

TOP TRENDS IN CYBERSECURITY





CONTENTS

03	Introduction	
04	Comprehensive Cybersecurity Protection	
	What you can do	[07]
	Pro tip	[08]
09	Emphasis on Cybersecurity Risk Management	
	What you can do	[11]
	Pro tip	[12]
13	Increase Use of Artificial Intelligence (AI)	
	Notable case	[15]
	Challenges & Tips	[16]
18	Greater Demand for Cybersecurity Professionals	
	Why the demand?	[19]
	What you can do	[20]
22	Regulatory Changes	
	Privacy Act Reform	[24]
	What you can do	[25]
27	Super Trends (That are here to stay)	
	Remote working, Mobile & IoT	[28]
	Resource constraints in IT Teams	[29]
30	To Sum Up	
	Top Trends	[31]
	Top Tips	[31]

TOP TRENDS IN CYBERSECURITY

2024 FORECAST FOR AUSTRALIA

How many are you aware of? Stay vigilant to stay ahead.

In today's world, every organisation is prone to cyber threats and attacks.

While there has been an increase in cybersecurity solutions in the recent years, there has also been a spike in scams, business risks and data breaches.

As we dive deeper into the digital age, cybersecurity is emerging as a paramount concern. It's an ever-evolving phenomena like technology itself, with new threats and challenges surfacing constantly.



In 2024, Australia is expected to witness several key trends in cybersecurity that organisations must prepare for.

It's time to say enough is enough.

Let's jump in and take a look at the top trends in cybersecurity and how you can keep your organisation safe from attacks and **protect your data and reputation for good.**

TREND 1

COMPREHENSIVE
CYBERSECURITY
PROTECTION

COMPREHENSIVE CYBERSECURITY

In 2024, basic anti-virus, firewall and malware protection just aren't going to cut it.

With the rise of technologies such as cloud, mobile and IoT, the traditional security architecture is no longer sufficient to provide complete protection.

Comprehensive cybersecurity solutions will be the new norm, providing a **multi-layered defence** to protect against a wide range of cyber threats.

WHY THE NEED FOR A COMPREHENSIVE PROTECTION?

In today's digital age, organisations of all sizes are vulnerable to cyber attacks. Here's a quick look at the evidence:

- According to a study, **46% of all cyber breaches impact businesses with fewer than 1,000 employees**. If you think small and medium-sized enterprises (SMEs) aren't prone to cyber threats, think again!
- In recent years, **there has been a significant rise in cyberattacks targeting supply chains**. These attacks can impact critical operations in the organisation that rely on an efficient supply chain network.
- **Data breaches continue to be a major concern**, with hackers targeting sensitive information such as customer data, intellectual property, and financial records.

NOTABLE CASES

We've all woken up to some alarming news about major data breaches in recent years.

Let's examine a few cases and the detrimental impact they faced:

Major Retail Data Breach

In 2022, a prominent Australian retail chain suffered a significant data breach. Hackers gained unauthorised access to the company's database, compromising sensitive customer information.

The result: severe financial losses and reputational damage.



Ransomware Attack on Healthcare Provider

In 2021, attackers encrypted critical patient data of a large healthcare provider, demanding a hefty ransom for its release.

The incident disrupted medical services and compromised patient care financial losses and reputational damage.



Phishing Incident at a Financial Institution

In 2023, cybercriminals sent deceptive emails to employees of a leading financial institution, tricking them into revealing their login credentials.

This breach exposed sensitive customer data and led to substantial financial fraud.



WHAT YOU CAN DO

To ensure comprehensive cybersecurity protection, consider these simple measures that will not only save time and cost but also provide a greater level of protection, ensuring safety from increasingly sophisticated cyber-attacks.



Robust Security Infrastructure

Implement industry-standard security tools, firewalls, intrusion detection systems, and antivirus software to protect against known threats.



Regular Risk Assessments

Conduct regular risk assessments to identify vulnerabilities and address them promptly. E.g. vulnerability scanning, penetration testing, and security audits.



Employee Training

Educate employees about cybersecurity best practices, including password management, recognizing phishing attempts, and safe browsing habits.



Secure Network Architecture

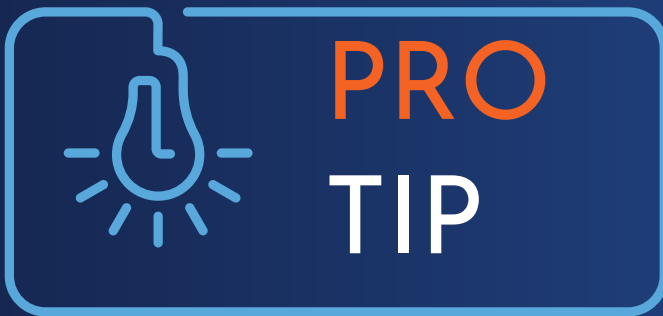
Design a secure network architecture that includes strong access controls, network segmentation, and encryption protocols.



Data Backup and Recovery

Regularly back up critical data and develop a robust disaster recovery plan to minimise downtime and data loss in the event of an attack.

TREND 1



Securing your digital realm is not just an option; it's a necessity.

In today's interconnected world, comprehensive cybersecurity protection is paramount for any organisation in Australia. The ever-evolving threat landscape and the potential consequences of cyber attacks underscore the need for robust security measures.

Act today for a robust tomorrow.

Consider a comprehensive cybersecurity to:

- Effectively fortify your organisation's defences without burdening limited resources.
 - Mitigate risks and safeguard sensitive information.
 - Bolster your resilience against cyber threats.
-

TREND 2

EMPHASIS ON
CYBERSECURITY
RISK MANAGEMENT

EMPHASIS ON CYBERSECURITY RISK MANAGEMENT

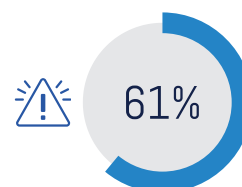
In an era where the digital landscape is constantly shifting, the emphasis on cybersecurity risk management in Australia is more pronounced than ever.

As a result, effective risk management will become a core component of every organisation's cybersecurity strategy.

WHY THE NEED FOR CYBERSECURITY RISK MANAGEMENT?

According to a recent survey by the Australian Cybersecurity Centre:

61% of Australian organisations identified cybersecurity as a high-risk area in 2021 with potential security breaches posing significant threats to their operational continuity.



In addition, the Australian Government's 2020 Cybersecurity Strategy highlighted an annual loss of over \$29 billion due to cybercrime.



These alarming figures are the reason why organisations are no longer taking cybersecurity lightly. Instead, they are now allocating more resources to their overall IT infrastructure.

WHAT YOU CAN DO

Simply put, it's time to be proactive, not reactive.

Shift your focus from a purely defensive approach to a more proactive risk management.



Identify vulnerabilities and assess potential impacts.



Implement effective protection measures ahead of time.



Actively identify and evaluate your cybersecurity risks.



Put preventative measures in place.

This shift towards proactive risk management will significantly:

- Enhance the overall safety of your digital assets
- Reduce the effect of security risks on your daily operations.

TREND 2



Combine advanced security measures with built-in risk management, intelligent policy control, and real-time visibility.

Key benefits:

- Streamline your cybersecurity efforts and reduce resource burdens, so that you can focus on your core business objectives and be there for your clients, always.
- Confidently adapt to changing business needs confidently while ensuring compliance with industry regulations.
- Proactively identify and mitigate potential threats before they cause significant harm.
- Empowered SMBs and enterprises can safeguard critical assets, maintain operational continuity, and protect the privacy of sensitive information.
- Experience unmatched flexibility and scalability.
- Monitor and optimise performance, secure access to corporate applications and SaaS applications from anywhere.
- Enforce corporate internet and access control policies.

In summary, effective cybersecurity risk management is not just about reactive measures; it's about proactive strategies that protect your organisation from emerging threats whilst ensuring the integrity of your digital assets.

TREND 3

INCREASED
USE OF
ARTIFICIAL
INTELLIGENCE

INCREASED USE OF ARTIFICIAL INTELLIGENCE (AI)

In the face of complex and adaptive threats, AI will play a crucial role in IT security.

AI can help detect patterns and anomalies that might otherwise go unnoticed, enabling you to respond to threats more rapidly and effectively.

Artificial Intelligence (AI) has emerged as a pivotal tool in enhancing cybersecurity in Australia, where organisations are leveraging its potential to mitigate cyber threats more efficiently.


WHY THE NEED FOR AI IN CYBERSECURITY?

According to Gartner, AI will be involved in 75% of cybersecurity incident responses by 2025.

As AI technologies advance, there is an increasing need to analyse large data volumes, identify patterns, and detect anomalies, which helps in anticipating potential cyber threats.

The rise of AI in cybersecurity is more than a trend.

It is a necessity given the increasing sophistication of cybercriminals. Australian organisations today are rapidly harnessing the power of AI to safeguard their digital assets and ensure a safer online environment.



In an environment where cyber protection is paramount, AI stands as a vigilante that can:



Analyse vast amounts of data
and identify patterns of malicious activities.



Enhance your ability to detect
and respond to cyber threats effectively.



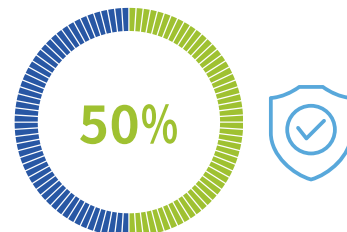
Significantly improve threat detection and response capabilities,
empowering organisations to stay one step ahead of cybercriminals.



Allow organisations to focus more on their core competencies
instead of constantly fighting off cyber threats.

NOTABLE CASE

Major Australian banks have integrated AI into its cybersecurity strategy, resulting in a significant decrease in fraud-related incidents. In a recent press release, they noted a **50% reduction in digital fraud cases within 12 months of implementing AI-based cybersecurity solutions.**



CHALLENGES OF AI AND WHAT YOU CAN DO

It's all good to harness the power of AI for cybersecurity, but beware of potential challenges.

Challenge: Data quality and bias

Ensure that the data used to train AI models is accurate, representative, and free from bias. This can avoid skewed results and potentially overlook certain threats.

Challenge: Adversarial attacks / sophisticated phishing


Cybercriminals may attempt to exploit vulnerabilities in AI algorithms, tricking them into misclassifying or misinterpreting data. Regularly update and test AI models to mitigate this risk.

Challenge: Lack of human oversight

While AI can automate many cybersecurity tasks, human experts are needed to interpret AI-generated insights, make critical decisions, and provide context to ensure a comprehensive defence strategy.

Challenge: Constant learning and adaptation

Cyber threats evolve rapidly, making it crucial for AI systems to continuously learn and adapt. Get regular updates and have close collaboration with your tech provider to ensure that your AI defences stay up to date.



TREND 3



Don't just go for AI because it's the trend.

Go for AI after undertaking a sound assessment of your organisation's specific needs and scope.

Don't know where to get started?

We've got you.

Visit www.north-bridge.com.au

Our team at Northbridge Systems can evaluate your current IT ecosystem to equip the people in your organisation with the best practice and insights about potential risks that follow after sharing or uploading business data onto unauthorised AI platforms that you may be using currently.

You deserve to always know exactly where your data is, where it's going and where it's stored.

TREND 4

GREATER
DEMAND FOR
CYBERSECURITY
PROFESSIONALS

GREATER DEMAND FOR CYBERSECURITY PROFESSIONALS

As organisations invest more in their IT security infrastructure, there will be a greater need for skilled professionals to manage these systems.

WHY THE NEED FOR CYBERSECURITY PROFESSIONALS?

Given the exponential rise in cybersecurity risks, **all-round safety and protection have become top priorities** for businesses across all industries.


- According to a report by the Australian Cyber Security Growth Network, Australia is expected to need nearly **18,000 additional cybersecurity professionals by 2026**.
 - Moreover, a survey by Robert Half indicated that **87% of Australian CIOs believe cybersecurity risks will increase** over the next five years.
 - Organisations are **now seeking individuals who are equipped with foresight to anticipate potential security** breaches, not just those who can protect their networks and systems.
- 

WHAT YOU CAN DO

Remember that protecting your data & network requires more than a combination of skilled professionals and robust solutions.

The most crucial element of cybersecurity is ongoing vigilance.

When in doubt, partner with a **tech accelerator** who can do all this for you and save your organisation from future time and damage repairment cost.

- **Go for an all-in-one solution** that includes robust network security, threat detection, and incident response capabilities. With a comprehensive approach, you can rest assured that your organisation is protected from the latest cyber threats.
 - **Gain access to a pool of highly skilled cybersecurity professionals.** When you partner with holistic cybersecurity provider, you can augment your existing workforce and leverage their expertise in managing and mitigating cyber risks effectively.
 - **Continuous monitoring and response:** Holistic IT solutions offer proactive monitoring and rapid incident response mechanisms. Their 24/7 surveillance ensures that potential threats are detected promptly, minimising the impact on your business operations.
 - **Tailored strategies and compliance:** A trusted IT partner understands your unique cybersecurity needs and can customize strategies to align with local regulations and industry best practices. This also ensures compliance while fortifying your defences against cyber threats.
- 

TREND 4



THERE'S NO BETTER TIME THAN NOW.

Empower your organisation, mitigate risks and safeguard your digital assets today.



TREND 5

STAY UPDATED ON
REGULATORY
CHANGES

STAY UPDATED ON REGULATORY CHANGES

Regulatory changes will continue to impact the cybersecurity landscape in 2024.

Compliance with regulatory requirements will be critical for businesses to avoid hefty penalties and safeguard their reputations.


With the rising number of cyber-attacks, the Australian government is likely to enforce stricter regulations to ensure organisations take adequate measures to protect their digital assets.

CYBER SECURITY STANDARDS OVER THE YEARS

The Notifiable Data Breaches scheme in 2018.

- Mandates organisations to immediately report any data breaches posing a likelihood of serious harm.
- Since its start, a total of 1,050 breaches were reported in the 2019-20 period alone, a 47% increase compared to the previous years according to the Australian Information Commissioner's report.

The Australian Prudential Regulation Authority (APRA) CPS 234 Information Security standard in 2019

- Ensures that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with the size and extent of threats to its information assets.
- 

PRESENT-DAY: GOVERNMENT TO OVERHAUL PRIVACY LAWS

Digital technology continues to take over various aspects of life, such as work, education, healthcare, shopping, and staying connected with family and friends.

While the digital economy has brought positive changes like innovation and increased productivity, it has also resulted in significant data breaches, putting millions of Australians at risk of identity theft and scams due to the large amount of data being exchanged in digital ecosystems.

The recent 2023 survey by the Office of the Australian Information Commissioner (OAIC) called the Australian Community Attitudes to Privacy (ACAP) Survey showed that Australians really care about keeping their personal information safe.

Out of the people surveyed, 83% expressed a desire for more control and options when it comes to how their personal information is collected and used.

WHAT YOU NEED TO KNOW: CURRENT PRIVACY ACT REFORM

- It uplifts protections
- It strengthen enforcement
- It brings the Privacy Act into the digital age
- Increase clarity and simplicity for entities and individuals
- Improve control and transparency for individuals over their personal information.

WHAT YOU CAN DO

Navigating regulatory changes doesn't need to be tricky.

Simply ask your IT provider about current amendments. Or, partner with a holistic tech provider who has:



Expertise in privacy laws

Get access to their team of cybersecurity professionals who understand the intricacies of privacy laws in Australia, and can guide you through compliance requirements, helping you implement appropriate safeguards to protect sensitive data.



Continuous monitoring and auditability

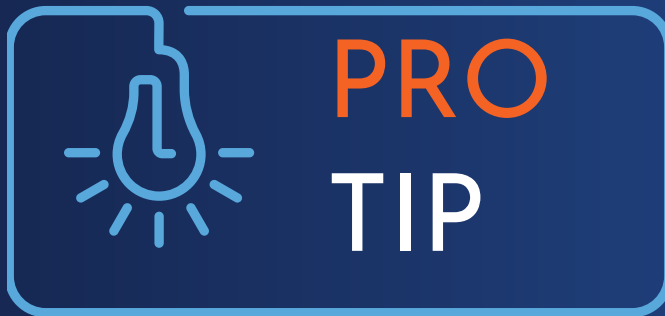
These are part and parcel of a tech accelerator like us. These capabilities enable you to track and log security incidents, demonstrate compliance during audits, and respond effectively to regulatory inquiries.



Adaptability to changing regulations:

Regulatory changes are inevitable in the cybersecurity landscape. The right tech partner will always help ensure that your organisation remains up to date with evolving privacy laws. Their expertise and ongoing support help you proactively address new compliance requirements as they arise.

TREND 5



PARTNER WITH A TECH ACCELERATOR THAT TAKES THIS STRESS LOAD FOR YOU.

Compliance with data & privacy laws is essential for maintaining the trust of your customers and stakeholders. And now it doesn't have to be nerve-wracking anymore.

You can now be aware of privacy laws and have the necessary cybersecurity measures in place to meet compliance requirements effectively.

Don't just stay compliant. Do it with confidence.

SUPER TRENDS THAT
CONTINUE TO GROW

HEIGHTENED DATA
SAFETY FOR
REMOTE WORKING,
MOBILE & IOT

RESOURCE
CONSTRAINTS IN
IT DEPARTMENTS
IN ORGANISATIONS

HEIGHTENED DATA SAFETY

REMOTE WORKING, MOBILE & IOT

A trend that overlaps all the emerging trends we've covered so far is the importance of monitoring the movement of data.

In today's remote working landscape, as more and more people use mobile and IoT devices, it's crucial to understand how and where data is used and shared, and to protect them.

QUICK TIPS

Protect sensitive information to prevent valuable data falling into the wrong hands.

By managing data movement and unauthorised access.

Secure remote access to maintain the confidentiality and integrity of the data.

By establishing secure VPN connections and MFA (multi-factor authentication), so that sensitive information is not compromised while employees work remotely.

Safeguard mobile devices used by your employees and protect data from being compromised if a device is lost or stolen.

By encrypting all mobile devices and enforcing strong passwords and policies, for efficient Mobile Device Management (MDM).

Protect IoT (Internet of Things) devices to ensure the vast amounts of data they collect remain protected from potential threats and cybercriminals.

Through comprehensive security measures: device authentication, data encryption, and regular audits and vulnerability assessments.

RESOURCE CONSTRAINTS IN IT DEPARTMENTS

It's the era of digital transformation, and IT departments in Australia are facing unique challenges.

With increasing demands and the right resources to match, organisations often struggle to effectively monitor and manage cybersecurity threats.

But fret not. Here's how you can address more issues even though you're resource-restricted.

QUICK TIPS

Prioritise comprehensive cybersecurity.

Allocate dedicated time and budget to ensure adequate protection against potential threats.

Invest in training and awareness.

Promote a culture of cybersecurity awareness by conducting regular training to equip your employees with the knowledge and skills to identify threats.

Collaborate with external experts.

Partner with cybersecurity experts with specialised knowledge and support that can augment your IT department's capabilities, and fill any resource gaps to enhance your organisation's overall cyber defences.

Remember, just because you are resource constrained, doesn't mean you deserve to be breached or attacked.

Cybersecurity experts can always help you stay proactive and protected.



TO SUM UP

**TOP TRENDS IN
CYBERSECURITY**
AND HOW YOU CAN
STAY PROTECTED,
STAY VIGILANT,
STAY AHEAD.

2024 TOP TRENDS IN CYBER SECURITY YOU NEED TO WATCH OUT FOR

- TREND 1** Comprehensive Cybersecurity Protection
- TREND 2** Emphasis on Cybersecurity Risk Management
- TREND 3** Increased Use of Artificial Intelligence (AI)
- TREND 4** Greater Demand for Cybersecurity Professionals
- TREND 5** Regulatory Changes
- SUPER TRENDS**
 - Heightened data safety for remote working, mobile devices and IoT
 - Reduce resource restriction to effectively address cybersecurity threats

TIPS TO STAY ON TOP OF YOUR CYBER SECURITY

Consider a comprehensive cybersecurity strategy that fortifies your organisation's defences without burdening limited resources.

Combine advanced security measures with built-in risk management, including intelligent policy control, and real-time visibility.

Don't just go for AI because it's the trend. Go for it after undertaking an assessment of your organisation's specific needs and scope.

Consider partnering with a cybersecurity expert who have an arsenal of skilled professionals, robust solutions and knowledge of regulations.

IT'S YOUR RIGHT TO STAY PROTECTED

Today, tomorrow and beyond.

CHAT TO US TODAY

☎ 02 8424 7900

🔗 www.north-bridge.com.au

📍 Ground Floor, 52 Chandos St
St Leonards NSW 2065

Adopt securely. Adapt fearlessly. Accelerate confidently.

