ROUNDTABLE WRAP UP:
SECURING THE EDGE WITH SOFTSOURCE VBRIDGE

Well, that's a wrap for our Securing the Edge virtual roundtable event! We'd like to thank everyone who tuned in, our guest speaker Andrew Fox from Aruba, and our very own Barry White for facilitating an insightful event. If you missed it, or just want a refresher, below are the highlights of the hour.

While there's a lot of information on cyber security in other countries, New Zealand businesses often have trouble gaining insights specific to them. That's why we brought in Andrew, Aruba's New Zealand Country Manager, to fill in some of the gaps for you with his cyber security experiences across a range of New Zealand businesses.

What Does Zero Trust Mean and Why is it Important

In our hybrid and remote work era, it's critical to protect your network from within and outside the business. To put it simply, a Zero Trust framework is where no device or user is trusted by default. Instead, they need to be continuously validated to maintain access to the network. So, access to the network is granted only when certain boxes are ticked and then if a device is behaving suspiciously this access is removed.

A Zero Trust framework is a journey, not a quick fix. The first step for New Zealand businesses is gaining visibility over their network because you can't protect it if you can't see it. This step is much easier than you think with technology like Aruba.

Once you know who is on your network, you need to make sure that devices only have the access they require and can't move around the entire network. This helps your monitoring system to automatically pick up if a device is behaving suspiciously—an approach that could have prevented a leading New Zealand home improvement company from being one of the largest-ever cyber breaches. In this case, by the time action was taken against the cyber breach approximately 56 million payment card numbers were exposed.

Another example is where a university student plugged their laptop into the network and left it to run a malicious program through the system. Thankfully in this case, the attack was identified and stopped before large amounts of data were stolen. With intelligent network security, this type of activity can be quickly identified and shut down before damage is done.

Cloud Technologies Require a Different Network Approach

While New Zealand businesses are quick to adopt cloud technologies—an important step that fuels digital transformation—they've been slow to update their network approach to tackle the new vulnerabilities this brings. We heard from event attendees that the proliferation of devices on top of employees using their own devices to connect to the business network has posed a significant challenge in our hybrid workforce era.

The good news is that the Zero Trust framework solves this challenge—particularly with the assistance of AI. For example, Aruba networking technology uses AI to read if a device is behaving in a way it shouldn't be. Is an employee logged on at an irregular time or trying to access part of the network they shouldn't? Even if the device is authenticated, it could be infected and this kind of AI detection is what nips a potential threat in the bud.

If the employee is away from their device, AI can detect suspicious activity and remove the device from the network so that the attack surface is immediately minimised. This could be the difference between losing massive amounts of data and only losing a small portion or none at all. Andrew Fox describes this as containing the blast radius.

What are the Main Causes of Privacy Breaches?

In New Zealand, the most common cause of privacy breaches is human error. This can include anything from email errors to accidental disclosure of sensitive information, data entry errors, or postal and courier errors.

- Human error (61%)
- Malicious attack (25.2%)
- Theft of information (7.5%)
- Other (4.1%)
- System fault (3.3%)
- Privacy Regulations and Playing Your Part

From 1 December 2020 it became mandatory to notify the Office of the Privacy Commissioner within 72 hours if your business experienced privacy breaches that have caused, or have the potential to cause, serious harm to people. Having network visibility and a Zero Trust framework in place are critical to, firstly, minimise the risk of a serious breach and, secondly, identify a breach and reporting it in time to meet your Privacy Act obligations.

Want to learn more about protecting your network from modern IT threats? Get in touch with our cyber security experts today!

Get in touch

Softsource Cloud Services

Softsource Network as a Service (NaaS)

Secure the edge with Zero-Trust Architecture—for the threats of today and tomorrow.Windows 11 and Intel®.

Infrastructure as a Service

Access leading edge computing infrastructure

Disaster Recovery

Recover your services after a disastrous interuption