Peloton
CYBER SECURITY

10 questions to ask when choosing a cyber security partner

90% of security leaders say their organisation is falling short of addressing cyber risks.

The reason? Too many tactical distractions make it hard to put a robust strategy in place.[1]

A data breach is inevitable

We all see the headlines, bombarding us with fear, uncertainty and doubt. About the cost to the economy and losses as a result of cyber crime. About the next global corporation, government or election facing a cyber attack. About the billions of dollars being spent on cyber security.

The rise of high-profile attacks on Australian corporate giants like Optus and Medibank shows how breaches can happen to any business.

Faced with acute technical skills shortages and rising risks, awareness and scrutiny, it makes sense that leaders are increasingly turning to external cyber security experts to bolster their defences.

However, with a barrage of messages from security vendors claiming to offer the panacea for it all, how do you cut through the noise to make the right investment and partnership choices?

In this guide we arm you with 10 key strategic cyber security insights and questions to ask before you pour money into yet more technology, tools and services.

45

cyber security tools on average are deployed by enterprises.[2]

Yet we know that more tools add complexity and weaken cyber security defences.

QUESTION 1:

Are you a cyber security generalist or specialist?

Not all security providers are the same. It is important to find a partner that can cater to your specific business needs, your in-house expertise and your cyber security maturity level.

Broadly speaking there are two provider categories you may be considering:

Managed Services Partner (MSP)

MSPs typically provide broad enterprise technology offerings from cloud and digital transformation to business platforms and cyber security, with teams that work across multiple IT disciplines.

The breadth and depth of an MSP's security offerings can be highly variable between providers. Therefore, it's important to validate their services against your specific needs. You may like to ask if they have 24/7 cyber security monitoring, if they triage and respond to events and what systems they have in place to effectively manage patches and back-ups.

Managed Security Services Partner (MSSP)

MSSPs are pure play security experts who are 100% focused on cyber security strategy and execution.

This specialist approach means they offer in-depth skills and experience to support you through your end-to-end cyber security journey to complement your in-house skills, technology and maturity levels.

Partnering with you over the long term, an MSSP can help you holistically assess your vulnerabilities, build a strategic plan and continuously optimise risk management.

Takeaway: Put people and intelligence before technology

When choosing a partner, ensure you have access to the strategic expertise you need – whether in house and/or external – to build a sustainable cyber security strategy that can be measured, validated and continuously optimised.

"Huge surges in cybercrime, including ransoming, fraud and data theft, will leave Australia 30,000 cyber professionals short over the next four years."

Max Mason,
Senior Reporter, AFR[3]

QUESTION 2:

What are the fundamental building blocks of a successful partnership?

In a landscape of ever-evolving threats and heightened compliance and reporting requirements, many leaders understandably feel forced into an expensive and risky 'whack-a-mole' approach. Shifting from a reactive to a proactive approach starts with gaining visibility across your unique environment.

To begin, your security partner should take a step back to ensure you have an up-to-date asset inventory – because you can't protect what you can't see – and identify your crown jewels. **This is the intellectual property, asset, supplier, partner, platform or process that if stolen or shut down would disable your business or destroy your competitive advantage.**

Next, they should help you design a multi-layered strategy with everyone pulling together to protect what matters most. Taking a holistic approach can balance immediate vulnerabilities with long-term strategic opportunities to accelerate innovation, transformation and growth.

Takeaway: Start by gaining visibility and identifying your crown jewels

Context is everything. To build cyber resilience, start by protecting your most valuable assets, closely followed by building a sustainable strategic plan to monitor and continuously optimise your defences. From here you can find your ultimate sweet spot between risk and reward.

QUESTION 3:

How will you engage our senior leadership?

Achieving a sustainable level of cyber security is not possible without the support and knowledge of senior executives and the Board. Choose a partner that can work with you and your leadership team to make security part of your strategic growth agenda.

There are several ways the right partner can assist with this:

1. Shared understanding:

Invite your cyber security partner to meet with executives to understand their business strategy, priorities and vulnerabilities, and provide a high-level overview of the latest cyber security threats, solutions and benefits.

2. Build confidence:

Build a strategy that embeds your business strategy, digital platforms and people to protect mission-critical data and give leaders the peace of mind to pursue growth.

3. Demonstrate results:

Deploy analytics that show how the cyber security investment reduces risk and makes the best use of people, technology and capital to maximise ROI.

4. Communication:

Report regularly to the Board so they understand the risks well enough to oversee, challenge and contribute to the process.

Takeaway: Effective cyber security needs C-level backing

Make cyber security part of your strategic growth agenda by ensuring senior executives are educated, engaged, accountable and informed of your initiatives.

QUESTION 4:

How much should we invest and what is the ROI?

*"**It is not possible to reduce cybersecurity risk to zero…** it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls."*

Justice Helen Rofe, judgement on ASIC vs RI Advice Group, 2022[4]

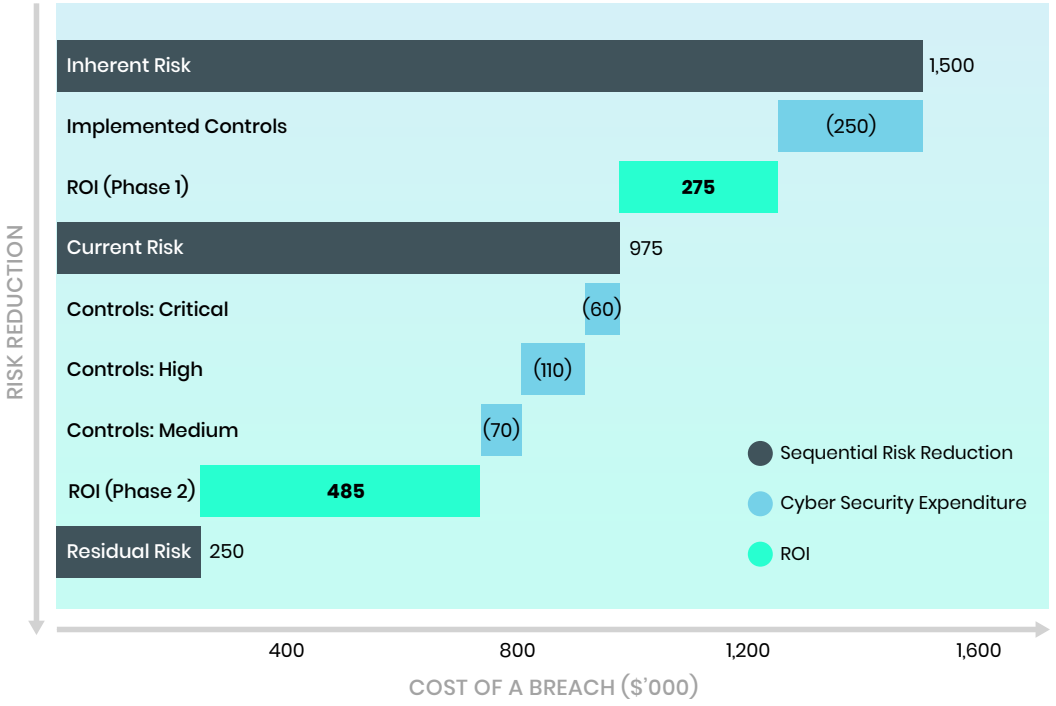
Your security partner's first job is to understand your most valuable assets and how they drive your competitive advantage to accelerate growth. First, work with your partner to quantify expected losses for a breach – based on intelligence and data from cyber insurers and other partners – to justify the spend. For example, there's no point investing $100,000 to protect your key assets if the potential loss is only $70,000.

From here, they can develop a risk-based and threat-focused defence strategy tailored specifically to you. It's important that risk mitigation strategies are validated with a quantitative risk reduction with tangible proof of the return on your investment.

There will consequently be a baseline level of investment required in cyber security to balance acceptable financial loss with mitigation costs. As a leader you can sleep soundly knowing you have appropriate protections in place.

Takeaway: Find your sweet spot between investment and acceptable risk

Done right, cyber investment is a value creator, not a cost centre. Ask your partner how they find the balance between the investment in effective security measures versus potential losses, and what evidence they draw on to measure success.



QUESTION 5:

What should we keep in house vs outsource?

There's no right answer to this question, but one thing is certain – throwing your cyber security responsibilities over the fence to a third party is not the answer. Ultimately, internal governance and controls must become a core internal capability and accountability.

Work with your partner to understand the skills, roles and knowledge that are outside your core competencies. Focus on outsourcing areas that are hard to maintain in house such as 24/7 operations, specialised technical staff, forensics and major incident response. Identify what gaps your partner can help fill as well as where they can educate and upskill your internal team.

Beyond people, review your existing technologies to see what is missing, unnecessary or underutilised. For example, tightening embedded security settings on your existing software and cloud platforms is often more effective than bolting on extras.

Your independent partner can also help validate how your internal controls are governed in line with the three lines of defence model.

Finally, consider what resources you'll need to continually monitor and refine your strategy. The internal/external equation will be a flexible balancing act of budgets, expertise, availability and evolving threat levels.

Takeaway: Cyber resilience is a shared and evolving responsibility

Working with partners who bring specialised skills and experience AND who teach your people to better manage risk internally is likely to create an effective, sustainable long-term partnership.

QUESTION 6:

What is your proven process for deployment?

It's important to confirm your security partner employs proven best-practice frameworks to put adequate protections and protocols in place without slowing or disrupting growth and innovation.

The end-to-end process should cover the full roadmap of cyber security from understanding your risk baseline and developing a threat-focused plan to reducing immediate risk levels and optimising your defences over time. For example, the steps may include:

01

Understand your cyber risk

- Asset discovery
- Vulnerability assessment
- Cyber risk assessment
- Identity assessment
- ASD Essential Eight review

02

Develop a strategic plan

- Business case
- Security program defined
- KPIs and Board reporting
- Metrics and risk appetite

03

Reduce your cyber risk

- Security operations (SIEM)
- Vulnerability and network review
- Incident response plan
- Security training and upskilling

04

Manage your cyber risk

- Virtual CISO / security manager
- Audit, metrics, policies
- Business continuity
- Threat modelling
- Security hardening / certifications

Takeaway: Ask to see the map before starting on the journey

Your partner should have a clear process from the first step in your cyber security journey to how it will look as it evolves over months and years.

QUESTION 7:

What is your track record of results?

Yes, technology is at the core of cyber security; however, it is the quality of the strategy, people and relationships that will deliver the results that set your business apart.

Before you jump into comparing technical skills, look at the depth and breadth of your partner's executive and management team and ask to see evidence of their results.

- How have they educated staff to embed cyber resilience into the core of organisations from senior managers to front line workers?
- Can you assess their track record of change management, taking senior leaders and operational teams along for the journey to implement successful projects?
- Do they offer uniquely deep expertise in your industry and/or technology stack?
- Are they technology agnostic or aligned with specific vendors?
- Which best practice frameworks do they follow such as NIST Cyber Security Framework, ISO27001, ASD Essential 8 and FAIR?
- As threats are present around the clock, do you need a partner that provides a 24/7 Cyber Security Operations Centre (SOC)?

Takeaway: Validate your partner's pitch by talking to their customers

Ask to speak with one or more of your partner's long-term customers to understand their approach, gain insight into quantifiable results and seek a referral.

QUESTION 8:

How will we work together to respond to an incident?

Whether it's simple human error or a malicious attack, a security breach is not a matter of if, but when. That's why it's critical to have a documented cyber incident response plan.

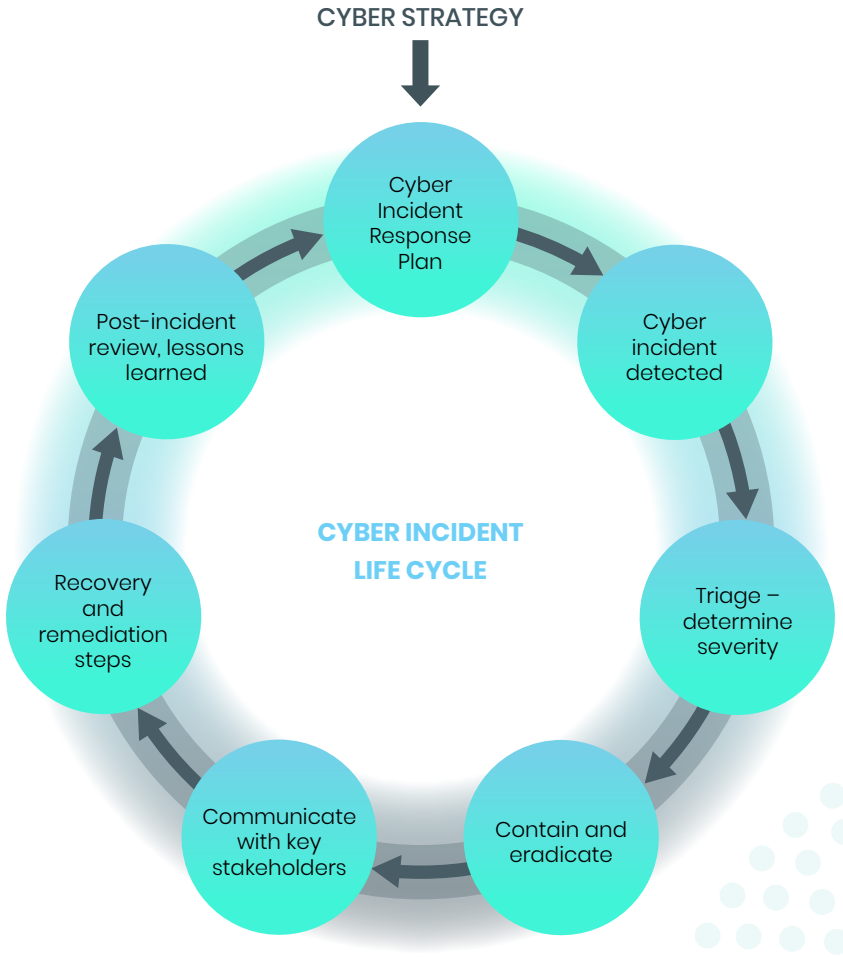
Most security contracts have monthly maintenance including automated monitoring, notifications and technical support, but in the case of an alert or incident it's crucial to define who will triage alerts, assess the threats and take responsibility for remedial action.

Confirm that your partner has a process to differentiate between high- and low-level threats to avoid wasting time and money chasing shadows.

Ask how your partner uses simulation exercises and penetration testing tools to help prepare your executives and staff to respond to and recover from significant incidents.

Takeaway: Insist on a documented cyber incident response plan

As outlined by the Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) in their Cyber Security Governance Principles,[5] a documented cyber incident response plan is a critical tool.



QUESTION 9:

How will you help my organisation move faster?

In recent years, business growth took a back seat to survival. Now, it's back on the agenda, and every leader is striving to accelerate their journey to success. In uncertain times, an effective cyber security strategy is one of the most powerful secret weapons.

By building your organisation's cyber-resilience, you're in a better position to create value, accelerate transformation, grow productivity, and so much more.

Cyber security can drive innovation, transformation and growth through M&A, global expansion and opportunities to tender for significant projects with stringent security and compliance protocols. Having cyber security embedded into your business gives you a competitive advantage by eliminating question marks and fast-tracking deals.

Takeaway: Getting cyber right is both a necessity and an opportunity

While cyber security is rapidly becoming mandatory for compliance and insurance, embedding cyber security into the core of your business gives you peace of mind and confidence to accelerate your strategic goals.

QUESTION 10:

How will you help us reach cyber security maturity?

While cyber security is a continuous process of optimisation, your goal should be to achieve a level of cyber security maturity where your day-to-day business is protected and you are able to detect and respond to any incident.

Achieving this takes time and requires a partner that can show you a roadmap of where you need to be, and who can define the key success metrics as well as guide you through the steps to get there.

Starting out requires a partner to help you gain an understanding of cyber security strategies, set up baseline protections for mission-critical assets and align your Board and risk owners with a shared framework for implementation.

As you consolidate your strategy, you'll build your in-house skills and deploy the combination of people, intelligence and technology you need to continuously shore up your defences.

Takeaway: Choose a partner equipped to go on the cyber journey

We recommend finding a partner whose processes align with Cyber Security Governance Principles[5] laid out by the AICD and the CSCRC:

1. Set clear roles and responsibilities
2. Develop, implement and evolve a comprehensive cyber strategy
3. Embed cyber security in existing risk management practices
4. Promote a culture of cyber resilience
5. Plan for a significant security incident

AT A GLANCE:

10 questions to ask when choosing a cyber security partner

01 **Are you a cyber security generalist or specialist?**

Takeaway: Put people and intelligence before technology

02 **What are the fundamental building blocks of a successful partnership?**

Takeaway: Start by gaining visibility and identifying your crown jewels

03 **How will you engage our senior leadership?**

Takeaway: Effective cyber security needs C-level backing

04 **How much should we invest and what is the ROI?**

Takeaway: Find your sweet spot between investment and acceptable risk

05 **What should we keep in house vs outsource?**

Takeaway: Cyber resilience is a shared and evolving responsibility

06 **What is your process for proven deployment?**

Takeaway: Ask to see the map before starting on the journey

07 **What is your track record of results?**

Takeaway: Validate your partner's pitch by talking to their customers

08 **How will we work together to respond to an incident?**

Takeaway: Insist on a documented cyber incident response plan

09 **How will you help my organisation move faster?**

Takeaway: Getting cyber right is both a necessity and an opportunity

10 **How will you help us reach cyber security maturity?**

Takeaway: Choose a partner equipped to go on the cyber journey

OUR VISION:

To reduce $10 billion of cyber risk for businesses globally.

The Peloton Difference

At Peloton Cyber, our proven process starts with people – not tools and technology.

We know it's not possible to reduce your cyber security risk to zero. But we know it is possible to regain control and visibility over your threat landscape – and even turn cyber security into a competitive advantage.

When senior executives and Boards clearly understand the risks, they can focus their resources and investments on protecting what matters most.

A robust cyber security strategy finds that all-important sweet spot between risk and investment. It bridges the gap between strategic imperatives and operational teams. And it creates a shared language that increases knowledge, creates transparency and enables your entire organisation to pull in the same direction.

To secure your business and its most critical assets, we help you build a sustainable and resilient cyber security strategy that can be measured, validated and continuously improved over time – with predictable costs.

As a Managed Security Services Provider (MSSP), Peloton focuses 100% on cyber security strategy, managed services and optimisation. Our experienced team has helped organisations through countless cyber breaches. We use these real-world experiences and learnings to deliver security outcomes tailored to your needs.

Learn how to make cyber security your strategic advantage at
pelotoncyber.com.au

GET IN TOUCH

Speak to us about making cyber security your strategic advantage.

1300 735 686
info@pelotoncyber.com.au

Head office:
Level 11, 45 William Street,
Melbourne, VIC 3000

References:
1. Foundry (an IDG, Inc. company), Sept 2022, Security Priorities Study
2. ZDNet, June 2020, The more cybersecurity tools an enterprise deploys, the less effective their defence is
3. AFR, Sept 2022, Cyber skills shortage 'to hit 30,000 in four years'
4. Australian Institute of Company Directors (AICD), July 2022, Cyber security: Be prepared
5. AICD / CSCRC, Oct 2022, Cyber Security Governance Principles