CYBER SECURITY ALERT !!!

RUSSIA INVADES UKRAINE – WHY SHOULD I BE CONCERNED

Those that have attended earlier Cyber Security/Crime presentations given by the writer would recall the writer spoke of the 'NotPetya' malware infection.

Specifically

- **DLA PIPER**
- **Global law practice located in more than 40 countries.**
- **In 2017 the hackers (of Russian origin) attacked the Kiev office of DLA Piper with the 'NotPetya' malware infection. It spread through every server, computer and devise attached to the system throughout every office in every country.**
- **Starting in Ukraine the malware then spread rapidly throughout the world and at the time was estimated to have a cost of over $10 billion**

The Australian Signals Directorate through the Australian Cyber Security Centre (ACSC) has put its ALERT STATUS to HIGH.

There has been a historical pattern of cyber attacks against Ukraine that have had international consequences. Australia has had a history of increased State sponsored cyber security activity after it has offended the countries in question.

ACSC recommends that everyone should adopt a posture of enhanced cyber security posture and increased monitoring for threats to help to reduce the impacts to Australian organisations.

The reader may recall the following in the last alert:

Ransomware

There has been another ransomware attack, identified as coming from Russia. All files, trust and office records were encrypted and lost to the law practice. A ransom was paid to retrieve the decryption key and restore the data.

Don't forget – a ransomware attack is only possible if someone has downloaded the malware. Hence, the need to be forever vigilant. Do not click onto links or open attachments from people/organisations you do not know, and where you do know them, where you are not expecting any such attachment.

Since the last alert

There have been another 3 incidents.

One involved a direct debit from the trust account from what appears to be a client paying a debt. (see previous alerts on direct debit transactions).

The other incident involved a scammer pretending to be the principal of the law practice. The scammer sent an email to the employed solicitor directing them to go to Woolworths

and obtain 8 Steam Gift cards valued at $100. In this case the employed solicitor queried the email and discovered the fraudulent activity. All the necessary details for the scam were obtained from the law practice's website.

The way this scam works is that the scammer asks that the registration details be scanned and forwarded to them. They are then able to obtain a financial benefit using the registrations, and because they were successful with the first attempt further attempts are made.

The third incident involved the law practice's computer being compromised and Rule Changes being made in Outlook (see previous numerous alerts about looking for these Rule Changes). When the email went out requesting $180,000 for stamp duty be deposited into the law practice's trust bank account, the hacker intercepted the email and changed the bank account details. Luckily, during a conversation, it was determined that the client had received the wrong bank details and the bank was immediately contacted to freeze the account to which the money was deposited. The $180,000 was recovered.

Following on from this, the law practice's IT people have set up a system of double authentication such that if anyone wants to make a Rule Change the system automatically sends a code to the principal's mobile phone and that code is required before the Rule Change can be effected.

This is a discussion you can have with your IT people.