What Can We Learn From The Qantas Data Breach?

That failures of third-party vendors and humans can be your biggest vulnerability.

In today's hyper-connected business environment, organisations rely on an ecosystem of suppliers, vendors, service providers and the humans working there, to operate.

Third-party vendors are fast becoming the most exploited gateway for cybercriminals. In fact, a growing number of high-profile breaches can be traced back to compromised suppliers rather than the targeted company itself. Yet, many businesses still underestimate the extent of the exposure they inherit through their partnerships.

Take the recent Qantas breach for example. It was an attack that compromised 6 million customer profiles. The entry point? An offshore call centre, where an employee was tricked into handing over login details to a third-party platform containing customer information.

Cybercriminals know that people are a predictable vulnerability in most organisations, which is why social engineering remains one of the most common attack methods.

Third-party risks are uniquely challenging because you can’t protect what you don’t control. Vendors often operate outside your direct oversight, yet they may have access to your systems, data, or customers. Security standards vary widely and not all suppliers follow robust cybersecurity practices, including employee awareness training. Cybercriminals take the path of least resistance. If your perimeter is strong, they’ll target your weakest link which is often a third party.

To help protect against these threats:

> Map your vendor ecosystem. Understand who your third-party vendors are, what data they access, and how they connect to your systems.
>
> Assess and tier vendors by risk. Not all vendors pose the same risk. Prioritise those who have access to sensitive data or critical infrastructure.
>
> Have an incident response plan for vendor breaches. Prepare for the scenario where a vendor is compromised. Know how you'll isolate the threat, communicate with stakeholders, and recover quickly.
>
> Train your staff. People are still an important cog in the wheel of defence. Even the most advanced security systems can be undermined by a single click. Regular, practical cybersecurity training is essential.
>
> Encourage a culture of shared responsibility. Cybersecurity is everyone’s problem. Ensure you’re engaging suppliers in conversations about joint resilience and shared risk.

Proactively managing these risks doesn’t just reduce the chance of a cyber incident, it also improves operational resilience and demonstrates that you take security seriously at every level of your business.

Let’s stop thinking of cybersecurity as an IT issue and start treating it as what it truly is, a business imperative.

Issued by ATC Insurance Solutions Pty Ltd ("ATC") (ABN 25 121 360 978, AFS Licence No. 305802), Level 4, 451 Little Bourke Street, Melbourne VIC 3000 acting under a binder as an agent of certain underwriters at Lloyd's.