



# The state of third-party access in cybersecurity



# 01 Introduction

The modern enterprise relies on third parties – including vendors, contractors, suppliers, partners, and broader supply chains – to operate effectively and to be successful. But it can often be those same third parties at the source of cyber incidents. In fact, 42% of organisations in Australia experienced a breach or attack that involved third-party network access in the previous 12 months. That's lower than the global average of 47%, but still troubling.

The Ponemon Institute surveyed 238 IT professionals from Australian organisations from healthcare, the public sector, financial services, manufacturing, and other industries. Here are the key findings based on what they told us:

- The cybersecurity risk posed by third-party access is significant, and it's not going away.
- Organisations are trying, but struggling, to address the threat, with regulatory complexity and the inability to hire for the right expertise as the primary reasons.
- Organisations need to refine and mature their strategies for securing third-party access.

The remainder of this mini report will focus on key takeaways from the Australian environment, presented with supporting data, related to the prevalence of the third-party risk. For full discussion on context about the global figures, and further insights on other takeaways, check out the full [\*\*\*"State of third-party access in cybersecurity"\*\*\*](#) report.

# 02

## Key takeaways: Prevalence of the third-party threat in Australia

The third-party risk is significant, and attacks can have meaningful business, financial, and operational impact. The threat is expected to remain at current high levels – or get worse – and organisations recognise that the third-party access threat is one they must address.

42%

of organisations in Australia have experienced a data breach or cyberattack over the past 12 months involving third-party access

35%

said the attack or breach was the result of the vendor having too much privileged access

29%

where unsure of the cause, likely due to a lack of visibility

### Biggest breach consequences



Loss of sensitive information **(48%)**



Regulatory fines **(45%)**



Loss of revenue **(45%)**

**57%**

of organisations think data breaches caused by third parties will remain the same or increase in the next 12-24 months

**46%**

of organisations say that third-party remote access is becoming their weakest attack surface

**\$116,000 AUD** is the average cost to restore access after a breach in Australia

# 03

## More on the third-party access threat

Organisations in Australia face an uphill battle when it comes to third-party access risk. When nearly half of organisations reported a third-party access-related attack or breach, and when 57% think those types of attacks are likely to stay the same or increase, the need for a better access strategy is clear. With proper prioritisation and funding, organisations can elevate their strategy for protecting against third-party access risk.

Download the global report, *"The state of third-party access in cybersecurity,"* for full insights into the third-party threat, how organisations are trying to combat it, why they're struggling, and what types of strategies are being deployed.

[Download now](#)