



AUSTRALIA: SECOND MOST CYBER ATTACKED COUNTRY IN THE WORLD!

Did you know, second only to the US, Australia endures the highest rate of ransomware attack in the world?

Ransomware, as you will have read in my previous posts, is a concerted campaign by cybercriminals to gain and “lock” access to a business’s information. Paying a ransom to the cybercriminals is the only way to regain access to your information. The most worrying trend is the targeting of small and medium sized businesses (SMEs). You may wonder what the strategy behind that is – surely large corporates are more lucrative targets? They certainly are, but they also have the resources, and the risk profile, to develop and deploy consistent, yet expensive, cyber security protocols. In other words, entire departments are dedicated to mitigating the risk of online security breaches. SMEs on the other hand have to make difficult decisions around cost versus perceived risk, and most do not perceive themselves to be at exceptional risk of online security breaches, and therefore do not spend the resources to protect themselves. This is a mistake.

Between January and June 2016, the number of ransomware attacks was 172% more than the *entire* year of 2015. The reason for the increase is that hackers are targeting more and more individuals and small businesses. The “Ransomware Trade” is a lucrative and well-organised global business in itself. According to Intel McAfee, around 16,000 new ransomware code

changes are created each day, therefore antivirus companies are always playing catch-up in releasing updates to their customers.

Let's take a systematic look at why SMEs are being targeted, and what small business owners can do about it:

1. Small businesses underestimate the risk.

Cyber security is typically not considered a high priority when businesses need to grow and adapt to challenging economic environments. Profit, cash flow, product development, recruitment and customer service are prioritised in terms of management time, as well as resources. The truth is, a cyber-attack can not only dilute or damage your business, it can destroy it overnight! Take time out with your team and engage a cyber security specialist to assess your security risk, audit your processes, services and product development. A specialist will soon identify where your business is vulnerable to information leaks, and intellectual property theft.

2. IT and other services are often outsourced to third parties.

Streamlining your operations by outsourcing tasks such as bookkeeping, marketing, HR and IT makes sense. However, it also compounds information replication across increasingly insecure or unknown entities. The further your information flows out of the business, the more insecure it becomes. Understand what cyber security features your service providers use, and insist on quality assurance measures when they deal with your information. Don't take the providers word for it – confirm for yourself by engaging an independent cyber security specialist to perform a security check on your providers.

3. Cyber security is not a management principle.

A good new year's resolution for your business would be to engage a cyber security specialist to design an appropriate cyber security system, both technological and procedural, that is regularly reviewed by management. A simple set of standards and practices can be implemented across your business. It can then be used to bring management as well as staff to account, via performance assessments, quarterly reviews and annual reports. Don't assume your existing IT staff, or external IT provider, has the knowledge, experience and qualifications of a cyber security specialist.

4. SMEs do not have processes in place to evolve or change their security posture.

Even those SMEs that have implemented dedicated security systems lack the appetite or capability to review and fine-tune their security systems and processes regularly. Hackers are continuously changing their code, methods and tools. SMEs must dedicate time and resources to stay abreast of the changing threat and update their security system/s and responses accordingly. Unfortunately, if your IT staff or IT provider "don't know what they don't know" in relation to specialist cyber security, then your business is at high risk by default. Again, engage an independent cyber security specialist to work with your IT staff or provider to ensure there are no security gaps.

Australia's SMEs make up an impressive 97% of all businesses in the country, and employ 4.7 million people. The Australian government is therefore taking the cyber security threat to this

important sector seriously and their latest [Cyber Security Strategy](#) is available on our web site. This programme will offer businesses the opportunity to have their cyber security tested by certified practitioners, and plans to develop a portal where SMEs can share cyber security experiences and direct threats. The portal will make it easier to detect and respond to various forms of cyber-attacks, and will offer practical advice on how SMEs can bolster their cyber-attack defences.

By Johann Koelmeyer (CEH) - Cyber Security Engineer at
<https://onlinedigitalsecurity.com.au/>

