tecala

The top 5 challenges to securing your organisation from cyber attack.

Posted by Murray Mills, Manager of Cyber Security at Tecala

As the cyber security challenge escalates, we explain how our Managed Cyber Security Services deliver expertise on demand to stay ahead of the threat actors.

In its "The State of Data Security – The Human Impact of Cybercrime" report, Tecala's data security partner Rubrik explains that, "IT and Security leaders are in need of essential resources to secure their data."

Exacerbated by the global talent shortage, the cybersecurity industry has faced a well-documented shortage of specialised IT personal for years, and cyber is one of the most impacted.

The Rubrik Zero Labs research respondents unsurprisingly placed talent as their top challenge to protecting their organisations, followed by tools, budget, and C-level and board support.

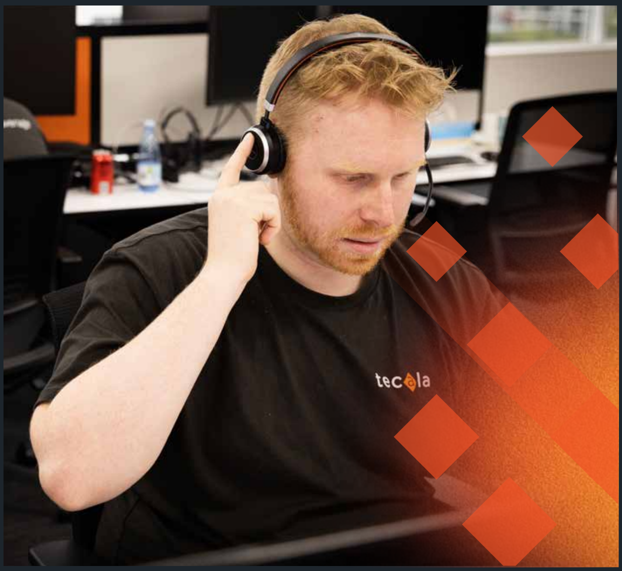
This is having a huge impact on the operations as well the culture and moral of organisations, with human burnout, increasing complexity, and a highly volatile threat landscape placing significant strain on operations and a high-demand, low-density talent pool. As more intrusions go public, the negative impacts from a single breach are felt across the entire organisation.

tecala rubrik

The Top-5 cyber security challenges and how Tecala can help

Tecala's central point when it comes to cyber security is that there's no room for complacency. With so many potential entry points and exploitable vulnerabilities around your organisation, the scope for potential attack is ubiquitous. Amplifying this growing threat are the increasing numbers of threat actors and their ever-more sophisticated techniques.

So, using Rubrik's own research findings as a framework, we've identified the top-five challenges to securing your organisation from cyber-attacks, placing significant strain on operations and a high-demand, low-density talent pool. As more intrusions go public, the negative impacts from a single breach are felt across the entire organisation.



1 Insufficient talent in IT or SecOps teams

With the global cybersecurity workforce gap continuing to increase in 2022 (the ISC 2022 Cybersecurity Workforce Study reporting a stark increase in the shortage of cybersecurity professionals), more mid-sized Australian organisations are turning to managed security experts to deliver round the clock eyes on the glass, as they simply don't have the people in house to ensure effective outcomes.

By delivering expertise and forward-thinking solutions when you need it – often coming in to lead complex or disruptive ICT projects – we'll partner with you to get the outcome you need.

- Get access to highly skilled consultants and engineers
- Easily conduct third-party reviews
- Save time recruiting and speed up value-generation

2 Lack of cybersecurity tools and solutions in place

Tecala's Managed IT Security Services experts will create a secure environment for your organisation, in which you have complete awareness and confidence in the integrity of your data and the efficacy of your security systems, procedures, and protocols.

When you partner with us, you'll gain visibility and advance warning of potential threats, which enables you to take preventative action before there's any impact on your business.

Using our Strategise, Transform, Manage, and Optimise (STMO) methodology, we undertake a cyber security review from which we craft a security strategic roadmap that tailors a security journey to your organisation's needs over the next couple of years. The review is aligned to a threat mitigation framework – either the Essential Eight or the CIS Controls.

3 Insufficient budget for data security

While you can buy and implement a security solution yourself, without the industry understanding and experience of a dedicated team (like Tecala) it's unlikely you'll be able to realise the full potential of that investment.

Ensuring your finite budget is allocated in an optimal way is the essence of what we do. Everything we recommend and implement will have a clear operational objective and predefined value to your organisation.

We then deliver ongoing managed cyber security as a service, so you only allocate budget to the things your organisation needs. No wasted expenditure – that's our promise.

4 A Lack of security prioritisation from C-level/board

Tecala comes from a Consultancy and Advisory heritage. Our approach is very much focused on the formal documentation of analysis pieces. For example, our Audits and Assessments are formally presented to your management team and Board by our Senior Technology Consultants to ensure you fully understand the implications of our findings.

These Audits and Assessments are formulated to enable you to make informed and educated decisions in relation to your ICT elements. This removes any barriers to progress, innovation, and growth.

5 Alignment between different teams and how to protect against cyber-attacks

Based on our findings, we'll then lead you through our expert industry recommendations and, if necessary, integrate these into your Strategic Technology Roadmap.

As we explain on our website, the roadmap gives you certainty and cross-organisational visibility on what the vision for the next three years is going to be. Plus, it gives you clarity on how it will all come together. This technology roadmap ensures you make decisions that are in line with, and in full awareness of, everything else in your organisation that are necessary to achieve your objectives.

This approach ensures everyone in your organisation is on the same page regarding your security policy.

Register for your **Penetration Test.**

And know your threat landscape.

With Tecala's automated Penetration Testing service (internal and external) you get a lot more coverage through our 5-phase, end-to-end penetration testing methodology.

Here are the 5 elements:

1. Phase One: Reconnaissance / Information Gathering
2. Phase Two: Fingerprinting and Scanning (includes Vulnerability Scanning)
3. Phase Three: Attack and Exploitation
4. Phase Four: Privilege Escalation, Post-Exploitation and Lateral Movement
5. Phase Five: Automated Reporting / Dashboard

We are offering to a select few businesses **FREE penetration test**, so you can start identifying your risks and creating cyber security roadmap and journey to reduce, mitigate, and remedy these risks.

Register Here

tecala

Trusted by Australia's most **progressive businesses.**

CatholicCare MY Plan Manager NOBLEOAK StHilliers NSW GOVERNMENT Customer Service CXC