AUSCSEC

CEO Newsletter – Issue # 1

COVID-19: The long road back - *a cyber security perspective.*

Since 21st December 2019 the COVID-19 virus has disrupted life as we know it in every sector and in the lives of millions of people across the world. Organizations rushed to develop strategies to protect their staff and vulnerable members of our community. We are advised that borders will reopen on 10 July and that will give businesses and the community a sense of normality and a sense of returning to business as usual, however, we should not be complacent. COVID-19 has changed the way we live and the way we go about our daily business, it is the new normal, and the new normal has new caveats for maintaining zero cases. The new norm has also spiked the sale of goods online with online shopping and parcel delivery out numbering letter delivery, and its set to increase as Victorians face yet another lockdown for at least six weeks. This type of activity could see fluctuations over time until Government officials see the number of cases decrease.

Coming out of COVID-19 may be a long road back for some states. The winding back of restrictions has placed additional stress on citizens, movement in and out of those states and has seen some of the toughest and highly monitored practices coming into play. That’s true of Cyber Criminals also, the only way to keep them at bay is to ensure you put in place some of the highest levels of monitoring practices to ensure they aren’t taking advantage of these exceptional times. Your own staff unknowingly leave a trail of bread crumbs out in the Internet all the way back to your environment, allowing rogue elements to follow them home and attack your business. Working from home means that your staff are working in a less structured or formal operational environment. Are they responsible with your resources and are they demonstrating good online security practices? Now is a great time to remind them of their responsibilities when using work resources and to ensure they are cyber aware. The Government is encouraging all Australians to remain vigilant and ensure sound cyber security practices are being maintained.

The events of Friday 19 June - should have made all Australian’s feel extremely uncomfortable hearing the Prime Minister describing the events as they unfolded. Australian organizations, including governments and businesses, were being targeted by a sophisticated foreign "state-based" hacker.

The Prime Minister emphasized the attacks "hadn't just started", that they were ongoing and constant threats to Australia, and said the accumulation of attacks required a firm warning to the government and private sectors to harden their shields. This should have reminded us all to incorporate cyber security into our business planning and to ramp up our cyber security awareness in every corner of our business.

Over the coming months I'll be conducting a 5555, where I ask 5 questions in 5 minutes of 5 CEOs over 5 months from small to medium businesses. I'll be asking them to share how they have been impacted and what they are doing from a cybersecurity perspective to prepare for their journey into the new normal. We will publish the interview in our newsletter with a view to share their stories in order for other businesses to pick up tips on how to survive during and post pandemic".

So let's meet Tom Royal from Swift Taxi Trucks Couriers the first of our CEO's to be interviewed.

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

Tom Royal - *Thanks Deb, great to be speaking with you.*

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

Tom Royal - *Sure, Swift Taxi Trucks & Couriers has 3 core business lines:*

1. *Taxi Trucks & Couriers, Semi-Trailers both local and interstate.*
2. *Transport and logistics which includes Third Party Labour (3PL) for example; Pick and Pack. We also have a container and storage service.*
3. *Swift GAS we provide Gas to the hospitality industries. We also provide gas to general and private hospitals as well as other relevant industries who require gas.*

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

Tom Royal - *We have been forced to change in a number of different ways, and at short notice, for example we had to work with our bank to enable extra capital to be made available.*

We unfortunately had to let a lot of casual staff go and I did that in an effort to keep our permanent staff.

We had to ask all out permanent staff to take their annual leave and we relied heavily on the Governments' Job Keeper initiative to keep our business running.

We have had to pull our permanent staff out from the hospitality industry because the work had just stopped, understandably so.

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

Tom Royal *– No, not really from a COVID 19 perspective, I think the issue with Toll made a lot of companies think about how they would survive if it ever happened to them. As a result of Toll we picked up some work but overall our business suffered. We were onto our IT support and discussed cyber*

> ***"Don't be mistaken - your local IT Support person is not your Cyber expert!"***
>
> ***Most won't know what to do or where to start, they may say - "I can fix your PC or monitor your infrastructure offsite, but I'm not really a cyber expert.***
>
> ***You're probably asking the wrong person!"***

security in general with them and what we needed to do to be cyber resilient.

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

Tom Royal – *Well its strange isn't it – we thought we were fully covered and then after a discussion with AUSCSEC it became very clear that my expectations of my local IT guys and what they should have had in place were completely different. Just the simple things weren't being done and I considered my IT support staff to be fairly switched on. But what I've come to realise is that your local IT Support staff who fix the PC's when you have an issue aren't cyber experts and when you ask them, they really aren't sure what's needed. But they were quite confident that they would have it all covered. Bottom line was, they didn't, and if it wasn't for AUSCSEC and their advice to my IT support staff I'd still be exposed.*

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

Tom Royal *– I think we are a 2-3 and I say that because we still have some way to go on our journey with AUSCSEC, but already I've learned so much and at the very least I've learned what questions to ask my IT staff, these are important questions that all CEO's need to be able to ask of their Executive and IT staff.*

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

Tom Royal – *Speaking to AUSCSEC has been a real eye opener, there have been so many in such a short space of time and hopefully someone will benefit from my conversation and think about their own environment.*

In general I would say don't necessarily trust what your staff are telling you about the state of your business from a cyber security or resilience perspective, they don't tell you anything that you don't want to hear and they simply just don't know.

This includes discussions around back-ups, monitoring and logging. Even simple things from like staff spending unnecessary time surfing the internet I always thought it was only a productivity issue but now I know they can be leaving opportunities open for cyber criminals to take advantage of their lack of cyber awareness.

You need cyber security experts and regular ongoing monitoring of your environment. If I had been made aware of the risks earlier I would have been happy to invest the money to know I'm doing the best I can to keep my business secure.

Your local IT Support person is not a cyber security expert – with a bit of help I was able to get to the heart of what was needed to be done quickly as a first set of steps, but I will be engaging AUSCSEC to work with us on our cyber resilience journey from here on.