PwC Security Leaders Roundtable Luncheon

Cyber Leaders –
The Collaborative Imperative

There has never been as much activity on cybersecurity issues across the entire economy as there is right now. The launch of the Australian Government Cybersecurity Strategy document by Malcolm Turnbull in 2016 put the issue at the centre of the economy.

The document substantially lifted the priority profile of cyber issues within government, putting the public sector's cyber attention on par with that of larger corporates from private sector. Although SME's are still playing catch-up, the landmark document set a fire under first cyber awareness and then cyber activity in Australia. There is quite simply a lot going on.

But two years later, there is still much to be done. The policy imperative is past awareness and education campaigns – although the small business sector still needs attention – and moved to a more mature discussion about collaboration and information sharing.

Cyber professionals understand the value trusted networks of security peers and the role these informal networks play in disseminating threat intelligence across an ecosystem. But when cyber security is an economy-wide issue, more formalised and institutionalised networks for sharing intelligence becomes even more important.

Information sharing is not always a straight forward issue, with the critical need for CEO's and boards to fully understand the mutual benefits. Driving the message to boards and senior non-technical talent has been a key to bolstering faith around the benefits of sharing threat information.

At this Cyber Leaders Roundtable, PwC's Asia Pacific Cyber Lead Steve Ingram leads a discussion on strategies for building trusted networks for sharing threat intelligence and for building stronger cyber relationships across the economy.

James Riley

Editorial Director
InnovationAus.com

pwc

InnovationAus.com
Public Policy and Innovation in Australia

A stronger cybersecurity ecosystem is good for the economy

Steve Ingram, Partner, Asia Pacific Cyber Leader, PwC Australia

Intelligence sharing is critical to cybersecurity. Whether through peers or formal networks, organisations and cyber professionals rely on information from others to learn about the latest threats and security techniques. But experts who participated in the recent Cyber Leaders Roundtable in Sydney called for even broader collaboration and the creation of a strong 'cyber ecosystem'. The consensus from the forum, was that such an ecosystem would better protect our data and people, whilst also strengthening the economy.

Information security executives from NBN Co, Telstra, The Star Entertainment Group, TransGrid, icare NSW, the Australia-Israel Chamber of Commerce NSW, Primary Health Care, Cylance, AustCyber and Ricoh Australia participated in the roundtable, which PwC Australia sponsored and hosted.

They pointed out that cybersecurity is now an issue that affects every sector of the economy. Accordingly, they called for a more diverse range of players – from business and cybersecurity leaders to politicians – to work with each other to protect our data and people. This would also help ensure cybersecurity is treated as the multifaceted issue it has become.

If successful, this stronger ecosystem would contribute to the economy by attracting more investment from firms that see Australia as a secure business destination.

Collaboration is the first step

Better collaboration – and not just among cybersecurity professionals – is the first step in building a robust ecosystem. Michelle Price, Chief Executive Officer of AustCyber, said we would be better off considering a whole range of different perspectives rather than talking about cybersecurity or making decisions in silos. To collaborate, we need to go beyond information sharing and put ourselves in the position of other organisations.

Collaboration means helping industry peers to raise their game and make their organisations more secure, according to Wouter Veugelen, Chief Information Security Officer at Primary Health Care. Indeed, we need to overcome the propensity to keep information to ourselves or within our organisations and play a role in strengthening information sharing. If we want to be a part of the change and build a stronger cybersecurity ecosystem, we need to bring people together and have conversations about cyber issues.

As everyone at the roundtable acknowledged, there is still so much more we can do to create awareness and encourage others to work with us in bolstering our cybersecurity ecosystem.

Richard Burke, Information Security Manager at Ricoh Australia, added that many of today's cybersecurity challenges still have to do with awareness and the need to embed security into organisational governance and culture. As much as we have tried to make progress during the past two years, propelled by the launch of the Australian Government's cybersecurity strategy in 2016, we have not seen systemic improvements in cybersecurity.

The strategy – which sets out the Turnbull Government's philosophy and program for meeting security challenges – has helped raised the profile of cybersecurity, but some areas of our economy still have a lot of catching up to do.

The small business sector, for example, generally lacks maturity in user and data protection. Small businesses may not reach a high level of maturity when it comes cybersecurity, and for this reason, it's important to make it easy for them to improve their security, according to Veugelen.

Robert Martin, Partner, Cyber and Forensic Consulting, at PwC Australia, agreed it was essential to provide small businesses with easy-to-implement solutions, as well as intelligence.

Vendors and larger companies have a role to play in making it easy for small businesses to improve their security. Large businesses, for example, can make cybersecurity a value proposition for small businesses that they work with, suggested Hank Opdam, The Star Entertainment Group's General Manager of IT Governance, Risk and Cyber Resilience. "'If you would work for my organisation, we are going to offer an assessment for free'. This has got to be a conversation for companies now," Opdam said.

Vendors also need to go out of their way to show small businesses how to easily improve their security.

Targeting cybersecurity throughout supply chains can influence processes and even bring about cultural and behavioural changes, according to Brad Watson, Director of Cyber and Forensics at PwC Australia. This, he said, would go a long way in mitigating cybersecurity risks to companies' supply chains.

Engaging government leaders and politicians

Government leaders have a crucial role in building a stronger cyber environment. As cybersecurity moves from being a largely practical and ethical issue into a political one, government leaders and politicians are paying more attention. In fact, AustCyber's Price expected it to start to play out in the next federal election. "We might not directly hear the word 'cyber' in human conversations, but we will hear all the indirect relationships where cyber can come through," she said.

The government has so far taken laudable steps to bolster the discourse on cybersecurity. The launch of the cybersecurity strategy, for example, has put cybersecurity at the centre of the economy. The government has also set a good example by publishing information on data breaches annually. But it needs to go beyond that. There's still room to improve its approach to cybersecurity – such as by providing more resources and taking the lead in building trusted cyber networks and stronger cyber relationships.

People expect the government to be on top of cybersecurity issues – or at the very least, to be thinking about them. More people see cybersecurity as a social contract and expect the government to protect them and their data, according to Anna Aquilina, Director of Cyber and Forensics at PwC Australia. "It's a social contract and you need to negotiate," she said. "If I pay my taxes here and I get a certain amount of healthcare, is there actually something in the cyber world that is being given? And how is government thinking about that?"

Keeping an open debate

Now that the public sector's focus on cybersecurity is nearly on par with that of the private sector, it's important to sustain the interest of government officials and politicians, and keep the conversation with them going. Keeping a healthy and open debate about cybersecurity – as a social contract and an area that helps strengthen our economy and makes Australia a better place to do business – is also crucial to building a more robust ecosystem.

It may also help to educate our government and political leaders about cybersecurity and the risks involved. At the same time, I believe that we in the private sector can do more, including sharing more intelligence, to better protect our data and people.

Contacts

Steve Ingram
Partner
+61 (3) 8603 3676
steve.ingram@pwc.com

Robert Martin
Partner
+61 (2) 8266 5261
robert.w.martin@pwc.com

Brad Watson
Director
+61 (2) 6271 3481
brad.watson@pwc.com

Anna Aquilina
Director
+61 (2) 8266 3699
anna.x.aquilina@pwc.com