STORY ALAN DEANS

At war in the cyber world

Chaos reigned in Victoria's regional hospital network some weeks ago when a cyber attack installed ransomware on its computer systems. Hackers tried to steal millions of dollars in what is an all-too-familiar story.

Earlier in the year, a separate cyber attack had emails attempting to steal identities to access Paypal accounts. Another attack included sham emails claiming to be from the CIA and threatening to expose alleged online sexual activities unless people paid $10,000 in bitcoin. Then an apparent intrusion from China on major political parties and Parliament House was exposed leading up to May's federal election. It seems there's no end to the threats posed by the internet.

Are we fighting a losing battle? Matthew Wilson doesn't believe so. He is a founder of Penten, one of a growing number of home-built cyber security businesses doing their darndest to turn the tide in our favour. Australians, it seems, increasingly are developing effective capabilities to fight hackers.

"Don't get me wrong, it is still an arms race," says Wilson. "It always has been. Defence is a lot harder than attack. With attack, you just need one successful vector, but from a defence perspective you need to cover a lot of bases. The pendulum shifted very much towards the attacker five or so years ago."

He says this pendulum is again moving closer to balance. Part of the reason is the level of sophistication, scale and seriousness with which organisations are starting to treat cyber security threats.

Fact file

Matthew Wilson

Co-founder of cyber security firm Penten; age 46; lives in the southern suburbs of Canberra.

He was gifted a $1000 share portfolio from his grandfather at 16, leading to a life-long interest in investing. Enjoys cycling, supports Team Ineos, a multi-winner of the Tour de France, and invests in a cycling tech company. Grows vegetables, recently planting tomatoes, zucchini and cucumbers for the summer.

"They have really been through pain. Our small businesses have been particularly hit by ransomware over the last five years. Organisations can no longer afford to not think about cyber security," says Wilson.

The annual cost of cyber attacks to Australia probably exceeds $1 billion. A recent Accenture global survey estimates the average cost per company in 2018 at $US13 million ($19 million), up 72% in five years. The most common attacks were from malware, followed by web-based attacks, denial of service, malicious insiders and then a combination of phishing and social engineering.

The report warns new age hackers are no longer simply trying to steal data. They now want to disrupt and destroy industrial control systems by attacking data integrity. Sometimes this can involve the use of malicious insiders.

Penten's three founders have more than 20 years' experience in cyber security, initially using offshore technology to secure government networks. More recently they spotted an opportunity to develop capabilities of their own.

"There were a bunch of problems that we could no longer wait to be solved overseas first," says Wilson. "We saw a clear need for an organisation that was building cyber capability here first in Australia, and then exporting to the world."

The challenges they are tackling are ones that haven't been solved globally. That way, they hope to establish a competitive advantage that will prise open export markets.

Penten is focusing on two areas. One is secure mobility. High level government workers haven't been able to use mobile devices like laptops, tablets and mobile phones because they aren't secure enough. That hampers their ability to work effectively.

The business's team of 72 techies has developed software that provides high-level security for mobile devices and has a range of new products in the pipeline. This work led to the company being named Australian Business of the Year in 2018 at the Telstra Business Awards. Wilson was also EY's 2019 Entrepreneur of the Year (emerging male category).

Penten's second focus is to apply machine-learning artificial intelligence to thwart malicious attacks in the cyber arenas of defence forces.

"The technologies in the hands of cyber criminals are particularly advanced," he says "Crime knows no bounds, so threats come from all over the globe. We focus on emerging threats, and look at developing maturing

"The technologies in the hands of cyber criminals are particularly advanced. Crime knows no bounds."

Plan for the worst ... Wilson says businesses need to think about how they would keep going in the event of a cyber attack.

technologies that we can implement in Australia and then take to overseas clients."

An important client is the army.

Penten's work is based around the idea of decoys. For example, it creates artificial documents that are inserted into online directories to trap hackers. The content has no relevance to the directory, which might for instance be about a submarine propulsion system. People authorised to use the system have no reason to open such a decoy document, simply because it shouldn't be there and has no use. But an unwitting hacker doesn't know that. If it is opened, then the system is tripped. Everyone then knows a hacker is at work.

With the army, Penten is taking this work further. "In some instances, decoys can be used to confuse hackers," says Wilson, "For instance, if there is one vehicle moving through a battlespace but the wireless emissions [seen by a hacker] look like there are 80 vehicles, that can be used to confuse.

"When you're creating those 79 decoys, the emissions aren't real. Any interaction with them would show that someone was trying to have a go. There's no logical reason for anyone to interact with wireless communications coming off a decoy."

A battle commander would then know someone was probing their movements. He could try to confuse them, perhaps causing them to put their resources in the wrong place. Penten's battlefield system is still being developed and tested, but its document decoy program called TrapDocs is in commercial use.

"If we look back through all the major data breaches that have been documented even over the past five or 10 years, they all had enough information to know something bad was going on," says Wilson. "They just couldn't get to the information quickly enough. That's part of the reason why we created TrapDocs."

> "I like engaging with motivated founders and management to crack ideas that can have global impact"

Penten doesn't directly engage in the broader cyber security market. But Wilson says technologies developed within the government space always find their way into the enterprise environment. "Thinking about all the major technologies in IT security, whether it be firewalls or antivirus or sandboxing or log correlations, they all have their seed. They all began in a government environment."

The initial founders first worked together in a company called iSecure. It was purchased by SecureNet, which is where Wilson worked. Sometime later, the US telecoms giant Verizon bought the group. The team then formed a new business, M5 Network, which was later bought by US defence contractor Northrop Grumman. Clearly, its work is good enough to draw international interest.

"I am always genuinely surprised that people are perplexed by the world-leading capabilities coming out of Canberra. My answer is, 'Why wouldn't you expect it to be?' We have an amazing set of people. Canberra has four universities. We've got close access to federal decision makers, and those that have some more difficult problems within our space. It's a ripe environment and a very strong entrepreneurial culture. By the way, we're not alone. There are some amazing organisations here developing world-leading capabilities."

So what advice does he have for businesses to survive a cyber attack?

"I tell them to think about cyber in the context of it being a continuity problem. If your networks didn't exist for six hours or 24 hours or seven days, how would you survive? How would you recover? How would you be able to support and service your clients? They need to realise what the real impact would be, and having a clear business continuity plan rather than leaving it up to the IT people."

Wilson grew up in Melbourne, but has either lived in Canberra or commuted there for the past 20 years. As a youngster, he wanted to be a marine biologist, but his career kicked off in accounting.

It was only when he entered university that he realised ledgers were not for him, so he turned his focus to corporate strategy before becoming an entrepreneur.

"These days I have investments in property and other places, but my focus is really to support and invest within the venture sector. It is not for the fainthearted. You need a clear understanding of the risk profile that you're operating in. But I like building things, and engaging with really motivated founders and management to crack ideas that are genuinely important and can have global impact."

Influential people in his life include his wife, Joy, who put her career on hold to allow him to develop tech companies. "Without her, there was no chance of me being able to generate the success that we have had."

He also says that his father, Spencer, who owned a factory making doors and windows, was a valuable role model. "He's one of the more conservative businessmen I have ever met. I've always gone a bit to the right of him."