DELL Technologies

vmware

Accelerating the Cyber Resilience Mandate

A CXO's Imperative

Each year the cyber threats faced by Australian organisations continue to mount, placing greater pressure on cyber and security executives responsible for defending against them. Building resilience in the face of an evolving threat landscape was the key topic of discussion for a roundtable series of leading Australian technology and cyber security CXOs, convened by Dell Technologies and 6 Degrees Media. Guests including one of the world's sought after cybersecurity experts, **Mikko Hyppönen**; and the Australian Ambassador for Cyber Affairs and Critical Technology **Dr. Tobias Feakin**, joined Dell Technologies' General Manager for Data Protection Solutions **Lucas Salter** in a robust discussion about the nature of the threats in the current landscape – and the essential steps required to defend against them.

Top (left to right): Mikko Hyppönen, globally renown cyber security expert; Dr. Tobias Feakin, Australian Ambassador for Cyber Affairs and Critical Technology. Bottom (left to right): Lucas Salter, General Manager for Data Protection Solutions, Dell Technologies; Brad Howarth, Journalist/Moderator.

It's no exaggeration to say that cyber threats today are universal. Australian Cyber Security Growth Network (AustCyber) estimates that cyber-attacks are costing the Australian economy $29 billion annually. The impact of cyber-attacks is not measured purely in financial losses. According to Dell Technologies' *Digital Transformation Index*, almost a third of Australian and New Zealand IT decision makers cite data privacy and security concerns as a barrier to digital transformation. And then there's the immeasurable cost of reputational damage, which some experts claim is difficult to repair.

Defending against these threats is a complex and potentially expensive exercise, requiring careful planning and decision-making.

But they are decisions that globally renowned cyber security researcher and practitioner Mikko Hyppönen is very familiar with. Hyppönen has lectured on cyber security at Stanford, Oxford and Cambridge Universities, and was ranked as Cyber Security Person of the Year for 2020 by *CSO Magazine*.

He said that the critical starting point for any organisation when future-proofing its cyber defence was always to ask itself some very basic questions.

"One of the core things you should be doing when you plan how to secure your organisation is to think through the potential attackers," Hyppönen said. "What kind of an organisation are we? Who would like to attack us? Who would like to steal from us? Who would like to

make us look bad? And so on. That helps you put your limited resources and limited budget in the right place."

His sentiments were echoed by Dell Technologies' General Manager for Data Protection Solutions Lucas Salter, who said the most common pain points discussed by clients were where to start and what to do next.

"A lot of investments have been made in this space, and organisations still don't feel comfortable with their position across cyber resilience, across recovery of platforms, and across their ability to secure their environment," Salter said. "Data growth and proliferation of the locations where their data and applications reside is really making that 'what to do next' challenge a big one.

"And when they're adding to that competing budget priorities and resourcing challenges, it's really a difficult decision."

The Importance of Engagement

According to Hyppönen, every single successful attack could be categorised in one of two ways: as either stemming from 'technical problems' or 'people problems'.

"The technical problems can be really hard, slow, and expensive to fix. But at least we know we can fix them," he said. "You find the bug, you fix the bug, you apply patches, you update everything.

"But there's no patch for humans, there's nothing we can do to just supply a patch for our employees and make them avoid phishing attacks. The only way we can do that is through education, and this is even slower, even more expensive, and harder."

However, Hyppönen said this hadn't stopped organisations from stepping up to the challenge using training, which he said worked best when it was ingrained in a worker's everyday life – especially when it could be turned into a game or corporate challenge.

"In some organisations, people really get into it [corporate challenges] and really start paying attention to the emails they get, which is exactly what we'd like them to do, if we want them to avoid attacks like these," Hyppönen said.

The problem of how to raise awareness of cyber issues is a familiar one for Dr Tobias Feakin, although in his role as the Australian Ambassador for Cyber Affairs and Critical Technology he takes on the challenge at a national level. Dr Feakin described the best approach as being to get everyone to understand that cyber security is a team sport that needs everyone to participate.

"The problem that we have try to address is that this is one of those security issues that affects everyone across society," Dr Feakin said. "Whether you are an individual citizen at home, or the top CEO or Prime Minister of a country, you will at some point be affected by a cyber security issue."

Case studies and examples were also great tools for driving change, but Hyppönen said all too often organisations waited until they themselves were the victim of a breach before taking the necessary steps to prevent another one.

> **"The technical problems can be really hard, slow, and expensive to fix. But at least we know we can fix them. But there's no patch for humans, there's nothing we can do to just supply a patch for our employees and make them avoid phishing attacks."**
>
> – Mikko Hyppönen, globally renown cyber security expert

> **We are seeing communication across different teams and departments growing, and having different stakeholders coming to the surface and identifying priorities at a more rapid rate.**
>
> – Lucas Salter, Dell Technologies

Doing this work before a breach took place was a much rarer occurrence and required elevation of cyber awareness to the board level. Unfortunately, he also suggested that many board directors lacked sufficient awareness of digital and cyber concepts to engage in these conversations.

One senior security attendee, however, volunteered their own successful strategy for building board engagement.

"We were struggling to get our board to recognise the risk, and we tried to bring it to life through cases and other means. In the end, we went to the dark web and got the prices that people were willing to pay for personal information, and brought that to the board. And when they could see this was real for them on a personal level, the conversation switched to how they could invest to make sure this information wasn't lost."

Sharing the Burden

While threats are ever-present, a clear message to attendees throughout the discussion was that they were not on their own.

Dr Feakin described how governments and industry were working together with international partners to understand and combat threats.

"The way that we're going to get out of this is through international collaboration, information sharing, and better relationships with each other as humans and through our various networks," Dr Feakin said.

"We do that through sharing information on various threat signatures. We distribute that through our computer emergency response teams globally. We do that through bilateral operational channels directly. And we also do that in terms of sharing with the private sector."

Dr Feakin said another critical action was the work being undertaken internationally to raise the risks for cyber criminals, as a way of deterring them from this kind of activity.

"A really good example of where this had benefit for all of us across government and the industry, was around the managed service provider issue that we highlighted in 2018," Dr Feakin said. "We shared the threat signatures and used it as leverage to get that information out there as far and wide as possible, so that business could protect itself."

Salter described how Dell Technologies was working with organisations to help them conduct exercises that brought together stakeholders to improve awareness and communication.

"We're seeing more conversations and decisions not being made in isolation, but in fact being made collaboratively," Salter said. "We are seeing communication across different teams and departments growing, and having different stakeholders coming to the surface and identifying priorities at a more rapid rate."

Defence in Practice

Attendees discussed how the diversity of threats and the options available to defend against them could result in a baffling range of options, with little clarity

regarding whether they had done enough to protect their organisations.

As one attendee asked; "I understand that constant investment needs to be made, but when do you know enough is enough?".

According to Hyppönen, this was the core question for defenders everywhere. "Even when you do your job right, people are not sure if you've done anything at all, because rarely is anyone thanked for stopping the disaster that did not happen," he said. "But if we fail, and when we do fail, it can be very visible.

"You know you've done your job when nothing happens, and you hope that it wasn't just luck, but it was actually something you did."

Salter suggested that existing frameworks such as the NIST Cybersecurity Framework supplied a roadmap for how organisations could develop their cyber capabilities.

"The organisations that we see operate with best practice are those that are taking a holistic view and getting across multiple stakeholders to understand and take an informed position of risk that they can move forward with," Salter said. "There's no real one silver bullet that's going to solve the problem."

As Hyppönen pointed out, the problems continue to evolve, also. One example he gave was with regard to ransomware. As organisations have learned to better protect themselves from ransomware attacks through use of strong backup regimes, criminals in turn have changed their focused to what he called Ransomware 2.0.

"Here, attackers saw that less and less of their victims paid the ransom, so now we are seeing this new tactic which started in 2020 where if you don't pay the ransom they will start leaking your information," Hyppönen said. "And this is the reason why we have seen so many multimillion dollar ransoms paid over the last 12 months. And with Ransomware 2.0, your backups don't help you at all.

"So if you can't keep the attackers out, the next best thing is to detect that you have been breached as quickly as possible so you are able to react and stop the attack before they are able to carry it through."

Hyppönen did suggest however that there might be light at the end of the tunnel in terms of spending, which he expected would not continue rising indefinitely.

"I think we are getting better," he said. "If you look at the defences that everybody has at their disposal today, and what we had 10 years ago or 15 years ago, clearly we have much more advanced defences. If you look at the kind of attacks we used to see, none of that would work today."

But he said as long organisations kept making their environments more complex, the threats they faced would grow. "The best thing we can do is simplify, and that's an easy thing to say, and hard to do," Hyppönen said.

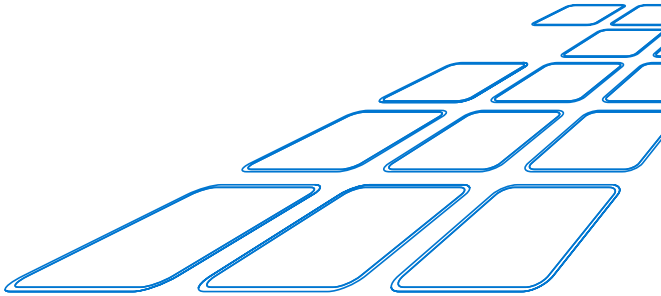
"We all know legacy systems never die and more and more code keep getting added to the systems we use. But I think we are on the right track and I think eventually it's going to get better."

AI and ML on the Horizon

While the arsenal of tools available to cyber criminals was vast, Hyppönen said there was one emerging technology that had yet to be fully weaponised – artificial intelligence (AI) and machine learning (ML). Indeed, Hyppönen said many CISOs were probably already using these tools, as they were often embedded in popular cyber defence tools.

"The amount of samples, the amount of attacks, the amount of network traffic every security company has to wade through today is way too big to be done with human power, and that's why machine learning systems

While the arsenal of tools available to cyber criminals was vast, Hyppönen said there was one emerging technology that had yet to be fully weaponised – artificial intelligence (AI) and machine learning (ML).



> **I hear that everyone's fatigued. It's relentless, this work. But I'm always inspired by the motivation of those who are doing this work, and I find that incredible.**
>
> – Dr. Tobias Feakin, Australian Ambassador for Cyber Affairs and Critical Technology

have been a crucial part in our defence," Hyppönen said. "Now, when we look at the attackers, we actually aren't seeing machine learning-fuelled attacks from criminals in large scale, yet. It's obvious that this will happen, because there's great benefits for attackers from using code which learns how to modify itself, or phishing attacks, which learn what kind of attacks work and which won't, and adjusts as such."

Where criminals had taken an interest in AI and ML, however, was in attacking the systems that used it by poisoning data sources.

However, Hyppönen believed the inevitability of AI-based attacks should concern all executives today.

"The barriers for entry are getting lower and lower," Hyppönen said.

"You used to need a couple of PhDs if you wanted to program machine learning systems. That's getting easier and eventually any person off the street will be able to use machine learning systems and that's when we'll start seeing malware and other attacks using machine learning systems."

Hence, Hyppönen stressed that one of the smartest things any CXO could do right now was to educate themselves about AI and ML.

"The chairman of our board went back to university to go through a programming course on how to program machine learning systems, just to understand what it really means," he said. "So read a book, watch a video, go and take a course so you can really understand what it is."

Another technology that was also causing concern for CXOs was the Internet of Things. Hyppönen recommended that attendees could reduce their threat surface by thinking carefully about the devices they deploy, as his eponymous *Hyppönen's Law* described how adding intelligence to any device served to make it vulnerable.

As for longer term solutions, Hyppönen also recommended attendees investigate the concept of deception technologies, which could mislead attackers who were able to gain access to networks and cause them to hit 'trip wires' and expose themselves.

The Case for Optimism

Despite the potential for doom and gloom in the face of growing cyber threats, Hyppönen said he was happy with what the industry had managed to achieve. "I know it looks like we're failing when you look at the headlines, but the fact is we've improved people's security immensely over the last 15 years," he said.

But as long as the threats remained complex and constant, Dr Feakin reiterated the need for people to band together to provide a united front. "Reach out to one another, start sharing information on what's going on, what your problems are," Dr Feakin said. "Treat each other as counsellors. Don't worry too much about process and structures, just get talking and start sharing.

"I hear that everyone's fatigued. It's relentless, this work. But I'm always inspired by the motivation of those who are doing this work, and I find that incredible."

DELL Technologies

6 DEGREES MEDIA
WHERE LEADERS CONNECT

About Dell Technologies

Dell Technologies helps organisations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

About 6 Degrees Media

6 Degrees Media was established by Angela Horvat, former Editor and Publisher of award-winning publications including *Computerworld, Information Age, My Business, The Who's Who of Financial Services* and Founder of FST Media; and Emma Charter, one of Australia's most connected and respected media and events strategists.