BUSINESS

Q & A with Penelope Green

Cybersecurity alert

Dr Alana Maurushat, professor of cybersecurity and behaviour at Western Sydney University, will brief Newcastle businesses this week.

WHAT will you discuss as keynote speaker at the second Diamond IT Cybersecurity Industry Breakfast in Newcastle on June 20?

I'll be discussing some of the current cybersecurity threats faced by organisations. We'll take a deeper look behind scenes at the individual criminals, organised criminal syndicates and the underworld where they operate such as on Dark Net Forums. I'll explain how cybersecurity threats are becoming increasingly sophisticated by looking at artificial intelligence (AI) enabled cyber fraud. This fraud encompasses a range of traditional online fraud using new tools to automate aspects of the process. My talk focuses on two primary online frauds that are the subject of two research projects at Western Sydney University - payment diversion and ransomware. I will go through each type of fraud, explaining the concept and then providing a case study. We'll look at the common ways in which fraud is committed, from financial data to accounting practices, to network intrusion to social engineering aspects. Automated AI aspects will be explored within these threats. The case studies are based on real cyber frauds, but the personal information and case specific details have been generalised to protect the parties involved.

Are scammers savvy?

The myth is that the scammers are always one step ahead in terms of technology. This is incorrect. Scammers thrive due to a number of factors only some of which is related to technology. Other factors include human behaviour, unwarranted trust, difficulty in investigating criminals located overseas as law enforcement is defined within geographic borders, and limited resources.

How has the ever-involving modernisation of banking services and social media affected the cyber security of individuals?

People volunteer personal information on social media such as LinkedIn, Facebook and Twitter. We have seen time and time again how this publicly available information is harvested into an automated tech tool to assist with cyber fraud. The modernisation of banking services is a double-edged sword. Many banks have exceptional fraud detection tools that are also AI enabled. While the cybersecurity of the individual may be affected, banks have become more adept at preventing, deterring and protecting individuals and business.

How real a threat is cyber security to the average Australian small business?

Cyber threats are an even greater challenge and threat to small businesses than they are to large businesses. I have seen small businesses hit hard by cyber fraud or attack. They often don't have insurance and can't afford to lose the amount stolen.

CYBER FACTS: "The myth is that scammers are always one step ahead in terms of technology," says cybersecurity expert Dr Alana Maurushat.

> Devices are listening to everything! This frightens me a great deal, more than criminals in my systems.
>
> **Dr Alana Maurushat**

Are corporates more or less susceptible?

Absolutely not. Cybercrime does not differentiate between sizes of companies. Breaches and fraud against small business often have a much more substantial effect on the business too. Cyber attackers use methods tailored for small business and different methods for larger corporations. The only difference is that larger corporations are more likely to be involved in sensitive commercial matters, have valuable intellectual property (IP), and participate in tenders for larger contracts. Competitors are increasingly gaining access to other competitors' IP, tender details and other data in order to gain commercial advantage.

What are the most common breaches of cyber security that affect businesses in Australia?

Data breach, payment diversion fraud, ransomware and IP theft. Ransomware is a form of malware that locks the user out of their files or device, then demands payment to restore access.

Where do "attacks" come from?

Everywhere, but it is often difficult to ascertain as technologies are used to make trace-back to the source extremely difficult.

What are cost effective way for businesses to protect themselves?

Cyber insurance. Work with a company dedicated to cybersecurity from a holistic approach, not just a 'sell you software' approach. Cybersecurity is NOT a technical problem.

Scammers use AI to leech money, how can companies use it to their advantage?

They can invest in products that utilise AI (most security products do this already) to gather smarter intelligence that better enables detection and mitigation.

What will be the biggest concerns in cybersecurity in the next five years?

Internet of Things (IoT). There is virtually zero cybersecurity built into IOT devices, such as Google Home and Amazon Echo, and the surveillance aspects is pervasive and largely unregulated. If you have one of these devices, or even a mobile phone, start to talk about a disease that you don't have, and have never searched for before. Watch how advertisements directed at this disease begin to pop up when you use social media and Google afterward. These devices are listening to everything! Try to get travel insurance quotes, before and after you've done this, to see if they are priced the same. This frightens me a great deal, more than criminals in my systems.