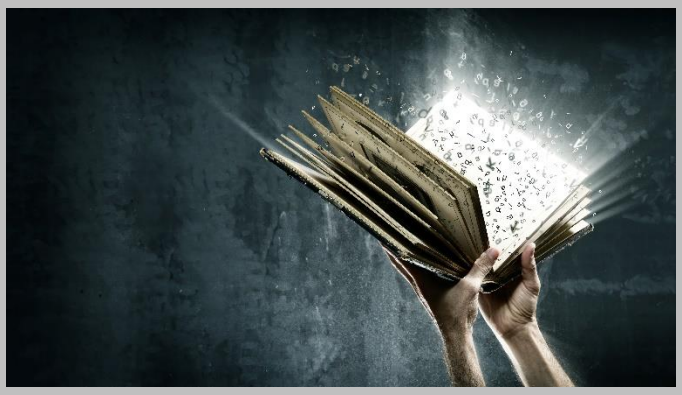
AUSCSEC

CEO Newsletter – Issue # 3

The Year of Living Dangerously with COVID 19.



In this month's newsletter, my third, I discuss, how COVID 19 has provided evidence that we as a nation are at high risk of significant impact and disruption by both a biological pandemic, and a cybersecurity pandemic.

Analysis from world renowned experts suggests that there are lessons to be learnt from comparing both types of pandemics and there are some insights on how we could better prepare for a major cyber event. Furthermore, comparing the infection rate of a biological pandemic to that of a cyber pandemic helps us understand that a cyber-attack with characteristics similar to the coronavirus would spread faster and further than any biological virus.

One of the fastest worms in history, the 2003 Slammer/Sapphire worm, doubled in size approximately every 8.5 seconds, spreading to over 75,000 infected devices in 10 minutes and 10.8 million devices in 24 hours.

In 2008 the Conficker worm spread to millions of unpatched PCs. That flaw was patched by Microsoft on October 23, 2008 — 29 days before Conficker began its assault.

In 2010 the Stuxnet believed to be responsible for causing substantial damage to the nuclear program of Iran, the Stuxnet hid inside their systems for 18 months before attacking.

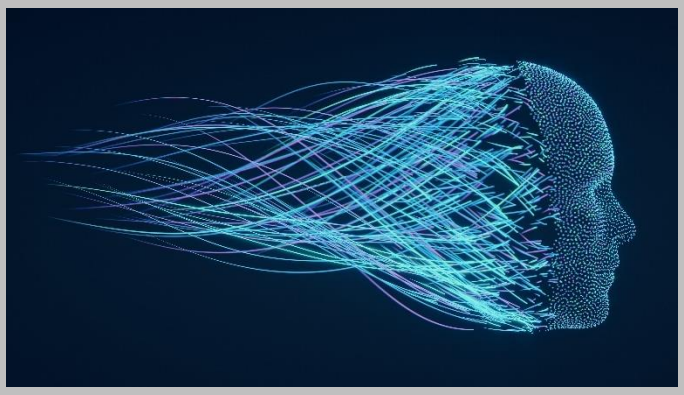
The 2017 WannaCry attack exploited a vulnerability in older Windows systems to cripple" approximately 230,000 computers in 150 countries within a four day period.

Yet despite the history before us we are still behind other countries in our collective and strategic understanding of the importance of cybersecurity and the benefits it can offer our citizens, our businesses and community.

Learning from these lessons could enable planning on a broader scale, we could achieve a greater level of granularity around essential criteria associated with critical supply chain requirements and know well in advance, where and what is considered critical and a priority, and when to authorise these activities when certain criteria have been met.

We as a nation are taking too long to formulate our collective understanding to make any progress on a collective national resilience programme that will enable us to secure our citizens data, our communities and their businesses, our economy and our nation.

Both Taiwan and Iceland created a great deal of trust with the focus on public-private partnerships, it is a lesson for the rest of the world to take notice of. Trusting our citizens in all types of roles to work with Government to solve big problems gains trust. Recognising the value of reliable data and using it as you would other valuable assets in your country's arsenal, builds the trust that is critical to enable real learning through a biological and cyber pandemic, thus creating an awareness beyond just compliance.



Cybersecurity awareness and a strong understanding of our critical risks as a nation are needed, right now to keep our critical infrastructure safe.

Over the past 6 months AUSCSEC has interviewed a number of companies deeply rooted in the traditional transport industry. This industry has been heavily relied upon by our nation to get us through the COVID 19 pandemic. Thank you to all of you for your perseverance, persistence and resilience, you really made a difference.

This month I have had the absolute pleasure to interview Morris Giavara from Swift Transport Services Dandenong South Victoria for our third CEO interview. I have published the interview below in this newsletter with a view to share Morris's stories so other businesses can pick up tips on how to survive during and post this pandemic.

So, let's meet Morris Giavara from Swift Transport Services, Dandenong Victoria.

AUSCSEC CEO - Welcome Morris and thanks for taking the time to speak with AUSCSEC.

Morris Giavara *- great to be speaking with you.*

AUSCSEC CEO - could you tell us briefly what type of business you have.

Morris Giavara *- Sure - Swift Transport Services have couriers and taxi trucks based all over Melbourne and can cover deliveries to and from any Melbourne suburb. We offer our clients same day delivery services for all of Victoria through our large fleet of courier taxi trucks of various sizes. We do door to door mainly and some interstate freight and onforwarding. We also do some specialised work like cranes up to 14 Tonne.*

AUSCSEC CEO - How has COVID-19 forced you to change?

Morris Giavara *– no great changes apart from some small policy tweeks around operational aspects of the business, i.e. the need for drivers to stay in their trucks and use COVID 19 safe practices, and some changes to allow staff to work from home. The workload dropped by 20% (worst case 700 jobs per day for a short period, it's now back around 15%). Internally we had to reduce hours for staff to reflect the workload, so we rotated staff every 4 and 5 days, or upon their request, but we didn't let staff go. We have a great group of people and we wanted to keep all of them. Some worked from home. We had people in office with up to 3 working from home on a rotational basis or upon request.*

AUSCSEC CEO - Has the change driven you to consider securing your business further from a cybersecurity perspective?

Morris Giavara *– Yes, I had heard about Toll, I was concerned, but thought that large organisations like Toll are probably a target. My IT specialist says we're 8 out of 10 from a security perspective. We have staff policy on email, and websites, but staff do browse websites, especially when I'm not at work.*

AUSCSEC CEO - Do you have the right cybersecurity people on your journey to new normal?

Morris Giavara *– No probably not, our everyday IT specialist says that we are reasonably safe but we wouldn't be able to prevent an attack from a state-based actor so I will be considering bringing someone in to review our cybersecurity posture and look to improve on that outcome.*

AUSCSEC CEO - On a scale of 0-10 where do you think you are on the cyber resilience scale? Why do you think that?

Morris Giavara *– based on our IT specialist's comment of being an 8 out of 10, I think we would be closer to a 6, I'm having several conversations to identify any ways to improve that and I'm also seeking advice from people like AUSCSEC to see what else would help.*

AUSCSEC CEO - Any lessons you want to share with the business community on how to better protect themselves and their businesses?

Morris Giavara *– There wasn't a great deal of change, mainly staffing matters. I didn't want to lose any staff members, we worked together to ensure they could take holidays a bit earlier, they are a good crew and they all work well together. I think if you manage staff well, they will reward you in more ways than one, our success has been through our people. Fortunately for me, being in the transport services business has been the right choice, now we just need to make sure it remains secure.*

Editorial Note: It is a common mistake amongst smaller businesses to think that organisational size is a factor in driving target selection by malicious actors, i.e. the bigger the organisation the more likely it is to be targeted. Consider for a moment that the bigger the company the more likely they are to have a substantial IT spend and so probably a substantial cyber investment. Smaller companies are likely to be the opposite and therefore much easier targets. To that end, its all about reward vs effort for malicious actors. Low effort for low return, but it's a much bigger pond with a lot of little fish in it. Fishing then becomes trawling.