest againt particular legislation.

Kind regards,

Simran Gambhir