BRENNAN
People first – secure always

INSIGHTS: ADAPT Security Edge - Sydney

On 27th April, 130+ CISOs, CSOs and IT executives from an array of leading Australian enterprise and government organisations attended ADAPT's annual Security Edge event in Sydney.

Throughout the day there were peer networking sessions, roundtables and keynotes providing fact based and research lead insights around the overarching theme - Crisis Preparation and Resilient Risk Culture.

Whilst we appreciate that it's often hard to escape your desk to attend an all-day event, Brennan was fortunate enough to be a proud sponsor and have therefore put together the key insights and learnings from the day for you. Read on for our top insights from the Security Edge event.

Put Your People First – Cybersecurity is a Collective Effort

During each keynote, roundtable and meeting discussion there tended to be one commonality throughout, that is, the importance of people. Taking a humanised approach to security is absolutely fundamental and crucial – whether it's reviewing your organisation's existing security posture or forward planning your strategic business priorities. Therefore, when the ADAPT research and advisory team revealed their latest insights from their executive surveys, it wasn't surprising that 44% of CISOs intended to prioritise their investment in cybersecurity awareness over the next 12 months. Given that human error is the primary cause for a security incident, this further highlights the importance of investing in cybersecurity awareness training and ensuring that your employees are equipped with the right tools to mitigate and manage any potential incident.

Cyber Transformation is Imperative for Business Resilience

Thanks to COVID, we have seen a rapid shift in cloud adoption, where 10 years' worth of cloud adoption was compressed into 10 months. Now that cloud has become mainstream, so has the number of cloud incidents that occur – with an alarming 188% YOY increase in cloud incidents in 2022.

With attackers now having a wider surface to attack, Cyber Transformation is a top priority for every organisation in the urgent effort to enable new ways of working whilst protecting themselves against ever-increasing threats.

So how do go about driving your own Cyber Transformation and Infrastructure Modernisation?

1. **A Simple Architecture is Best:** the hardest step is often getting started but don't wait for a contract renewal or even worse, a security breach - take a proactive approach to reviewing your existing architecture and security.
2. **Adopt the Zero Trust Principles:** never trust, always verify. Rather than assuming your IT environment is safe it's best to adopt a Zero Trust model and assume breaches and verify each request as though it originates from an open network.
3. **User Centric Experience:** a silo of tools will result in a silo of teams, therefore when creating cyber transformation and infrastructure modernisation keep the end user experience at the forefront of your design.

Embrace the New Expectations of Cyber Resilient Operations

With the hindsight of the past 12 months security professionals have the golden opportunity to rebuild their resiliency and security strategy with renewed vigour and clarity but where do you go from there.

It is suggested that in order to move forward and adopt new normal cyber security resilience in your business the following measures should be taken:

- **Resiliency and Isolation of your Data and Immutable Storage:** with the average cost of a data breach costing $4.25 million[1] and the average number of days to identify and contain a breach being 287 days[2], begin by internally reviewing your existing data and storage. Look at how your organisation is collecting and treating data, question whether you really need the data and take a reconnaissance to clean up your network and give out as little information as possible to help eliminate potential attacks.
- **Shrink your Stack:** with 50% of enterprises agreeing that they need to retain partners to help them with their multicloud resiliency processes, where possible it is important to consolidate your technology stack, keeping your operations automated and streamlined.[3]
- **Cyber Hygiene:** given that 57% of organisations cannot easily identify why they have security issues[4], following precautionary cyber hygiene measures is fundamental. As per the first point, 'Put your people first – it's a collective effort', Cyber hygiene isn't just the responsibility of IT, it is a shared responsibility that all departments and users must prioritise.

1. The Role of Automation in Managing Resilience in Hybrid Multicloud, a Forrester Consulting Study, April 2020
2. Cost of a Data Breach Report 2021
3. ADAPT Security Edge Event Insight, April 2023
4. ADAPT Security Edge Event Insight, April 2023

How to Manage Risk in a Hyperautomated World & Build a Resilient Risk Culture

Given a cyber incident is reported every 7 minutes (and that's just reported incidents), there's no getting around the fact that we are living in a hyperautomated world and that the need for organisations to change, digitise and adapt quickly is crucial. So how can executives manage risks and build a resilient risk culture within their organisation?

- **Ensure Alignment Between your Cyber and Business Strategy**: an effective cyber strategy is one that is accessible, simple and flexible but also aligns with your organisation's strategic priorities.
- **Adopt a People First Mentality:** as per the first point raised, your people are the backbone of your business and therefore your security design and strategy should be human centred. It is said that by 2025, 40% of cybersecurity programs will deploy socio-behavioural principles (such as nudge techniques) to influence security culture across the organisation, up from less than 5% in 2021 – highlighting how important it is to shift your people away from security awareness and to focus on improving behaviour and culture.
- **Governance is Essential:** remember it's not about control, it's about transparency and visibility of your IT environment. A lack of governance will result in no accountability and cost control, it will put your organisation's IP at risk and has the potential to jeopardise any regulatory/compliances that your organisation has in place.