AUSCSEC

CEO Newsletter – Issue # 2

COVID-19: Victoria in the grip of another lockdown – Stage 4 in Melbourne and Stage 3 in regional Victoria.

With peaks soaring to unheard of daily averages many people are forced back to working from home and many parents are set to commence home schooling again. Organizations again gearing up to ensure their remote networking is up to the mark.
The recent advice from the government indicates that malicious actors are actively targeting citizens and business organizations. These incidents are likely to increase as we work through the next stage of restrictions in Victoria and regional Victoria. Every new highlight of COVID 19 provides a new opportunity for COVID-19 related phishing and text campaigns to emerge. We need to remain vigilant ensuring that all of us are demonstrating good online security practices.

The government's advice serves as a timely reminder of what each of us should do when we work from home:

- Use your critical thinking skills to identify if the phone call, text, email or social media is a legitimate one, are you expecting this call or text? Is it unusual to receive an email from this sender;
- Use reason and common sense when opening an email that contains a link, do not click, just think. Do you know the sender of the email? Why would you be receiving an email or text message from this sender;
- Be very suspicious of any requests of you for personal details, bank account details and passwords and particularly if the request has an urgent timeframe attached to it. If the request is claiming to be from someone you would expect an email from, call them and ask if they have sent the email or message. Remember the scam calls to citizens last year from an organization claiming to be the Australian Tax Office (ATO), this put Fear, Uncertainty and Doubt into the minds of thousands of Australian citizens after being advised they owed the ATO substantial amounts of money ;
- If you are in any doubt, do not respond.

Protecting your business from malware:

- Automatically update your operating system; and
- Automatically update your software applications.

Regularly back up your business data:

- Choose the right back up solution for your business;
- Test you are able to restore back up regularly;
- Store a physical backup safely offsite; and
- Don't forget – if you are an industry that has obligations to keep data for a specific period of time make sure you are aware of what business data you are required to keep and for what timeframe.

Consider implementing Multi-factor Authentication because multiple layers make it much harder for criminals to attack your business. Some may manage to steal one proof of identity, but chances are lower for criminals to be able to steal multiple identities. Some examples of simple to implement and universally used are:

- the use of email and SMS to receive security codes, for example Qantas and the Commonwealth Bank use this process of an SMS and/or a phone notification;
- Other banking institutions use the authenticator application for their online banking; and
- Physical Tokens are simple to use and meet the Governments Maturity Model for level three.

Staff training in Cybersecurity awareness is an important line of defense, regular awareness training and a workforce that has a strong security culture will help protect your business from cybersecurity threats.

Australia's Cyber Security Strategy 2020 was launched last week emulating the Prime Minister's comments of the 19 June 2020 that stated. "*Australian organizations, including governments and businesses, were being targeted by a sophisticated foreign "state-based" hacker".*

In summary, this strategy will invest $1.67 billion over 10 years to achieve our vision. This includes:

- Protecting and actively defending the critical infrastructure that all Australians rely on, including cyber security obligations for owners and operators.
- New ways to investigate and shut down cybercrime, including on the dark web.
- Stronger defences for Government networks and data.
- Greater collaboration to build Australia's cyber skills pipeline.
- Increased situational awareness and improved sharing of threat information.
- Stronger partnerships with industry through the Joint Cyber Security Centre program.
- Advice for small and medium enterprises to increase their cyber resilience.
- Clear guidance for businesses and consumers about securing Internet of Things devices.
- 24/7 cyber security advice hotline for SMEs and families.
- Improved community awareness of cyber security threats.

This month we interviewed Steve Green from Open Systems Consulting for our second CEO interview. We will publish the interview in our newsletter with a view to share Steve's stories for other businesses to pick up tips on how to survive during and post pandemic".

So, let's meet Steve Green from Open Systems Consulting.

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

Steve Green - *great to be speaking with you.*

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

Steve Green - *Open Systems Consulting has more than 20 years' experience designing and analyzing courier software & dispatch systems for the transport industry. The business was set up around 1991 and focused predominately on the transport industry. The business has grown exponentially over the years and now includes a private cloud solution that suits the Transport and logistics companies that we look after.*

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

Steve Green – *I wouldn't say we've been forced to change, our business has not had to make major changes given we are an ICT consultancy business and our main aim is to provide services to our customers in what ever shape they require it, mainly in the Transport industry, for instance, COVID-19 has meant that more and more staff are working from home and more customers are wanting to interact with us and the transport companies for one off purchases. We needed to find a way to work with our customers and our co-providers to make this model work delivering the outcome to the customer with no fuss.*

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

Steve Green *– No, not really this change is reliant on credit card software vendors providing their plugins for us to host on our website. If anything, the change has been in the increased number of customers we are moving to the private cloud solution. We are ensuring that the security is tight as we move their legacy operations and data to the cloud.*

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

Steve Green – *I think we have the right expertise within Open Systems around the use of ICT hardware and software to; set up secure VPN's, utilize fire walls secure our customer's communications connections and use appropriate virus protection. I would say, however, that while any of our customers may be connected to the internet through a third party internet provider, that third party, in itself, may not have the right expertise for the task at hand at any point in time. It is a bit hit and miss sometimes and can be quite messy in that the hand offs aren't always that thorough and can leave you shaking your head at times. But what I've come to realise is that these Third Party suppliers aren't Cybersecurity experts either and they are most likely at best IT Support staff and we*

"the customer may be connected by a third party internet provider that may not have the right expertise, it's a bit hit and miss sometimes and it can be quite messy in that the hand offs aren't always that thorough and can leave you shaking your head at times.!"

find ourselves being involved in the lower level detail around which ports they need to open for an implementation, specifically we ask to open those certain ports only to find out the modem they operate is not that granular its either all on or all off . This type of activity can leave even the best provider of ICT services 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?

Steve Green – *It depends, I think we are a 7-8 and I say that most of our security is pretty good, but I'm not experienced enough to know how I could mitigate a cyber-attack. I think our business operating model is straight forward and does not offer opportunities for cyber attackers to get into our environment.*

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

Steve Green – *I have no suggestions for other businesses, but what I will say is that monitoring is the way to go. I am not a Cybersecurity expert, but I know enough to figure out how to set up ICT security configurations in a VPN or how to include firewall rules for my customers. Security is paramount, there are so many unknowns these days and different types of attacks if you did not have any monitoring in place you just wouldn't know what is happening in your environment.*