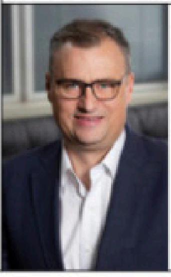
MAY-JUNE 2020 VOL.28 NO.5

ADM

AUSTRALIAN DEFENCE MAGAZINE

SERVING THE BUSINESS OF DEFENCE

VIEW FROM CANBERRA THIS MONTH ON ATTACK CLASS AIC CHALLENGES



ADM EXCLUSIVE

FROM THE SOURCE

Matthew Wilson CEO and Founder of Penten speaks to *ADM* this month

WWW.AUSTRALIANDEFENCE.COM.AU

Cyber in the Defence domain

Cyber protection and security is at the core of Defence and Defence Industry across the entire supply chain. How do we maintain the high levels of protection and mobility that users expect?

PRINT POST APPROVED 100008807

CYBERSECURITY FOR DEFENCE INDUSTRY

It's 2008. The US sub-prime mortgage crisis is dominating the news. Lehman Brothers has collapsed in America's largest-ever bankruptcy filing, the American stock market has dropped almost 40 per cent and most talk is now of the worst economic event since the Depression.

EWEN LEVICK | SYDNEY

GETTY

The cyber landscape security is just as important as the physical security, if not more so.

AS THE HEADLINES focused on Wall Street, another news story emerged in November that was no less momentous in its own way. At an American military base somewhere in the Middle East, someone picked up a stray USB stick – possibly from a stationary cupboard or off a colleague's desk. It was no bigger than a cigarette lighter.

That person plugged it into a laptop and inadvertently sparked a chain of events that would eventually land on the desk of US President George W Bush: the worst breach of military computer systems in US history.

The attack hit US Central Command, the HQ responsible for Middle East operations, and worked to pass on information on combat operations to a foreign state. It was described as a 'digital beachhead' by then-Deputy Secretary for Defense William Lynn, writing in Foreign Affairs.

"The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the US Central Command," Lynn said. "That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control.

"It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary."

Just two years later, researchers in Belarus were troubleshooting Iranian computer networks and found a code that has since become one of the most famous cyber-attacks in history – the Stuxnet virus. This is thought to have entered Iran's nuclear centrifuges, which are physically and digitally isolated from the outside world, on a USB stick.

> **"IT WAS A NETWORK ADMINISTRATOR'S WORST FEAR: A ROGUE PROGRAM OPERATING SILENTLY, POISED TO DELIVER OPERATIONAL PLANS INTO THE HANDS OF AN UNKNOWN ADVERSARY."**

THE THREAT TODAY

Twelve years later, the cyber threat has grown and evolved. Most people are now aware that buying a USB from a dollar store and plugging it into a secure network is a bad idea.

"Everybody knows the story – a few years ago, if you spread USBs freely you'd be amazed how many people plugged them in," Penten CEO Matthew Wilson said to ADM. "It's amazing. But I think education has moved us past a lot of that."

Yet a growing number of cyber criminals means the threat has not decreased. Troy Hunt, founder of data breach tracking website 'Have I Been Pwned?', has used the example of a breach of UK telecom TalkTalk to illustrate the point. The 2015 incident caused £77 million in damages and was initially attributed to 'Russian Islamic Cyber Jihadis' by police, before it was eventually discovered to be the work of two teenage boys.

"It strikes me that it is so often children breaking into these systems," Hunt said. "Kids have access to so much material to do this."

Highly-sensitive government networks, such as those used to run Iran's nuclear program, are physically cut off, or 'air-gapped', meaning hackers need a person – knowingly or otherwise – to carry their virus into the system. This puts them above the reach of many casual cyber criminals.

Many networks in Defence and the industry supply chain, however, cannot be digitally isolated from the rest of the world and are therefore vulnerable to those looking to deal damage or steal money. Therefore, as governments and militaries improve their own defences, malicious actors are turning their attention to an area in which cyber risk management is not standardised.

In January, for example, Mitsubishi Electric confirmed that it had been breached by an attack that may have compromised defence and commercial information. The company said that 'highly sensitive' information was not taken, but email exchanges with Japan's Defense Ministry and Nuclear Regulation Authority were stolen along with employees' personal data. The attack originated from China.

Another case from Japan is that of Kobe Steel, which disclosed a 2015 breach followed by a second attempt a year later. Kobe Steel is involved in building Japanese submarines.

The cyber threat is also increasing for SMEs. Three years ago, over 500,000 small Australian businesses were hit by cyber-attacks. Only a third of businesses self-reported backing up their data.

INTENT

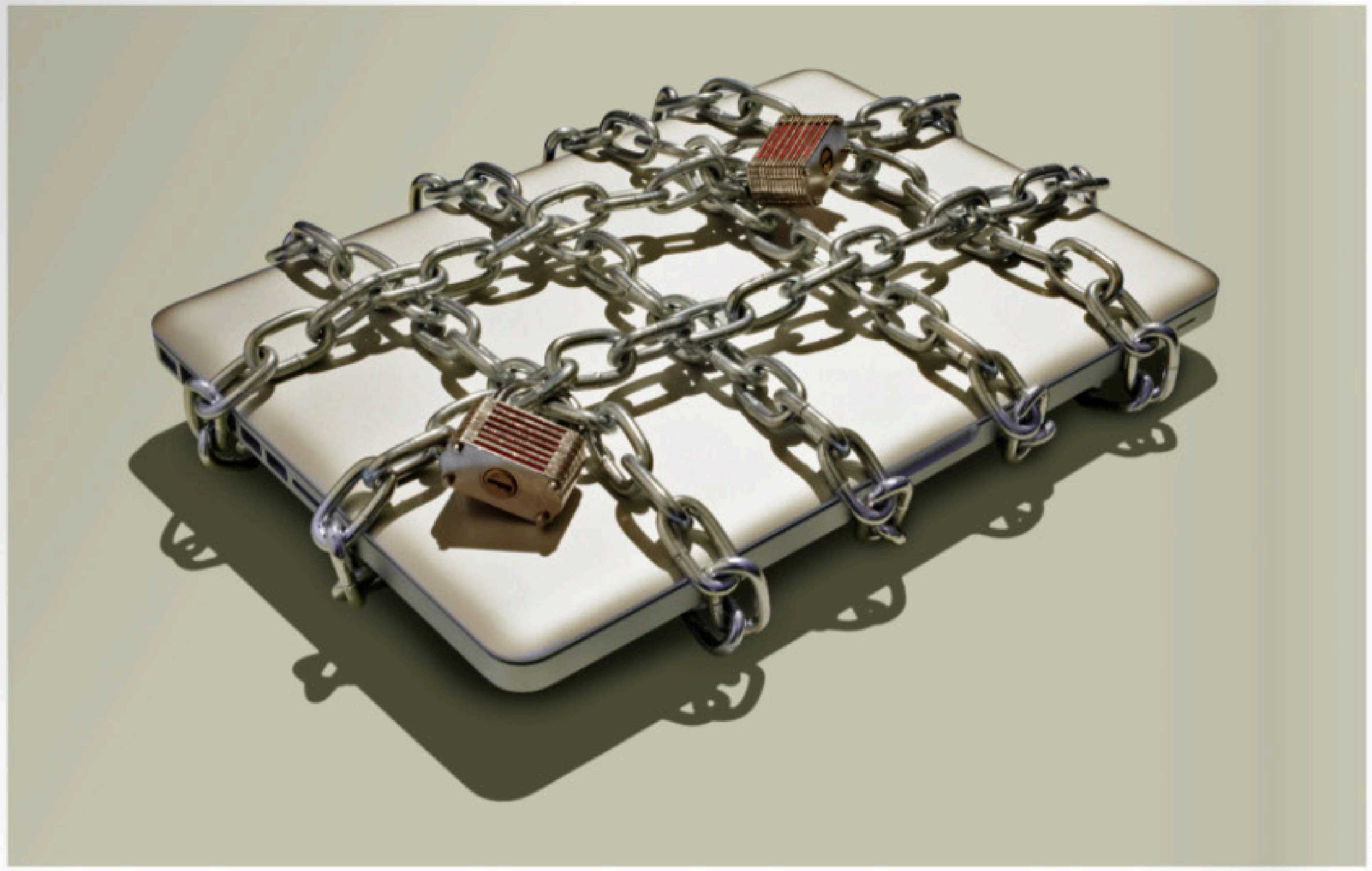
According to Penten's Wilson, the majority of cyber breaches are carried out with the intent of stealing money.

"The single biggest challenge in SMEs generally, and I include defence industry within that, is the age-old problem of criminals wanting to steal cash," Wilson said. "The simple way of looking at it is through a criminal's eyes. Criminals are motivated by cash and will spend as much as needed to get a return out of an individual or small businesses."

The risk is compounded for SMEs in the defence supply chain, who may have to contend with state-funded actors seeking access to military secrets in additional to non-state cyber criminals looking for easy money.

"In the context of defence industry, we have a range of additional cyber threats to the general SME populace," Wilson said. "We have to make sure we're supporting Defence by making it as difficult as possible for foreign adversaries to be able to use the machinery of defence industry, especially SMEs, to be able to lessen the advantage that the ADF has."

Digital avenues of attack, however, are widening as defence industry digitises concepts and processes. For example, Australia's first digital shipbuilding course began at the beginning of April for workers involved in the Hunter class build program, which will use an advanced 'digital shipyard' in its 'Industry 4.0' approach.



GETTY

"Businesses are on a path to digitise as many elements as they can, whether it be the actual entirety of what they do, or the machinery that's orchestrating and delivering some of their physical capabilities," Wilson said. "I think about it this way – over many years, we've developed physical security procedures that we have around our businesses, and some of the logic of that needs to transfer into the digitisation of our processes.

"We don't leave valuables in the back of an unlocked car, or even a locked car if it's visible. Some of those parallels are lessons some organisations are still learning."

GREAT EXPECTATIONS

Overall, education and advocacy, particularly on the part of government, has increased expectations of organisations and employees through the supply chain.

"You should be able to maintain a level of hygiene that means you're not low-hanging fruit from a criminal or foreign adversary perspective," Wilson said. "There are no excuses anymore."

Yet that does not necessarily mean that expectations are the same for all organisations. Government bodies and primes have a leadership role to play, even if all companies should strive for proper cyber hygiene no matter their size.

"Primes have a responsibility for leadership back within their supply chains, and they are absolutely taking hold of that. Some of that has been driven legislatively, particularly out of the US, and some of that flows down into the subcontractors here in Australia through requirements within their subcontracts," Wilson said. "But actually those requirements are not really different from what their requirements would be otherwise."

There is also the obvious: there is a difference in cyber requirements between primes and SMEs because there is a difference in the volume of information they possess, and the procedures in place to manage that information accordingly.

"Cyber requirements might seem ubiquitous, but they're not. You can think about it most easily at the extremes," Wilson said. "If you're a micro business supporting defence industry, and you're one person, your ability to manage and capture and understand the information within your space is very different to an organisation of thousands in which the central knowledge of information is being stored and treated."

CYBER COMPLIANCE

Expectations can also change quickly. Towards the end of last year, the US Department of Defense brought in the Cybersecurity Maturity Model Compliance (CMMC) to try and control damaging numbers of data breaches affecting almost six per cent of the American defence supply chain. Unlike the current model of self-evaluation, the CMMC is a 'unified cybersecurity standard' for military acquisitions that will apply to all US defence contracts irrespective of the bidders' nationality from June this year.

That is a quick turnaround. Despite concerns from within the US about the speed with which the CMMC is arriving, the Department of Defense is not budging.

The fundamental change in cyber expectations on companies bidding for US work is one of initiative. Rather than meeting cyber requirements once contracts are won, companies will have to demonstrate compliance to the CMMC before even responding to a request for tender.

"If you cannot demonstrate compliance certification to the level required in the RFI, don't bother calling," Ray Harvey, of Cider House ICT in Melbourne, has written for *ADM*. "CMMC will be the price of admission to the game."

PERSONNEL SHORTAGES

A separate challenge in Australia's cyber landscape is the on-going shortage of skilled ICT professionals. Last year, Telstra decided to move a number of jobs to Bangalore after predicting that Australia would have a shortage of 60,000 ICT workers within five years.

"We cannot find in Australia enough of the skills, like software engineers, that we need on the scale that we need them," CEO Andrew Penn said in a speech. "There simply are not enough of them. The pipeline is too small."

> **"AUSTRALIA IS PUSHING OUT WORLD-LEADING TECHNOLOGIES AND CAPABILITIES – THAT IN ITSELF IS EXCITING AND SOMETHING TO PROTECT."**

Like skills shortages in other STEM areas, the number of qualified workers available to Australia's defence industry is even smaller given stringent vetting requirements. This means that visa schemes like the 'Global Talent Independent Program', which aims to attract 'future-focused' skills into Australia, are unlikely to alleviate the issue.

"The rapidly accelerating demand for software services in Australia provides a clarion call to government and policymakers alike to help support an industry long faced with skills shortages and systemic issues concerning STEM participation," Peter Nguyen-Brown, co-founder of Australian tech start-up LiveTiles, said. "Critical skills in agile methodologies, software-as-a-service, business process improvement and software development are all in high demand."

Even the Australian Signals Directorate struggles with this issue. Former head Mike Burgess famously brought the service 'out of the shadows' in a 2019 speech to the Lowy Institute in order to drive recruitment, particularly of women. Burgess had previously highlighted competition with the private sector as a weight on the number applications the organisation was receiving.

AI AND MACHINE LEARNING

So what does the next few years look like in defence cyberspace?

A common answer is blockchain technology, famously used to create cryptocurrencies like Bitcoin. According to Wilson, however, this isn't particularly useful in a defence context.

"It has fairly specific use cases for non-reputability, but in the context of defence requirements it's not a technology that is likely to be widely adopted," Wilson said.

Instead, Penten is looking to machine learning and its potential implications on warfighting itself, which will increasingly be a contest between machines.

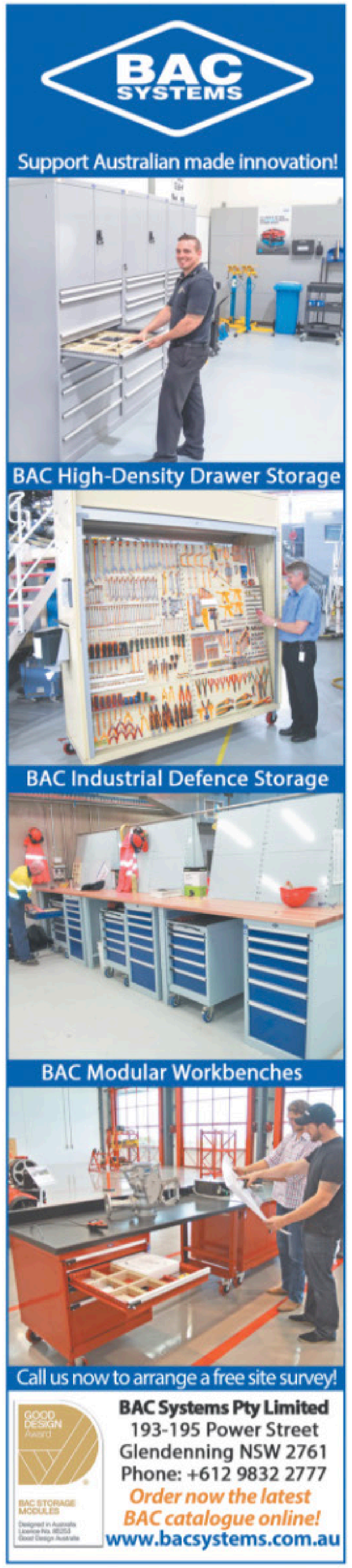
"Penten quite specifically is orientated around the logic of the Internet of Military Things and the expected outcome of machine-on-machine conflict," Wilson said. "We're building the pieces that are missing to ensure Australia and its allies have the advantage when this happens."

The company is tackling the concept from two angles. First, it is bringing government-grade encryption technology out of secure buildings and into more mobile technologies, including mobile phones. Second, it is researching ways in which machine learning can protect the networks machines use to talk to each other.

"We're only just beginning to understand the genuine advantage of machine learning and AI in terms of efficiency, speed and precision in ways we've not previously been able to achieve," Wilson said.

He is also adamant that Australia is the right place to be for a cyber protection business like Penten.

"Australian defence industry isn't just about the domestic implementation of foreign solutions anymore," Wilson said. "Australia is pushing out world-leading technologies and capabilities – that in itself is exciting and something to protect." ■



FROM BUNKERS TO BUSINESS: VETERAN CYBER STARTUP

"Have a cup of tea!" Cyber security expert Jared Cunningham's typically British response to being asked for his top tips on dealing with sudden and significant change.

ADM STAFF WRITERS

With a nearly 20-year defence career behind him, including serving in Afghanistan as an infantry platoon commander with the Yorkshire Regiment, the founder of Ravinn – a Brisbane-based cyber security company – understands well the feelings of stress and fear that can overwhelm people during challenging times.

"People are feeling a great deal of pressure at the moment, but it's essential to pause, to think, and then to move on," Cunningham said. "There are often things that are completely out of our control, so give yourself time to think about the things that ARE within your control – what you CAN do and what you CAN change."

Ravinn has recently been called on to help companies quickly pivot from a traditional model of working in an office space to a work-from-home environment – a scenario that can leave organisations vulnerable to cyber threats.

"We have several clients for which we provide CISO (chief information security officer) services. We're on call when they have an IT security issue, but the current rush to work from home poses a threat. It's easy to set yourself up to work from home these days, but to do so securely is different."

"We've recently seen a massive increase in deliberate social engineering and phishing attacks. Hackers and criminals are making the most of what they see as an opportunity. They're relying on people making mistakes and clicking on links and can easily fool people into believing an email they've just received is from the CEO when in fact it's been spoofed," Cunningham explained.

MATTHEW WILSON

CEO AND FOUNDER OF PENTEN

Canberra-based Penten have only been around for a few short years but are making their mark globally in the secure mobility space and cyber protection. *ADM* Managing Editor Katherine Ziesing posed some questions to founder and CEO Matthew Wilson about their journey and what's on the horizon for the growing SME.

PENTEN

ADM: The pilot program to protect Defence SMEs – can you outline what that is and why it's needed?

WILSON: One of the things that we've realised, especially as a small business that has been focused on defence and national security industry, is that it is the initial steps necessary to put in place the information protections to begin working within this space are a very big hurdle. The way it has to be done right now is a set of guidelines are given to you through the Information Security Manual and then you have to go and source and build all that capability yourself, and own it and know it and then get it accredited by yourself. That's probably fine if you're in the ICT space but if you're in not that space, if the logic of what you're doing is probably more in the physical capability space, then this in itself can be a particularly significant barrier.

What it really means is it's harder to move up the classification stack with regards to the capability that you're delivering as an organisation because you just don't have the infrastructure to be able to do it.

A simple example: if you just want to commence a secret network within a small business to be able to work on a tender proposal for Commonwealth or a submission as a subcontractor into one of the primes, you're talking probably about $300,000 to be able to implement a small amount of ICT just to be able to produce the document that allows you to deliver. And so, as you can imagine, there's a raft of implications that come out of that. There's a bunch of SMEs that don't move up the classification stack because they don't want to take on that burden. It's a step too far, or even worse, they try and compartmentalise information so they don't trip that classification trigger, and that in itself isn't necessarily delivering the best outcome for Defence.

We've been having this conversation with CDIC (Centre for Defence Industry Capability), with the Department of Industry, with Defence, in fact the whole industry has been talking about this for quite some time. Everyone kept coming back to us and saying, 'Oh, some of your mobility technology, this would be perfect for this!' Our ability to enable a secure network extension that would, cost-wise, look mostly like what normal non-classified ICT might cost a small business kept coming up.

We put a proposal to create a pilot program that allowed us to test this, and to do it in a way where it's not just about looking a small pilot but also testing our ability to scale this environment. When we started to think about this, suddenly we were starting to put ourselves in a position where if we could implement a system of this scale, we were actually going to give Australia's Defence Industry a competitive advantage like nothing else that exists in the world right now. It also gives Defence and our national infrastructure around protecting cyber a central place where they could bring the national capability to bear to protect the entirety of the industry.

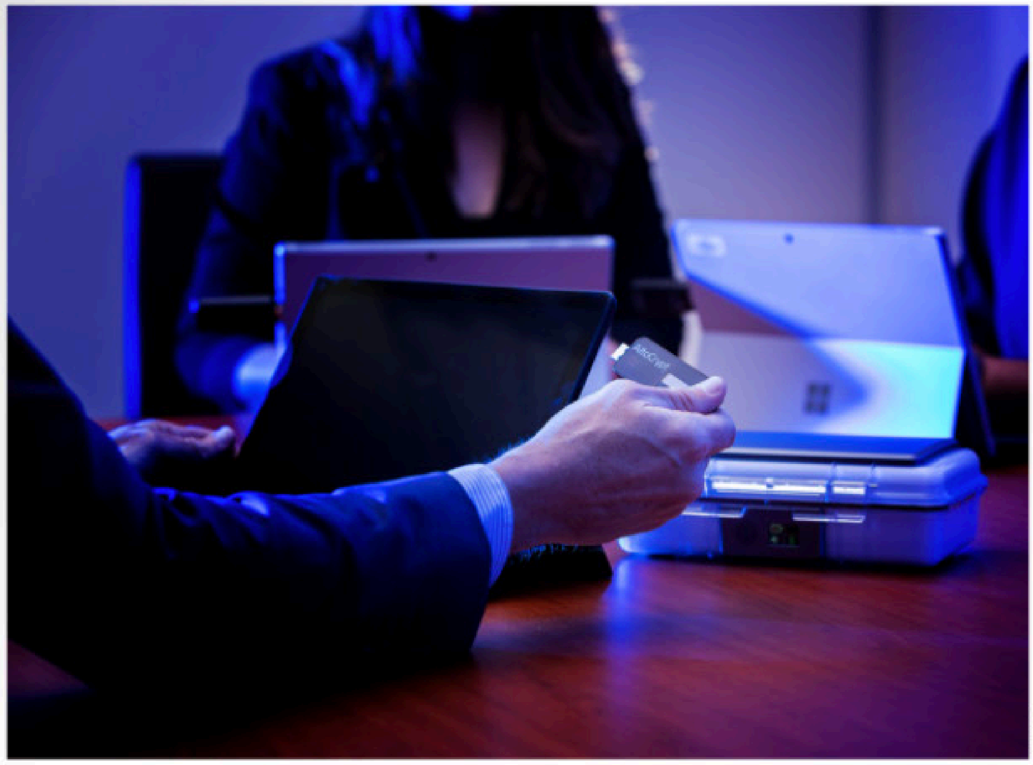
It is a small pilot but it in my mind it's particularly important because it shows that we not only have a solution to this requirement but this removes the handbrakes on innovation and our ability to really raise the bar on the cyber protections of our Australian defence industry.

What we've done with the pilot is really keep it nicely bounded so that we know that we can get a good working outcome and good learnings can go back into the Department of Industry and Defence. We can then say, 'Look, we've made all this investment and all this push into building this fantastic sovereign Australian defence industry,

PROFILE

2016	Co-Founder and CEO, Penten
2015	Non-Executive Director, Amiosec Ltd (UK cyber innovator) (current)
2015	Director, Today's Plan (training and analytics platform)
2012	Vice President, M5 Network Security (Northrop Grumman)
2003	Founder and Managing Director, M5 Network Security
2000	Business Development Manager, SecureNet Limited
1998	Business Analyst, Foster's Brewing Group Limited
1996	Secretarial Assistant, Foster's Brewing Group Limited
1994	University of Melbourne: B Comm, Corporate Finance

CONTINUED ON PAGE 46



PENTEN

LEFT: Secure mobility is everyday business for Penten.

CONTINUED FROM PAGE 50

we see some of the challenges that are coming down with regards to limits to its ability to grow and be able to participate more broadly in the global defence supply chain. Here is a strong competitive advantage that we can coordinate in country.'

We can coordinate and support a realistic cost based capability that will allow Australia's sovereign defence industry to stand out above the rest of its competitors and the world.

“WE CAN COORDINATE AND SUPPORT A REALISTIC COST BASED CAPABILITY THAT WILL ALLOW AUSTRALIA'S SOVEREIGN DEFENCE INDUSTRY TO STAND OUT ABOVE THE REST OF ITS COMPETITORS AND THE WORLD.”

ADM: A term that you've used a few times is 'secure mobility'. What does that mean? How does it affect users?

WILSON: We've talked previously about this idea of disconnected networks and this is a real challenge with the idea of broader digitisation. Digitisation works very well when you're connected to everything. But if you're working on classified networks that are disconnected, how do you access that if you're not sitting at your desk?

It's not just about working from home remotely, like we're facing today with regards to COVID-19, but also within our offices as well. One of the things that I keep describing to people is that 10 years ago you would never have expected in a million years to walk into a city train stop and see an advertisement for a job at one of the security agencies, but that is a thing that happens not just in Sydney's train stations, but it happens in a London subway as well.

And why? It's because our ability to attract and retain talent within the defence, national security and certainly in the operator policy making space is really built on our ability to create modern working environments. Being able to create the environments that will allow workers to use their brains the way it's been wired through high school and universities with mobile devices in their hands as part of their decision-making tools.

I'm almost 50. My university was rote learning things and if you're coming out of a university today, and certainly over the last few years, you do not do that at all. What you've learnt how to do is how to quickly find and bring together the information that you need and really add value on top of that; that is a significantly greater advantage to the nation.

My logic around that is we've got to think about the ways that allow us to create those tools to enable that generation of workers within that space. In some ways it's about that but also managing and supporting the protections that sit around military engineered things but more broadly it's about realising that in the defence space we will have more and more connected things and they will be more and more mobile and non-static places and still needing protection.

From Penten's perspective we've been focusing on building new technologies that allow that to take next step into secure mobility at every moment. We looked at the market globally and said, 'Here are the bits that are missing. Let's start building those.' And we're building them here from Australia and now exporting them to the world.

ADM: ASD is no longer certifying cloud providers on their security. What effect do you think this will have on the security of the sector more broadly?

WILSON: To be frank, it's been telegraphed for a while now so it was no surprise to anyone in this space. It doesn't mean it's not a bit disappointing but I also appreciate that ASD has and its ability to resource and execute on that remit. Part of that is really saying, 'We are an organisation that will provide advice, we will provide some direction where we can, but we will enable you to build the capability you, as a department or as an agency need to go and protect yourself.'

There are some elements of that that are difficult, because smaller organisations and smaller agencies aren't always necessarily going to have the same capability of evaluation for their own risk management purposes. It is in some ways an opportunity lost. I understand why ASD have gone down this path, but I'm also really mindful of the fact that there's some elements that need to take that place.

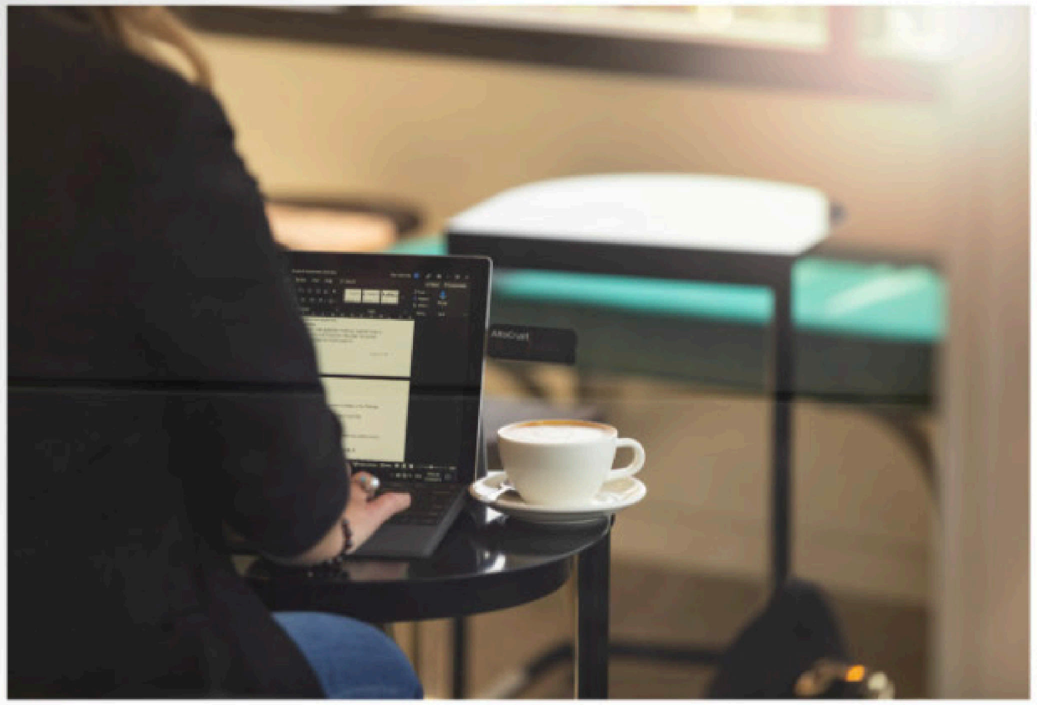
Now whether that's commercial organisations stepping up, whether there's some other support that's given, some structural support – something will need to step into that place because I just don't see every single agency being able to perform a blank sheet evaluation that allows them to make the informed decisions that they need to make.

ADM: The average time to detect a cyber security breach is 207 days. What can companies do recover from such breaches?

WILSON: The speed at which your recovery can take place depends on the amount of planning that you've done in the first place. You've got to have an expectation that an organisation is going to be breached. That might be big, it might be small but it's certainly going to happen. So your ability, the speed at which you can recover from that really depends on the planning that you've put in place to support that outcome.

The good news is there is an amazing cyber industry that's developing here in Australia at the moment and primed to be able to support organisations in managing through and recovering from those challenges that will take place.

Toll is a good example and a really salient reminder for us all (Editor's note: Toll deliberately shut down a number of systems across multiple sites and business units in February this year. The company said while only a small proportion of its freight was affected, it had apologised to affected customers and said there was "no evidence" personal data



PENTEN

LEFT: The AltoCrypt Stik enables secure mobility without the need for extensive cabling.

CONTINUED FROM PAGE 47

had been compromised); you need to invest the time, the money, planning and you need to have the relationships to be able to support your recovery process.

Because it will happen, and the question is whether it's a blip that causes you an inconvenience for 24 hours or whether it brings your business to its knees. The difference is genuinely up to the investments that you're going to make as a business in the days and months prior to that taking place.

ADM: Since being founded in 2014, what has the Penten journey been?

WILSON: The founders of Penten have built technology businesses in Canberra over the last 20-30-odd years really. Our thought process with Penten was about the realisation that there were a whole raft of challenges that were sitting in the defence and national security space that were not being addressed globally. This wasn't necessarily just about trying to support Australian capability, this was just about realising that we've got a bunch of amazing young engineers in Australia, yet the cyber challenges are growing exponentially.

But there is an opportunity in that growth globally and that we could orientate our engineering talents and capability on some of those global problems and for Australia to become a centre of gravity based in Canberra to support global programs.

As we sit here today after our first couple of years which were slow growth, we've really accelerated; we're doubling in size. Right now the team is about 80 people here in Australia; we have technologies that are being exported to the UK, NZ, Canada and other parts of the world. More of our tech is being used by the UK government than by the Australian government.

ADM: What lessons have you brought into Penten from ICT start-ups you've been involved with previously?

WILSON: I think the biggest lesson that I've had was really having a very clear understanding of your customer need and the environment that it operates within. The truth of the matter is that the defence and national security space is a little bit different to enterprise and respecting that the implementation of systems and systems to systems within those environments is actually quite important. You can scream at the clouds all you like but the environment is the environment and you're dealing with humans at the other end who are only given a left and right by which to operate.

So if you can find that orientation and know where those boundaries are, then you can bring everybody along for that journey. What that's meant for us is the speed at which we've been able to develop and mature technologies has been really built out of support and inclusion and participation by Defence and other parts of government in trying to build these solutions out. It comes with the knowledge, an expectation and understanding that we would be commercialising these, not only to support their outcomes but to support global customers.

ADM: How important are international contracts to your business?

WILSON: As I said, the UK government uses more of our technology than the Australian government does but that is changing quite rapidly at the moment. The UK for us has been very important. There's been an ongoing maturity of Australian government buyers in buying domestically made technologies and they hark back to bad old days, when government buyers seemed to assume that the only best tech was coming out of a foreign environment. That logic is not the same anymore. However, some of our procurement rules are still a little bit aligned to that logic; some technologies need to have been proven somewhere else before they're able to be implemented here in Australia.

But there is a logic now that allows people to stop and say 'No, if we're building Australian sovereign defence industry, it isn't just about implementation for our technology, it is about making our contribution back into the global defence construct. And it's not about having to make or do everything.'

> "THE SPEED AT WHICH YOUR RECOVERY CAN TAKE PLACE DEPENDS ON THE AMOUNT OF PLANNING THAT YOU'VE DONE IN THE FIRST PLACE."

ADM: How will AI (artificial intelligence) machine learning change cyber deception?

WILSON: So in a defence construct, deception has always been a very big part of the way that a commander will think about mounting operations. It's only been in more recent times that we've started to realise that from a defensive nature cyber deception technology creates some of the same opportunities within a digital environment. Just simple things; like we know that if we're trying to protect a piece of information, one of the things that we can do is to create decoy information that sits around it. When you see that decoy information outside somewhere else, we know that there's been a problem with the information that we've been trying to protect.

That's all great but it's all very mandraulic and very specific and so a couple of years ago we started to use, I would say very initially clumsily, but over the last three years have really to a world leading capability where we're using machine learning and AI to automate the process of building those decoys, making realistic decoys that are capable of effective deceptions and allowing us to build traps or track who is trying to steal some data. Or actually even better than that, really change some of the behaviours of those adversaries.

When we start to think about deception automation using AI, we've been doing it with documents, network traffic, network devices, or RF traffic. We've been doing it with a raft of digital and communication environments to be able to create a new generation of tools that are either effective counter-intelligence, detection or behavioural modification tools where we can modify the behaviour of the adversary to our advantage. ■