# Transcript of Interview

## So, tell me a bit about yourself? How long have you been in IT?

Michael: I have been in I.T. since 1998. I started as a support technician in the Dental and Specialist Medical field in Sydney then moved to the Central Coast where I became an onsite support technician.

When I was in my late 20’s I decided I needed a new challenge, so I went to University to get a degree. When I returned to the same company that I left to go to university I was promoted to Business Development Manager then to General Manager.

## What qualifications do you have?

Michael: I have three TAFE certificates from the late ’90s. I have a Bachelor of Science in Information Technology, Microsoft Certified Professional, CISCO CCNA, ITILv3 and most recently Certified Ethical Hacker.

## Feels like a great time to ask what life in the day of Michael is like? What is it you do daily?

Michael: Work, work and then work some more. For the last 18 months, I have been studying hard to become an Offensive Security Certified Professional so that takes most of my time outside of work. To relax I play soccer, watch sports of all sports (soccer, rugby league, cricket) and sometimes play the Xbox.

In work time, I manage a busy office of 15 performing technical, HR, accounts and sales and marketing duties. The number and variety of these particular tasks change from day to day, but most days will incorporate these tasks to varying degrees.

## What kind of people do you interact with daily? Is it other IT professionals? Clients? Investors? The public?

Michael: Clients, internal employees, and small business owners.

## Where do you spend most of your time? Are you in an office or have you been moved to a home with COVID?

Michael: I spend most of my time in the office. We were moved home during COVID for about two months then we returned to the office.

## What aspect of their position is most challenging?

Michael: People management, for sure. (mostly internal)

## How does a business stay current on the IT Landscape?

Michael: There are several ways to stay current. I always keep up to date with tech news via tech websites and podcasts and we make business decisions based on what our clients want. For example, as little as 5 years ago our mantra was “cloud is for clowns” where we were pushing against the move to the cloud because of unstable internet connections and the expense of moving there. Fast forward a few years and we are now promoting and recommending it. You need to always keep an eye on what your market is telling you and often you find yourself pivoting to meet the changing needs of your clients. Our push into the cybersecurity space started 3 years ago and is only now starting to gain traction. Sometimes you need to make some predictions and bide your time.

## You have recently started a campaign to be the face of cybersecurity on the NSW Central Coast. Tell us a little about that.

Michael has recently had the government choose his company to help spread knowledge out there about the insecurity’s that every day business may have without even realising it. Michael will be the spokesperson to help bring essential cyber security aid to the NSW central coast.

## Congratulations on this wonderful achievement. Can you shed some light on what this will entail and how it changes what you will do on that daily basis?

Michael: This will mean I will become a trainer, as opposed to a manager. I will be creating a studio where I will record podcasts and produce video recordings of “how-to” and Q&A videos. This will be a subscription service that is aimed at delivering the government’s Essential Eight cybersecurity recommendations to Small and Medium Businesses in the Central Coast region. It is expected that Loyal I.T. will be able to create revenue from those businesses who are aware of cybersecurity risks but do not want to use the instructional videos and prefer a professional to implement the security measures.

## Where do you see the industry moving to? Being an IT firm that caters mostly for small to medium businesses, do you think that on-premises servers are the way of the future or are you leaning more towards a cloud-based environment for these customers?

Michael: The cloud is absolutely where everything is going. In our region, the move to the cloud for many businesses is driven by lower costs. No longer do small businesses need an expensive server with expensive maintenance, they can do much of what a file server was done by purchasing an Office 365 subscription and using the cloud versions of other essential software such as accounting and CRM software. And all of this is enabled by stable and fast internet connections which the NBN has provided for in this region.

## This is more of a personal question that I have found I ask myself a lot at the moment, If you went back to do it all again, Would you pursue the bachelor’s degree? Or look at other resources for certification?

Michael: I would do the bachelor’s degree again. It comes down to personal goals. What do you want to achieve? When I was at uni, I saw so many people there who were forced into the study by their parents rather than pursuing something they wanted to do. I believe having a clear vision of what you want to achieve is key, then get qualifications that support your vision. There is no right or wrong answer. For me, doing the degree was key to moving my career forward to where I wanted to be. Right now, I will not go back for a PhD in computer science because I don’t envision a future where that will be useful. I do envision a future where a hacking certificate will be useful, so that is what I am studying for. It’s all about your situation and your goals.

## There seem to be a significant number of certifications and accreditations floating around different learning providers (TAFEs/Open Uni etc) that individuals can take to further their knowledge in the industry. If any, which do you recommend all cybersecurity professionals should have (besides any that are already industry standard), and if there are none, why?

Michael: I don’t have a lot of insight into what TAFE or Uni has to offer at the moment but what I use as a compass for what certifications are more valuable in the cybersecurity space is that job ads are looking for. At the moment there is a push for a degree in information technology or equivalent, OSCP and ISO 27001. This is my focus at the moment because it is what businesses are looking for. You have to be guided by market forces and if this is what the market wants for someone to gain employment, then this is what you need to focus on achieving at a minimum.

## What information do you need to oversee Cybersecurity Risks?

Michael: The best form of defence is to have your systems penetration tested.

As there is so many vulnerability’s getting the red team in, is the best form of figuring out where your weak and how to build your defences.

## How do you protect sensitive information handled and stored by a third-party vendor?

There is not a lot that can be done is this regard. “You are putting your data on their servers, there has to be a level of trust”.

## In today’s world, what do you think is the top cybersecurity concern businesses face?

Ransomware: Michael had elaborated on a client that has been attacked.

Ransomware can come from anywhere and as such. Once they have the data everything is compromised. The client had paid the money as they did not have backups, and as such the hackers ghosted the business owner. Leaving the owner out of money and still with no data.

## Do you think the creation of all the new crypto currencies are going to aid these ransomware attackers?

Can’t really be doing it any good. Nobody mines bitcoin anymore once they get onto a server as the turnover is low, so eventually you will see more of these other currency’s starting to show up and around a bit more consistently.