How CIOs Can Prevent and Respond to Cyber Threats

Interview with: Rob Wiggan, Former Associate Director Information Security, QUT

"Ransomware and cyber crime are here to stay, but CIOs can mitigate around 90 percent of risks to their IT infrastructure by actively managing the basic controls they should have in place," says Rob Wiggan, Former Associate Director Information Security, QUT.

Rob Wiggan is a speaker at the **marcus evans Australian CIO Summit 2021**.

How is cybersecurity shifting? What does the future look like?

Ransomware attacks are getting more and more sophisticated and targeted, and ultimately more successful. Considering the geopolitical tensions around the world, I believe cyber attacks will keep increasing.

What are the latest innovations in security technology that CIOs can make better use of?

There are enormous opportunities in the security orchestration and automation space. In combination with opportunities in artificial intelligence, data analytics and machine learning efficiency in identifying and reacting to events of interest will support a culture where security teams are better prepared for what is coming in the front door.

What issues might CIOs encounter when upscaling cybersecurity?

The big risk for many organisations is the thinking that they need to spend a lot of money on control uplift initiatives. What CIOs really should do is establish a programme around cyber security resilience, and zero in on the goals of that programme. CIOs must understand that establishing the programme is just the first part; it must be continuously improved. They need a solid incident response process and they must exercise that process, so everyone knows what they need to do when something happens. CIOs need to build the skills within the organisation, so the right people are in the right place and able to resolve and react to incidents as they happen.

It is very difficult to do the whole thing well. Some CIOs think they are, but if they are not testing their incident response, they do not know the process gaps until they have an incident, when it is too late to think about making improvements.

What does it take to future-proof business operations?

It is ambitious to think we can completely future-proof our operations, but if we do the basics well, then we can mitigate 90 percent of the risk that is out there. The ASD Essential 8 controls are a good place to start. We have to make sure to have a strong digital strategy that includes continuous technology upgrades to eliminate long-term technology debt. Finally, it is important not to lose sight of our organisation's value proposition, and make sure all the technology being used feeds into that value proposition.

With the pandemic and many people working from home, what additional risks have come about? How can they be prevented?

We had employees accessing our system from various locations and devices that we did not know if we could trust or not. There are basic things you can do like multi-factor identification, and not exposing the core of your network to external users. Consideration should be given to implementing the key elements of the Zero Trust framework.

What trends and new legislation should CIOs in Australia plan for?

The landscape is always evolving. The lines between cyber crime and nation state are becoming less clear. Cyber crime attribution is difficult as we cannot always definitively verify what is true or not. We also have the Critical Infrastructure Bill coming up, which will broaden the scope of what infrastructure is considered critical, which will introduce additional controls that will need to be implemented. We will probably see another review of privacy frameworks to align with what is happening elsewhere, such as the GDPR. Government agencies in Australia are very close to being mandated to be completely compliant with the Essential 8 controls recommended by the ASD.

A lot of legislation and regulation is coming up, and CIOs have to start preparing for this. They should try to get as close as they can to implementing those eight controls, even if they do not have to comply yet.

> CIOs must understand that establishing the programme is just the first part; it must be continuously improved

The **Information Technology Network - marcus evans Summits** deliver peer-to-peer information on strategic matters, professional trends and breakthrough innovations.

Please note that the Summit is a closed business event and the number of participants strictly limited.

About the Australian CIO Summit 2021

The Australian CIO Summit is the premium forum bringing elite buyers and sellers together. The Summit offers enterprise and government chief information officers and IT solution providers and consultants an intimate environment for a focused discussion of key drivers for IT innovation.

www.australianciosummit.com

Contact

Sarin Kouyoumdjian-Gurunlian, Press Manager, **marcus evans**, Summits Division

Tel: + 357 22 849 313
Email: **press@marcusevanscy.com**

For more information please send an email to **press@marcusevanscy.com**

About **marcus evans** Summits

marcus evans Summits are high level business forums for the world's leading decision-makers to meet, learn and discuss strategies and solutions. Held at exclusive locations around the world, these events provide attendees with a unique opportunity to individually tailor their schedules of keynote presentations, case studies, roundtables and one-to-one business meetings.

For more information, please visit: **www.marcusevans.com**

To view the web version of this interview, please click here:
http://events.marcusevans-events.com/australiancio2021-rob-wiggan