Guide to Outsourcing Cyber Risk in 2025

CyberCaddy®

In 2025, internalising cyber risk (e.g. self-insuring or building 24/7 cyber security team) is not practical unless your business has $1bil+ turnover or likes to burn cash. Throughout this article we cover how you can outsource cyber risk from your business. Here's the areas we will cover in detail:

1. Visibility & Evidence
2. Improve Data Recovery to Reduce Impact
3. Threat Detection & Response
4. Insure Against Cyber Risk
5. Annual Third-party Cyber Review

But first, let's cover what Cyber risk is and why you can't take a "head in the sand" approach anymore....

Cyber Risk is Business Risk

Cyber risk to a business refers to the potential for financial loss, operational disruption, reputational damage, or legal consequences resulting from failures or attacks on digital systems and data. Cyber attacks can come in the forms such as data breaches, ransomware, phishing, business email compromise and system outages, which can compromise sensitive information, interrupt services, and as a result, erode customer trust. Managing cyber risk is essential for protecting a business' assets, operations, and long-term viability in an increasingly digital world.

To put that in meaningful numbers....

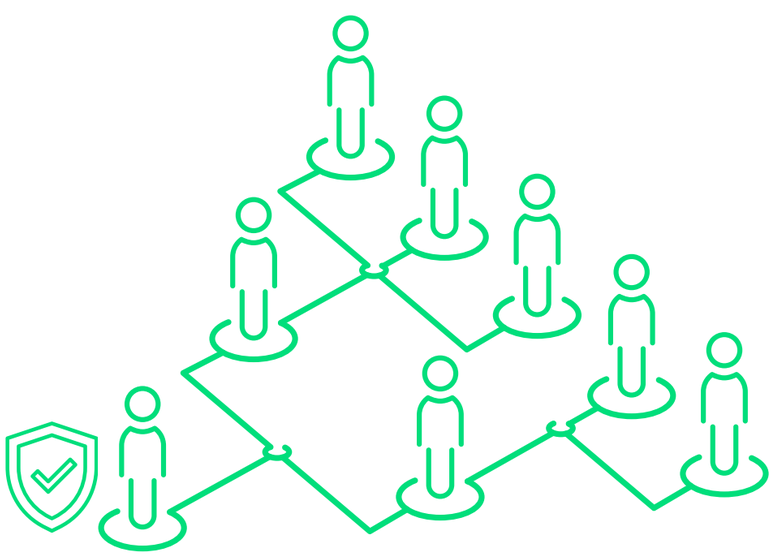
In 2024, Australian Businesses lost **$33 Billion** to Cybercrime according to the Australian Cyber Security Centre (ACSC).

- Australia is now the 4th most targeted country by cyber criminals
- In the last 5 years, 69% of Australian businesses experienced a ransomware attack and...
- 84% of those businesses opted to pay the ransom with the average ransom payment of $1.35M

(According to the Australian Cyber Network Ltd – State of the Industry 2024 Report)

While it's best practice to have an internal or outsourced IT provider to set up, patch and manage your technology, you cannot outsource cyber risk to your IT provider. An IT provider is not liable for your breaches, you are. If you are a company Director, you don't need to implement every recommendation in this guide, but you must have a clear understanding of them.

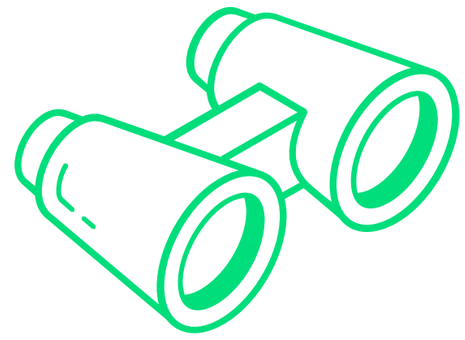
Accountability for cyber risk starts at the top.



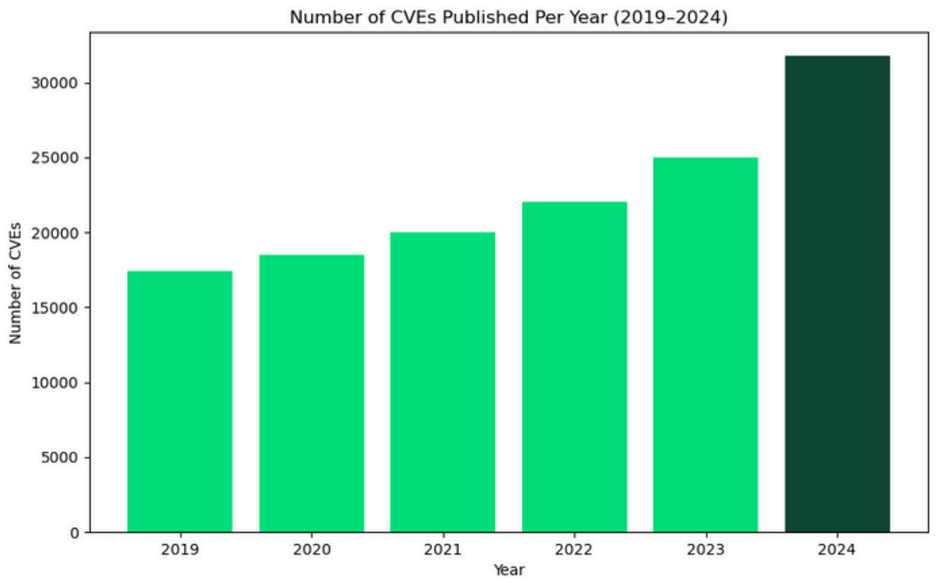
CyberCaddy®

1. Visibility and Evidence

The first step in understanding your current cyber risk profile needs to be visibility. This can be achieved through a one-time, independent assessment – conducted by a third-party, not your internal team or IT provider – or through ongoing monitoring using a SIEM (Security Incident Event Management) tool, ideally managed by external experts. Alarmingly, most Australian businesses currently lack any meaningful visibility into their cyber risk exposure.



Visibility: Visibility in cyber security refers to the ability to see and understand all activities within your IT environment. This includes network traffic, user behaviours, system configurations, and application activities. A properly configured SIEM solution provides comprehensive visibility across the entire business environment, forming a strong foundation for effective security monitoring.



According to the CVE Program Report for Q4 2024, In 2024, there were 31,770 new Common Vulnerabilities and Exposure's (CVE's) created. This number reflects the growing volume of publicly disclosed cyber security vulnerabilities.

Every business has hundreds if not thousands of risks in their environment. You need visibility to know where your threats are coming from.

Industry estimates suggest that only 30–40% of Australian businesses have implemented centralised logging platforms (SIEM). This lack of visibility means that when a data breach or business email compromise occurs, most organisations are unable to trace the attacker's movements. Without reliable forensic insight, it's often impossible to determine what data was accessed — forcing businesses to assume the worst. This typically results in disclosing the breach to clients, staff, and vendors, leading to significant reputational damage. Even among businesses that do have logging in place, many fall short on log retention — limiting their ability to investigate incidents that unfold over weeks or months. This highlights the critical need for both strong forensic capabilities and long-term, secure log retention.

Forensics: Forensic details involve the collection, analysis, and interpretation of electronic evidence to investigate cyber crimes and security incidents. This is critical for incident investigation, legal compliance and digital forensics when working through remediation and impact analysis.

Log Retention: Logging involves recording events that occur within your IT network. These logs provide a detailed account of all system activities, which are crucial for retrospective incident response and remediation work. This is also incredibly valuable when understanding the impact of cyber events such as a Data Breach, Ransomware and a Business Email Compromise.

Cyber Caddy's Read –

To effectively reduce the impact of a cyber breach, you must understand the risks within your environment and ensure comprehensive logging across all platforms. Unlike a decade ago, implementing this level of visibility is no longer cost-prohibitive. However, don't assume your outsourced IT provider has this covered — most are contracted for basic support and maintenance, not advanced security operations. If not using Cyber Caddy, your logging and monitoring platform should still be managed by an independent third party — not your internal IT team or provider — to avoid conflicts of interest and ensure objective, expert oversight.

CyberCaddy®

2. Improve Data Recovery to Reduce Impact

In 2024, 84% of Australian businesses that suffered a ransomware attack paid the ransom. This stark figure highlights a critical misconception: simply having backups does not eliminate the need to pay. While backups are essential for recovery, they don't prevent breaches — and they don't always negate the leverage attackers have, especially when sensitive data is exfiltrated. This reinforces the need for a more comprehensive cyber resilience strategy beyond just data recovery.

> "The Australian Cyber Security Centre (ACSC) reports that ransomware continues to cause significant downtime and data loss for Australian businesses. Without reliable backups, recovery may be impossible — and even paying the ransom offers no guarantee of data restoration or protection from data leaks."

Now that's out of the way...

One of the easiest ways to reduce the impact of a breach and general IT downtime, is to implement secure backups of all your core systems. Including cloud applications (M365/GCP), network configurations and infrastructure.

When reviewing backups, it's important to ensure the backup strategy is comprehensive, and follows the below points;

- **Regular Backups:** Ensure that backups are performed regularly and automatically. This includes daily backups for critical data and weekly or monthly backups for less critical information.
- **Diverse Backup Methods:** Use a combination of full, incremental, and differential backups to optimise storage and recovery times.
- **Offsite and Cloud Backups:** Store backups in multiple locations, including offsite and cloud storage, to protect against physical disasters and cyber-attacks, ensuring data sovereignty is considered.
- **Immutable Backups:** Ensuring immutable storage solutions are utilised so that backups cannot be altered or deleted, protecting against ransomware.
- **Alignment to RPO/RTO:** Understanding and reviewing current RTO/RPO's in place to ensure the backup frequency, retention and technology is capable to restore in a timely manner.
- **Backup Testing:** If we had a penny for every time a client went to restore from backups in a pinch, and the backups are either corrupt or unusable. This is why testing your backups and disaster recovery plans are so important.

Cyber Incident Response Plan & Business continuity:

- Incident Response Plan: Develop and maintain a Cyber Incident Response plan that outlines the steps to take in the event of a cyber incident.
- Business Continuity Planning: Integrate your backup and recovery strategy into your overall business continuity plan to ensure that critical business functions can continue during and after an incident.

If you're unsure about any recommendations, contact Cyber Caddy today. We can conduct a third-party cyber review to give your business a clear picture of your current backup strategy and identify any gaps.

CyberCaddy®

3. Threat Detection & Response

One of the best ways to reduce cyber risk is to stop being breached. Sounds obvious we know....but in 2024, the Australian Cyber Security hotline was called every 6 minutes reporting a breach.

What is Threat Detection & Response?

Threat Detection and Response is about stopping breaches before they cause damage — simple as that.

It’s the process of continuously monitoring your environment for suspicious activity and responding quickly to contain threats before they escalate. Whether it’s a compromised account, malware, or a rogue insider, the goal is to catch it early and act fast. Modern detection and response platforms are far more accessible than they used to be — no longer reserved for big enterprises with deep pockets. If you’re serious about reducing cyber risk, this is one of the smartest investments you can make.

Implementing threat detection & Response services can identify suspicious behaviour in your environment and contain breaches before they access sensitive information or worse. Enterprise grade detection & response services are nowhere near as expensive or time consuming as they used to be and in our opinion, the most effective method to bringing down the colossal $33Billion dollars per year that Australian businesses are losing to cyber criminals.

When you are evaluating Sec Ops / Threat detection & Response services, here's what you need to consider:

- **COVERAGE:** Is this service ingesting logs from all of my attack services? Ideally you want a SIEM platform that takes data from endpoint, cloud, identity, network and SaaS platforms.
- **RESPONSE TIME:** When a threat actor enters your environment the impact catching this in 30 minutes vs 3 hours could be thousands of client records or TB's of data
- **COSTS:** Legacy solutions can have hidden costs around data storage, software licensing and some are just expensive for no reason in our experience.
- **TIME TO DEPLOY:** Legacy SIEM platforms can take significant effort to deploy, sometimes requiring servers to be run up and slow at integrating to current technology stack. We have seen some providers take 3–4 months, which can leave your business exposed

Of course, if you want advice or further conversation in this area, feel free to email enquiries@cybercaddy.com.au or 1300 511 863.

Cyber Caddy’s Read –

When choosing a SIEM/SOC partner, Cyber Caddy recommends thorough due diligence by reviewing multiple providers. Prioritise a partner that offers ongoing consultancy from a named security consultant.

It's one thing to have Threat Detection & Response services, but it's another entirely to have an engaged consultant who can leverage those insights to continually improve your business's cyber security posture. The fight against cyber threats isn't a one-time fix; winning requires planned and strategic improvements to your overall risk state well into the future.

CyberCaddy®

4. Insure Against Cyber Risk

Given the widespread integration of technology into modern business operations, Cyber Caddy recommends that all businesses utilising technology invest in comprehensive cyber insurance. The landscape of cyber insurance premiums has shifted over the past 24 months, with costs generally trending downwards, particularly for organisations demonstrating robust cyber hygiene and effective security controls. Investing in cyber insurance is therefore a prudent and increasingly accessible measure for virtually all businesses.

Consider the following scenarios where a comprehensive cyber insurance policy can provide critical financial and operational support:

1. BEC (Business Email Compromise) – The compromise of an email account can serve as a gateway for malicious actors to infiltrate other systems, potentially causing extensive damage. Even in isolated BEC incidents, fraudulent invoices can be generated or approved, leading to significant financial losses. Many cyber insurance policies offer coverage for these lost funds and associated business downtime.

2. Ransomware incident – With a reported 69% of Australian businesses experiencing a ransomware attack in the last five years, the substantial financial repercussions are evident. The average cost of a ransomware breach in Australia in 2024 reached $4.2 million AUD. This figure encompasses several key expenses:

- **Ransom Payments:** The average ransom demand in 2024 was $1.35 million AUD. While coverage varies, some policies may include reimbursement for such payments.
- **Business Interruption:** Recovery from a ransomware attack can extend from days to weeks, resulting in significant revenue loss for affected businesses. Cyber insurance can help mitigate these financial impacts.
- **Digital Forensic Incident Response (DFIR):** Engaging specialised DFIR teams is crucial for assessing the scope of a breach, minimising its impact, and conducting thorough analysis. These services represent a significant cost.
- **IT Restoration Costs:** The process of restoring systems to operational status post-breach can demand substantial IT resources, often exceeding 100 hours of work. Associated costs can range from $5,000 to $300,000.
- **Legal Costs:** Mandatory data breach notification requirements and other regulatory compliance obligations (e.g., PCI DSS, CPS 234) necessitate legal counsel to ensure timely and accurate communication to clients, staff, and suppliers. These legal expenses are typically borne by the affected organisation without cyber insurance.

Beyond covering direct financial losses, many cyber insurance policies provide access to established networks of professionals in incident response, forensics, legal counsel, and IT recovery. The recent decrease in cyber insurance premiums, especially for organisations with strong cyber security postures, makes this risk mitigation strategy increasingly accessible.

It is crucial to recognise that cyber insurance is not a standalone solution for managing cyber risk. While it offers financial protection, it does not address the reputational damage and emotional toll experienced by directors, management, and IT teams following a cyber incident.

Disclaimer: CyberCaddy is not a licensed insurance broker and cannot provide specific advice around insurance, information in this section is for general advice only. Consult your current insurance broker for information about your specific requirements.

CyberCaddy®

Third Party Cyber Review

The Power of a Third-Party Cyber Review

It's understandable to feel overwhelmed navigating the complexities of today's cyber security world. Businesses often grapple with both significant cyber risks and a knowledge gap, leading to potential overspending or, more critically, a misunderstanding of their true security posture. This is where a third-party cyber review becomes invaluable. It provides an objective assessment of your current security state, illuminating your key risks and offering clarity on where to focus your future cyber security efforts.

Cyber Review vs. Penetration Testing: Knowing the Difference

Interestingly, penetration testing often takes centre stage in general awareness, while the strategic benefits of a third-party cyber review remain less known outside the IT realm. While penetration testing – a deep dive into specific systems to uncover vulnerabilities – is crucial for organisations with internally developed applications, complex infrastructure handling sensitive data, or public-facing client systems (requiring annual testing), it might not be the most effective starting point for everyone.

For many organisations that don't meet these specific criteria, a comprehensive cyber review offers a more holistic understanding of their overall security posture. This review typically delivers a clear and actionable roadmap for improving your security defences. Investing in a third-party cyber review, embarking on your security compliance journey, and establishing a robust cyber security roadmap can not only provide peace of mind but may also lead to lower cyber insurance premiums.

A Word of Caution: Choose Your Review Partner Wisely

It's crucial to understand that not all cyber reviews are created equal. We strongly advise against obtaining a cyber review or an Essential 8 assessment from your existing IT provider. Unfortunately, these are often low-value exercises designed primarily as sales tools for Managed Service Providers (MSPs). These biased reviews frequently result in a generic list of IT tasks without providing a genuine understanding of your actual cyber risk landscape. We've recently assisted numerous clients in redoing such reviews, highlighting the limitations of these internally-biased assessments. Engaging an independent, third-party provider ensures an unbiased and insightful evaluation of your security posture.

Contact our team today to schedule a Cyber Review for your business

www.cybercaddy.com.au/contact-form

CyberCaddy®

Summary

In summary, cyber risk is becoming one of the top risks to great Australian businesses. Hopefully this article has shed some light on what you as a director, or internal delegate, needs to understand about outsourcing cyber risk. Just remember that getting the right advice in this area can save you millions of dollars and a lot of heartache, you don't need to buy every cyber security tool out there but also, don't stick your head in the sand and say "we're too small, won't happen to us".

About Cyber Caddy

Frustrated by the escalating number of cyber security breaches affecting Australian businesses year after year, we founded Cyber Caddy to create a better solution. Recognising the confusion, high costs, and overwhelming noise in the industry, we are dedicated to offering businesses a clearer path forward.

At Cyber Caddy, we provide transparent, evidence-based, and practical cyber security advisory and protection services. Our commitment to independence ensures that our clients receive unbiased guidance tailored to their unique needs. We empower organisations to understand their current cyber security risk profile and effectively reduce the likelihood and impact of breaches.

Our mission is to simplify cyber security, enabling businesses to navigate this complex landscape with confidence and peace of mind.

Sincerely, your dedicated cyber partner,
Cyber Caddy
enquiries@cybercaddy.com.au
1300 511 863

References:

1. **Australian Cyber Security Centre (ACSC).** (2024). Annual Cyber Threat Report 2023–2024. Australian Signals Directorate. Retrieved from https://www.cyber.gov.au
   - Cited for: $33 billion in cybercrime losses, ransomware trends, and breach reporting frequency.
2. **Australian Cyber Network Ltd.** (2024). State of the Industry Report 2024.
   - Cited for: 69% of businesses experiencing ransomware, 84% paying ransom, and average ransom payment of $1.35M AUD.
3. **CVE Program.** (2024). CVE List – Q4 2024 Summary. MITRE Corporation.
   - Cited for: 31,770 new Common Vulnerabilities and Exposures (CVEs) disclosed in 2024.
4. **CyberCaddy.** (2025). Guide to Outsourcing Cyber Risk in 2025.
   - Internal publication providing strategic guidance on cyber risk outsourcing, including visibility, data recovery, threat detection, insurance, and third-party reviews.

Glossary of terms:

Ransomware: A type of malicious software designed to block access to a computer system until a sum of money is paid.

Business Email Compromise (BEC): A cybercrime where attackers impersonate a trusted contact via email to trick individuals or organisations into transferring money or sensitive information.

Essential 8: A set of baseline mitigation strategies recommended by the Australian Cyber Security Centre to help organizations protect their systems against cyber threats.

Penetration Testing (Pen Test): A simulated cyber-attack against your computer system to check for exploitable vulnerabilities.

CVE (Common Vulnerabilities and Exposures): A list of publicly disclosed information security vulnerabilities and exposures.

SIEM (Security Information and Event Management): A system that collects and analyses security data from various sources to provide real-time analysis of security alerts.

Incident Response Plan: A documented strategy outlining how an organisation will detect, respond to, and recover from cybersecurity incidents.

Cyber Review: A high-level assessment of an organisation's cyber security posture, identifying risks, evaluating controls, and recommending improvements.

Breach: An incident where sensitive, protected, or confidential data is accessed, disclosed, or stolen by an unauthorised party.

Business Continuity Plan (BCP): A documented strategy outlining how an organisation will continue operating during and after a disruption, including procedures for recovery and maintaining critical functions.

Backups: Copies of data stored separately to enable recovery in case of data loss, corruption, or a cyber incident.

RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time, indicating how far back in time data can be recovered after an incident.

RTO (Recovery Time Objective): The maximum acceptable amount of time it should take to restore systems and resume operations after a disruption.