

Brisbane Legal IT Community Roundtable 2018 - blueAPACHE

Canonical: <https://www.blueapache.com/blog/3893-2>

Details:

Last week, We and Palo Alto Networks had the pleasure of hosting an intimate roundtable discussion with senior IT leaders of the Brisbane Law Firm community. Hosted at the Alchemy Restaurant & Bar, the attendees including our team members were joined by very special guest Sean Duca, the Vice President and Regional Chief Security Officer Asia Pacific of Palo Alto Networks. The topic of discussion centred on how legal firms can obtain greater visibility and control across their network and gain a better understanding on the security gaps within their firm. It was widely accepted among attendees that it is not a matter of if they will suffer a data breach, but a matter of when, and therefore the focus should be on lowering the probability of a breach by improving protection, detection and response methods in relation to data protection. However, the IT landscape in today's Law Firms has become more complex; storing data not only in on-premise environments but in Private Cloud, Public Cloud, hosted applications (SaaS) and the devices of their mobile workforce. It was agreed that traditional security measures which only at the perimeter, or other 'point solutions', are not sufficient anymore. Many of today's stealthy, advanced and persistent cyber-attacks avoid traditional security measures throughout the attack life-cycle. It is becoming increasingly difficult to stay ahead of the curve when it comes to coordinating protection and response across multiple attack vectors. There were common challenges being experienced around end user education and staff self-awareness. Some believed that it's everyone's responsibility when it comes to being cyber-secure, whereas the counter viewpoint was it was the IT department's responsibility to implement technologies that will protect users from themselves. It was widely agreed that at the end of the day, there is no one silver bullet, but a combination or 'tapestry' of security layers that are needed to cover all potential security gaps. However, to understand what additional layers you require, first you need to understand the gaps that exist. A big thank you to all who attended, it was a very enjoyable and informative event. For anyone who is interested in how you can assess the security gaps in your organisation, or joining a future roundtable discussion, please reach out to us. Contact us here to speak to our experts on how we can help improve your organisation's risk profile.

What was the Brisbane Legal IT Community Roundtable 2018 about?

It was an intimate roundtable discussion hosted by us and Palo Alto Networks with senior IT leaders of the Brisbane Law Firm community, focused on how legal firms can obtain greater visibility and control across their network and better understand the security gaps within their firm.

Where and when was the Brisbane Legal IT Community Roundtable held?

The roundtable was hosted at the Alchemy Restaurant & Bar, and the blog post about it was published on June 6, 2018 (describing it as having taken place 'last week').

Who were the hosts and special guest at the event?

The event was hosted by us and Palo Alto Networks, with special guest Sean Duca, the Vice President and Regional Chief Security Officer Asia Pacific of Palo Alto Networks.

What key belief did attendees share about data breaches?

Attendees widely accepted that it is not a matter of if a legal firm will suffer a data breach, but a matter of when, so the focus should be on lowering the probability of a breach by improving protection, detection and response methods for data protection.

Why are traditional security measures considered insufficient for today's law firms?

Because the IT landscape has become more complex, with data stored not only on-premise but also in Private Cloud, Public Cloud, hosted applications (SaaS), and on mobile workforce devices, traditional perimeter-only security measures or other 'point solutions' are no longer sufficient.

What differing viewpoints emerged about cyber-security responsibility among attendees?

Some attendees believed cyber-security is everyone's responsibility, while others held the counter viewpoint that it is the IT department's responsibility to implement technologies that protect users from themselves.

What was the overall conclusion about how to address security gaps?

It was widely agreed that there is no single silver bullet, but rather a combination or 'tapestry' of security layers is needed to cover all potential security gaps, and understanding existing gaps is the first step to determining what additional layers are required.

How can someone follow up after reading about the Brisbane Legal IT Community Roundtable 2018?

The article invites readers interested in assessing security gaps in their organisation or joining a future roundtable discussion to reach out to us, with a link to contact our experts about improving an organisation's risk profile.

How long does it take to read the blog post about the Brisbane Legal IT Community Roundtable 2018?

Estimated reading time: about 2 minutes, based on 398 words of article text on this page at 200 words per minute, excluding the Q&A and image list.