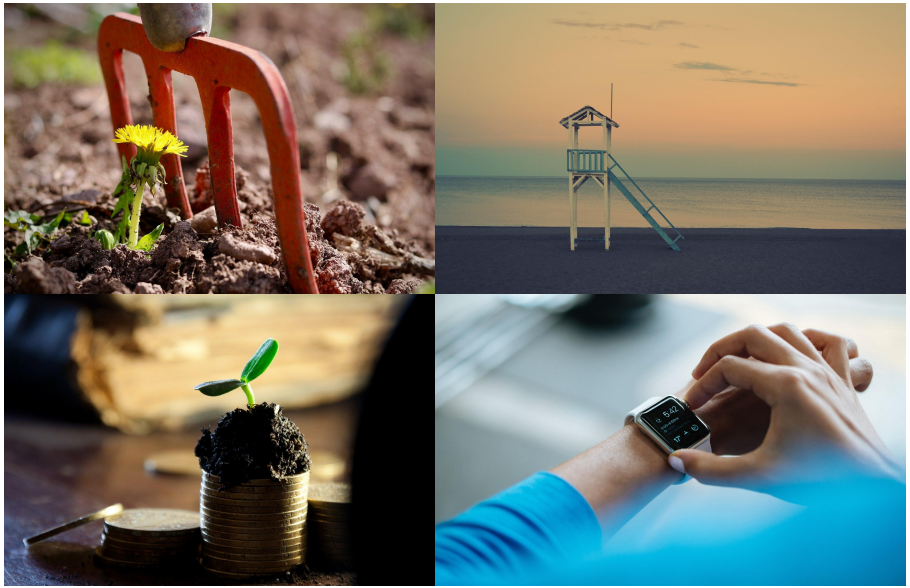
NSW Government
2020 Cyber Security Strategy



Stickman | Cyber Security by Design's Submission to the NSW Government.

We acknowledge the Hon. Victor Michael DOMINELLO, MP for leading the way in NSW for a stronger and more resilient cyber environment and having given us the opportunity to respond with this submission.

Ajay Unni
CEO and Chief Cyber Security Advisor
https://www.linkedin.com/in/ajayunni/

stickman
CYBER SECURITY BY DESIGN

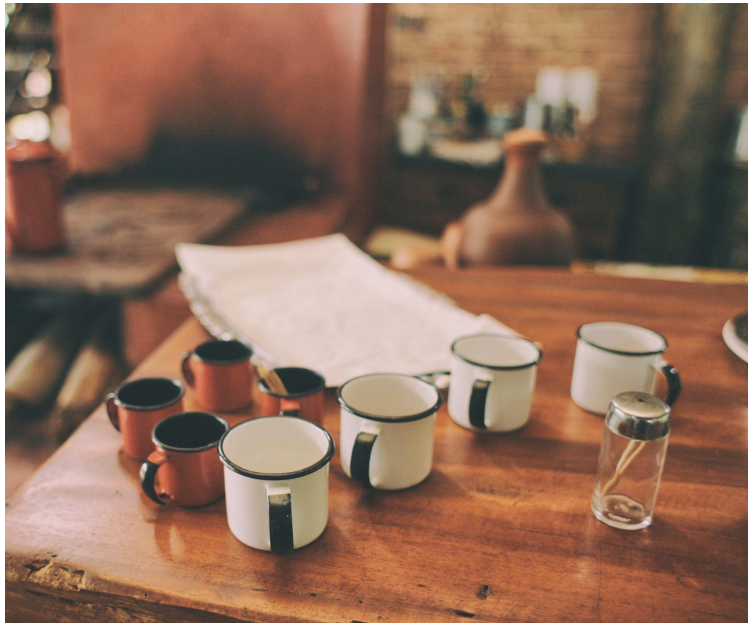
Executive Summary

Stickman | Cyber Security by Design has been on the forefront of cyber security for the last 15 years and has worked very closely with small, large, and corporate enterprises in developing, building, and creating a more secure and resilient cyber security environment.

Our mission is the relentless pursuit of excellence and achieving the highest level of customer satisfaction and the values to operate with care, respect, integrity, passion and authenticity focussed on our customers and our people through continuous feedback.

In this submission, we bring our 15+ years of cyber security experience along with our CEO's 30 years in the IT industry working across multiple domains and industries, managing large and complex cyber security projects across the globe.

We are honoured to take part in this submission and look forward to building a stronger and more resilient NSW and Australian Cyber Defence capability, industry, and infrastructure.



Enabling Cyber Security Resilience in NSW

Enabling Cyber Security Resilience in NSW

Resilience is built through training, education, awareness, measurement, sharing of insights, providing tools, access to expertise and emergency response and recovery in the event of an incident. In cyber security, resilience is built through the ability to face a cyber attack and recover from it, similar to preparing the community for a tsunami, hurricane or bushfire. We may not be able to stop a disaster or attack in its entirety, but we can definitely prepare for one and ensure we are able to combat an attack and recover swiftly.

Cyber is human. We tend to forget or ignore this fact and instead treat it like something intangible that cannot be quantified or measured. Unlike fires or hurricanes, cyber attacks have seldom taken life. However, cyber attacks have killed countless businesses and in turn destroyed the people that run them.

Much like the emergency response we have today for natural disasters, we need to create and develop similar capabilities for cyber disasters to help aid industry, government and the public on how to respond, address, and recover from such attacks.

A platform needs to be created where industry, government, and the public, share threat intelligence safely and securely and are able to take preventative action before an incident occurs.

All of this has to be supported by strong industry-led policy development and public consultation as there is no single entity or individual that has the consolidated knowledge or expertise to deal with and comprehend an end-to-end view of a strong and effective cyber security strategy.

Enabling Cyber Security Resilience in NSW

The threat landscape is constantly changing, and the only way to stay ahead of the curve is through constant observation, monitoring, detection, hunting, response, and having fast recovery measures in place. Technology alone cannot solve the problem, it is the ability to combine the right technology that is properly configured and aligned with people, processes, and policy that takes resilience to the next level. This cannot be achieved overnight, but it does mature over time. By practising these principles, governments can lead by example, instilling the creation of more robust methods and improving the overall chances of increased resilience.

To consolidate this and bring it home, data plays a very important role. The ability to create data lakes and reliable information sources that will aid in the detection and response capability is key. Today, monitoring, detection and response capabilities are impaired due to noisy data that creates distraction rather than targeted detection and response. Investment in more sophisticated technology coupled with people and processes is always going to be the winning factor. Unfortunately, there is no magic bullet as yet.

Ultimately, governments should instil the need for more strict cyber security due diligence across their procurement of products and services, which in turn will make industries more responsible. The flow-on effect to all parties in the ecosystem will then be more cyber awareness and the resilience to mitigate the weakest links in the cyber threat kill chain.

Addressing the Cyber Security Workforce and Skills Gap in NSW

Addressing the Cyber Security Workforce and Skills Gap in NSW

When India became independent, one of the first things the government did was to create a strong education system. The leaders of those days had a vision that the only way India could come out of that post-independence year and truly be free, was through education.

Similarly for our government in Australia, there is no second guessing. Our government needs to lead the way in the development and establishment of more institutions that can impart training, education, and war room style simulations of cyber attacks, on a new breed of cyber defenders who will safeguard the future of our economy, industry, and people..

There is no substitute. Cyber security is a serious topic that needs to become as ingrained in our children's education as maths and english.. The children of today are the future of cyber security and they need to grow with the knowledge and sense that cyber is human and will always be a part of our lives. Today, we teach children about sexual abuse, harassment, bullying, cyber bullying etc. Cyber security too should be made mandatory learning from an early age, so it has a direct impact on the overall resilience of not just groups of people, but an entire generation.

2020 has seen us face significant challenges with the spread of COVID-19, that has led to a number of job losses across various industries. This however, could also be viewed as an opportunity, to build a foundation for the recruitment, training, and development of a new workforce in cyber. Attracting talent both locally and from overseas.

I came to this country as a student, before applying for permanent residency, and for the last 15 years I've been running a company that is creating job opportunities, and attracting and training new talent. When a company like Stickman can do this, it is not impossible for the government and corporates to build and create in the same fashion. Through the recent announcement of budget allocations into cyber security by the Federal and NSW Governments, we see great possibilities and opportunities for the training and education of a new cyber workforce.

Helping NSW Cyber Security Businesses Grow

Helping NSW Cyber Security Businesses Grow

Businesses grow and flourish on the back of good government policy. Today, the key obstacle for smaller boutique and specialised cyber companies is the cost (time and resources) to enter into NSW Government tenders, due to the extensive RFP response criteria and documentation. If there was the possibility to pre-register cyber businesses with a set criteria (assessed annually), then it would create a level playing field for the small, boutique, and specialised businesses who are up against larger organisations with the resource capacity to address government tenders.

When I first came to Australia, I remember going to the Australian Technology Park to access grants to start my business. Similarly, there needs to be a platform and space for smaller companies and start-ups to innovate through access to such grants, as well as laboratories, test equipment, and simulation centres where people can experiment with their products and ideas.

Further to these initiatives, COVID-19 has taught us all a lesson about the ease and effectiveness of working remotely, while still accomplishing what we want to. There is nothing better than taking this learning and expanding our footprint into regional NSW where we can create new opportunities for people in townships that would previously have had to travel to the city to work in the field of cyber. This opportunity is not only good for the industry,, but for families and regional communities alike.

Finally, the NSW Government should make it possible for cyber companies to access procurement, and deliver services remotely, in order to truly showcase and distinguish the use of technology and to lead in the digital transformation space, securely and effectively.

I have lived in NSW from the time I first came to Australia and this state has created immense opportunities for me, my family, and my business. This is a true testament to the real possibility of what can be accomplished and how we can attract more talent from other states and countries to truly stand out.

Supporting Cyber Security Innovation and R&D

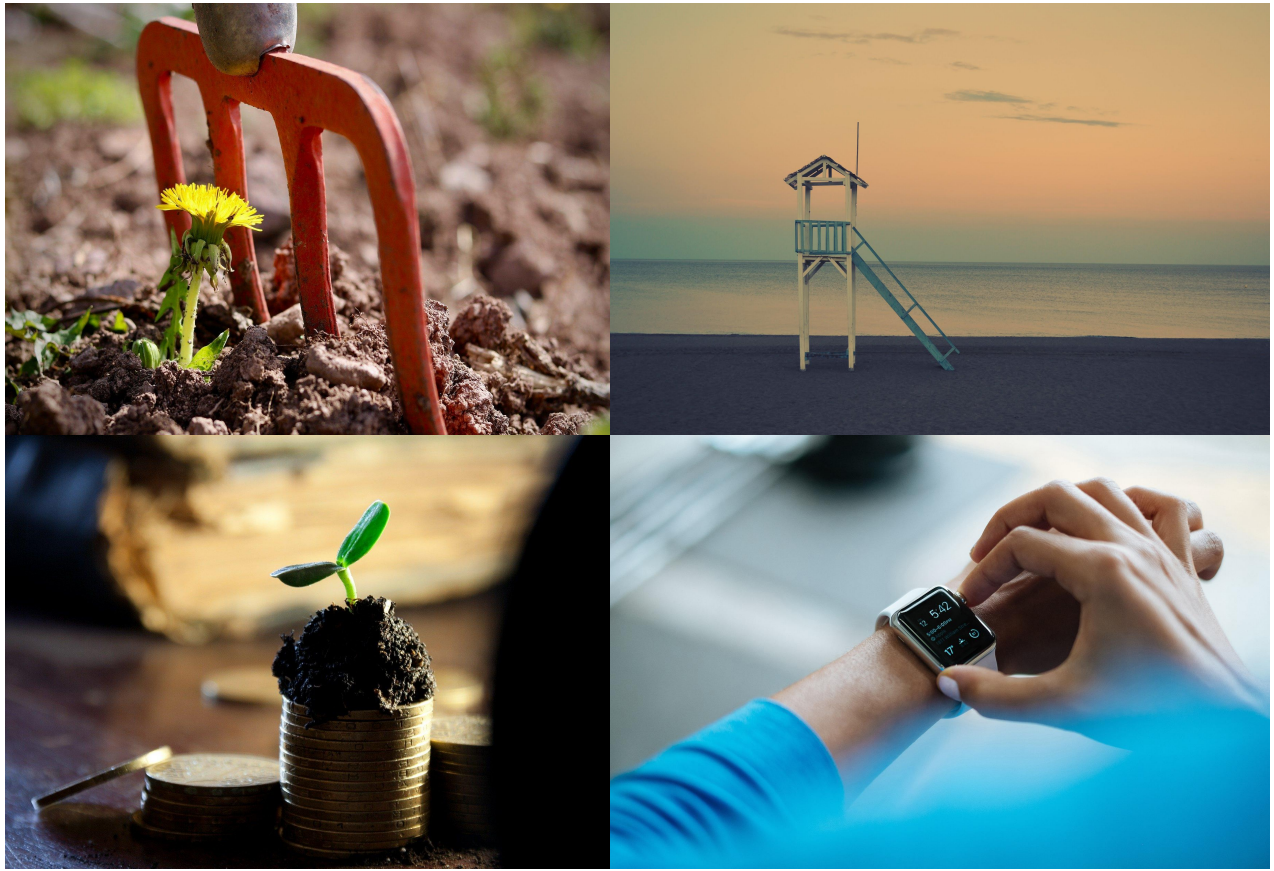
Supporting Cyber Security Innovation and R&D

When I graduated in 2002 as Valedictorian of the University of Wollongong, my speech focused on “how tough times never last, but tough people do”. That year, Australia was experiencing a recession and many people found it difficult to get work, but while the ‘going got tough, the tough got going’ and as a country we bounced back.

Today, the world is experiencing COVID-19 with job losses and uncertainty all around. It is during these trying times that innovation comes to the forefront. With more and more people facing unemployment, the sparks of creativity start to fly as people turn their hand to finding new ways of generating income. I have personally seen this happen over the last 30 years of my career, where a recession has created new entrepreneurs and innovators and I know there is no better time to create a platform supporting research and innovation.

Stickman has collaborated with the University of Wollongong’s Decision Systems Lab for a number of years and have worked on, and seen the benefits of, various research initiatives during this time. Unfortunately, universities today are facing their own set of challenges with a vast reduction in new enrolments due to the COVID outbreak. This however, presents a unique opportunity for universities to partner with the government, industry, and talent from the cyber sector, and to invest further into research, innovation and new technology (including AI). Maturity in the area of applying artificial intelligence (AI) and machine learning more effectively, and creating threat hunting capabilities that can significantly aid early detection and response to cyber threats and attacks, will help us better combat and defend ourselves, as those threats increase.

The learnings from research initiatives can help the NSW government improve their overall strategy and vision on cyber security and can help build a more robust and resilient cyber state that becomes the centre for Australia and the world. In conclusion, NSW is positioned strategically both within Australia and globally, and attracts a large number of skilled workers every year. We have the required infrastructure, people, leaders, and capabilities to be at the forefront of cyber security. What we need are the platforms and avenues that will allow us to build resilience, business, and innovation to attract the right talent and inspire others to be part of this journey, creating and expanding our capabilities in cyber security, both now and in the future.



Stickman Cyber Security by Design
Sydney, Australia

info@stickman.com.au
www.stickman.com.au

stickman
CYBER SECURITY BY DESIGN

LinkedIn | Facebook | Twitter