THE ULTIMATE GUIDE TO CYBER THREAT MANAGEMENT IN 2025

ABSTRACT

Cyber threats in 2025 are more advanced, driven by AI, cloud systems, and automation. This guide highlights key risks and strategies for detection, prevention, and response to help businesses strengthen resilience and protect critical data.

INTRODUCTION

As technology evolves, so do cyber attacks. Ransomware, phishing, and insider breaches remain major risks for businesses of all sizes. Effective cyber threat management now requires proactive planning, smart technology, and employee awareness to stay ahead of attackers.

I. Cyber security and your business

Effective cyber security helps protect your business from cyber-attacks. Learn about cybercrime, the types of online threats and what to do if you're a victim of cyber-attack or scam.

Latest cyber security threats

Stay up to date on the latest cyber security threats and alerts for small and medium businesses on the **Australian Cyber Security Centre (ACSC) website**.

What is cyber security?

Cyber security is about protecting your technology, data and information from:

- accidental or illegal access
- corruption
- theft
- damage.

You need to protect any digital information that your business creates, collects or stores. A secure system is essential to protect your business from cybercrime and maintain customer trust.

Here are some common online threats to watch out for.

Scams

A scam is when a criminal tricks you into giving them money or personal information. Online scams cost Australian people and businesses millions of dollars every year.

Scammers are always coming up with new ways to take advantage of people and businesses. Some common methods are:

- pretending to be from a bank or government department and asking for payments or personal information
- using fake dating or social media profiles to gain your trust
- telling you that your account or computer system has been compromised and they need money or personal information to fix it.

Account compromise

This is when a cyber criminal gains access to your email, social media, banking or other accounts.

Criminals can use compromised accounts to steal money, information or identities.

Phishing

Phishing is a type of scam. It uses fake emails or text messages to trick you into giving out private information or account details.

Phishing messages often seem to be from someone you trust, including people in your business. They can also appear to be from a large organisation or government agency.

Malware

Malware is short for malicious software. It means any programs or applications that are designed to cause harm.

Malware can steal your confidential information, hold your system to ransom or install other programs without you knowing.

It can enter your system by:

- spam emails and messages
- websites
- exploiting weaknesses in your software
- posing as a trusted application that you install.

Ransomware

Ransomware is a type of malware. It 'locks' your files, making your system or device unusable unless you pay a ransom fee.

Hacking

Hacking is when someone gains unauthorised access to your system, network or device. They might do this by finding out your password or exploiting a software vulnerability.

Once inside your system, a hacker could:

- steal your data, including passwords and financial details
- install malware
- watch what you are doing
- change how your system works.

Data breaches

A data breach is when sensitive or personal information is accessed, disclosed or exposed to unauthorised people.

This can happen by accident (for example, if you accidentally send an email with personal information to the wrong person). Or it can be the result of hacking or another security breach.

A large-scale data breach involving customer information can be very damaging to your business's reputation.

Identity theft

Identity theft is when a cyber criminal has enough of your personal information that they can pretend to be you. They use this information to do things like:

- steal money from your bank accounts
- create fake ID documents in your name
- apply for loans or government benefits in your name.
- Direct Financial Losses
- Quicker Attacks, Wider Effects
- Data Theft and Privacy Breaches
- Reputational Damage
- Increased Security Costs

II. 10 Ways Cybercrime Impacts Business

Cybercrime is among the most significant threats to modern businesses—no matter the size of the company or its sector. With damage estimated at $10.5 trillion globally in 2025—enough to make it the world's third-largest economy after the U.S. and China—cybercrime has become an unavoidable business risk that affects every organization with digital assets.

Here is a look at the most important ways cybercrime is affecting businesses today.

1. Direct Financial Losses

From Fortune 500 companies to small businesses, from traditional manufacturers to leading-edge tech firms, no enterprise is immune to these threats. Meanwhile, the average cost of a data breach reached $4.88 million in 2024, about a 20% jump since 2020.2

These costs are the best-known outcome of cyberattacks, which derive from the following:

The Immediate Costs

These can include the following:

- Ransomware payments, which are predicted to cost more than $265 billion annually by 20313

- Emergency IT services and cybersecurity consultants
- Legal fees and potential fines
- Customer notification and credit monitoring

Operational Costs

- System downtime and productivity losses
- Revenue losses during system outages
- Emergency hardware or software purchases
- Cost of recovering or rebuilding compromised data and systems

Long-Term Financial Effects

- Increased insurance premiums
- Investment in enhanced security measures
- Staff training and security awareness programs
- Ongoing monitoring and compliance costs

Real-world examples highlight how quickly major bills come due for those targeted by cybercriminals. In 2023, MGM Resorts International (MGM) reported that a September cyberattack caused a $100 million hit to its third-quarter results. The company then spent another $10 million on consulting, legal, and other fees related to the incident.

Cybercriminals aren't only targeting for-profit firms: London hospitals had to cancel over 800 planned operations and transfusions, as well as 700 outpatient appointments, in June 2024 because of a ransomware attack targeting their blood-test analysis system.

In addition, universities across the world have been targeted, with some forced fully offline for weeks.

2. While Attacks Are Getting Quicker, the Effects Are Far Wider

Modern cyberattacks move with stunning speed. In 2023, the average time it took cybercriminals to move laterally within a network (known as "breakout time") decreased by about a third. Thus, businesses often won't have the time to react and contain threats before a significant attack is in place.7

While the time attackers need is shrinking, their reach is expanding. Major incidents illustrate the broad effects of these attacks:

- A 2024 cyberattack on the medical payment processor Change Healthcare, which one expert called the "biggest ever cybersecurity attack on the American healthcare system," prevented healthcare practices nationwide from receiving payments for weeks.8
- A June 2024 attack on CDK Global, which provides software to thousands of car dealerships in the U.S. and Canada, affected about 15,000 dealerships, causing many to go without payments and stopping them from moving inventory off their lots.9

Often, the initial numbers seem small but grow quickly:

- A 2023 breach in the systems of the ancestry tracking firm 23andMe Holding Co. (ME) originally appeared to affect only 0.1% of customers (14,000 individuals) but ultimately impacted 9 million users through access to ancestry information.10
- Cloud storage company Snowflake reported in June 2024 that 165 customers were compromised by credential theft, with just one incident exposing 560 million Ticketmaster customer records.11

3. Data Theft and Privacy Breaches

Hackers focus on stealing sensitive information that can be monetized or used for further attacks. However, the consequences of data breaches go beyond the immediate theft, impacting regulatory compliance, customer trust, and operational continuity.

Businesses are shifting resources to focus on data encryption, multi-factor authentication, and regular audits to safeguard their systems.

4. Reputational Damage

The reputational impact of cybersecurity incidents can outlast all other consequences, affecting an organization's relationships with customers, partners, and investors.

- An immediate 3.5% drop in stock price following news of the breach
- Continued underperformance against the Nasdaq by 3.5%
- Long-term effects on their market reputation and investor confidence13

The erosion of customer trust can also be significant. According to research by IBM, loss of customer trust accounted for nearly 40% of the cost of breaches. This comes from customer churn, marketing needs, and other efforts to rebuild trust after such incidents.2

Fast Fact

While all industries are affected by cyberattacks, they don't all face the same hits to their reputation and stock price. Researchers at Comparitech found that healthcare companies had the steepest decline in share prices, lagging the Nasdaq by 10.6% in the six months after disclosure of a breach. It was followed by the finance sector (6.4% underperformance) and manufacturing (4.0%).14

Long-Term Reputational Effects

The impact on a company's reputation can be extensive over time:

- Greater difficulty acquiring new customers
- Challenges in maintaining business partnerships
- Increased scrutiny from regulators and industry watchdogs
- Higher costs for insurance and financial services
- Ongoing media and public relations challenges

5. Increased Security Costs

The investment required to prevent and respond to cyber threats represents a significant and growing business expense. Organizations face mounting pressure to strengthen their security posture through various investments.

Spike in Security Budgets

- Global cybersecurity spending is projected to total $212 billion in 2025; a 15% increase from the year before, and will only get more costly.15

Ongoing Operational Costs

- Staff training and security awareness programs
- Continual monitoring and threat detection
- Regular security assessments and penetration testing
- Compliance maintenance and documentation
- Higher insurance premiums

6. Supply Chain Vulnerabilities

Modern businesses depend on interconnected digital supply chains, making them susceptible to cascading risks if one link is compromised. Supply chain attacks are surging, with breaches often originating through third-party vendors. High-profile incidents, such as the SolarWinds hack, underscored how vulnerabilities in software supply chains can expose thousands of downstream companies.16

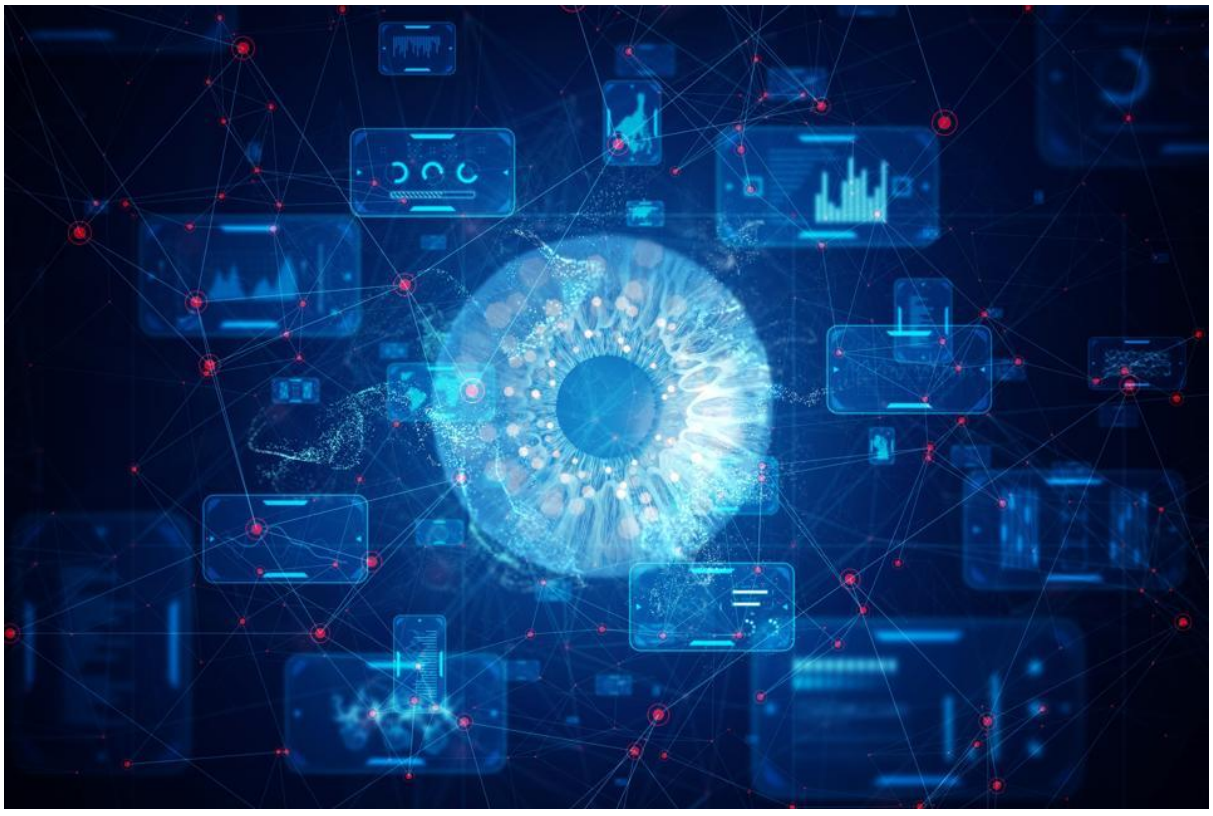
Businesses are increasingly investing in third-party risk management and supply chain security measures to mitigate these growing threats.2

7. Cloud Security Challenges

Cloud-based systems, essential for modern business operations, are facing unprecedented threats. In 2023, cloud-related cyber intrusions increased by 75%, largely because of systems, unpatched vulnerabilities, and the exploitation of shared environments.

To combat these risks, organizations are prioritizing investments in cloud-specific security measures, such as encryption, identity management, and multi-factor authentication.

III. How Cyber Risk Management Should Evolve With The Threat Landscape



When cybersecurity budgets are discussed in the boardroom, the expectation is that the chief information security officer (CISO), like any other C-level executive, will walk in with a clear financial breakdown: “You gave me $5 million to address our $100 million cyberrisk exposure. I reduced that risk by $23 million, and to continue this progress by $X million next year, my budget should increase by $X.”

But this isn’t how these conversations typically go. Instead, security leaders typically present compliance checklists, regulatory obligations and ambiguous risk scores that executives then struggle to translate into financial and operational impact. Let’s explore what can cause this disconnect and how leaders can bridge the gap between cybersecurity and business decision making.

More Data But Less Clarity

The explosion of AI has transformed the cyber threat landscape, creating both opportunities and challenges. AI-generated data has surged to an unprecedented scale. Meanwhile, adversaries are using AI to automate and scale attacks, exploiting weaknesses faster than many organizations can react. Amazon recently reported encountering 750 million cyberthreats per day (paywall) in 2024—up from just 100 million 6 or 7 months earlier.

Many security leaders are flooded with data but lack actionable insights. When every security tool, endpoint and cloud service generates a stream of alerts, it can lead to alert fatigue rather than meaningful risk reduction. According to a 2022 report from Orca Security, 55% of security teams reported missing critical alerts, often on a daily or weekly basis, likely due to the overwhelming volume.

Increased Threats And Regulatory Pressures

Cybersecurity is no longer just an IT issue—it is a core financial risk that directly impacts a company’s bottom line. The global average cost of a data breach has risen to $4.88 million, underscoring the financial stakes of ineffective risk management. What’s more, governments and regulatory bodies are requiring more active approaches to cyber risk. The SEC’s cyber disclosure rules now hold public companies accountable for reporting “the board of directors’ oversight of risks from cybersecurity threats and management’s role and expertise in assessing and managing material risks from cybersecurity threats.” Investors and customers expect transparency, and compliance checklists are no longer enough.

Security teams need to be able to articulate the financial impact of cyber risk mitigation, just as CFOs do with revenue projections and investment strategies. Yet instead of providing clarity, I have found that traditional governance, risk management and compliance (GRC) platforms can exacerbate the problem. Designed for structured reporting and static compliance, they often struggle to

integrate real-time risk intelligence, leaving CISOs to sift through fragmented data silos with no clear way to prioritize or quantify cyber risk in financial terms.

In my view, GRC was never designed for cybersecurity. It was built for a world where risk was assessed periodically, threats evolved slowly and compliance frameworks dictated security priorities. But today's cyber threats demand real-time risk assessment, continuous monitoring and strategic decision making at the highest levels.

Effective Strategies For Improving Cyber Risk Management

Digital transformation has pushed cybersecurity into the spotlight, and I believe AI is key to making cyber risk actionable at the board level. Cyber risk must no longer be treated as a siloed function—it must be fully embedded into the fabric of business decision making, aligning security, operations and finance under a single strategic framework.

The opportunity lies in transforming GRC into a true cyber risk management function—one that is dynamic, intelligent and seamlessly integrated into enterprise risk strategy. AI-driven cyber risk platforms ingest and analyze millions of data points in real time, correlating internal security telemetry with external threat intelligence. *(Full disclosure: My company offers a platform like this.)* This shift enables security leaders to provide actionable insights to executives, ensuring cyber risk is managed like any other critical business risk.

To achieve this, companies need to modernize their GRC programs with a proactive, risk-based approach. AI-driven cyber risk platforms are one powerful tool in this transformation, as they can ingest and analyze millions of data points in real time, correlating internal security telemetry with external threat intelligence. However, successful adoption requires careful planning. Organizations should establish clear data governance policies, ensure AI models are trained on relevant and high-quality datasets and integrate these capabilities into existing workflows to maximize value.

Beyond AI, there are other critical steps security leaders should take to improve their risk management programs:

• **Enhance risk visibility:** Implement continuous monitoring and automated controls to provide a real-time view of cyber risk exposure.

• **Align with business priorities:** Engage finance and operations teams in cyber risk discussions to ensure security investments align with business objectives.

• **Address common pitfalls:** Many companies struggle with outdated risk models and fragmented reporting. Streamlining risk assessment processes and leveraging frameworks like NIST 800-30 or the FAIR model can help create a more standardized and effective approach.

The shift from using traditional GRC alone is not a failure—it is an overdue evolution. Businesses that continue to rely on outdated compliance frameworks will likely struggle with inefficiencies, regulatory pressure and increased exposure to cyber threats. Those that embrace new tools and strategies can gain a strategic advantage and become more resilient in an era of escalating threats. The future belongs to organizations that recognize cybersecurity as a boardroom imperative. Those that fail to evolve won’t just be out of compliance—they could be outpaced, outmaneuvered and ultimately, unprotected.

IV. Top 10 Cyber Threats Facing Australian Businesses

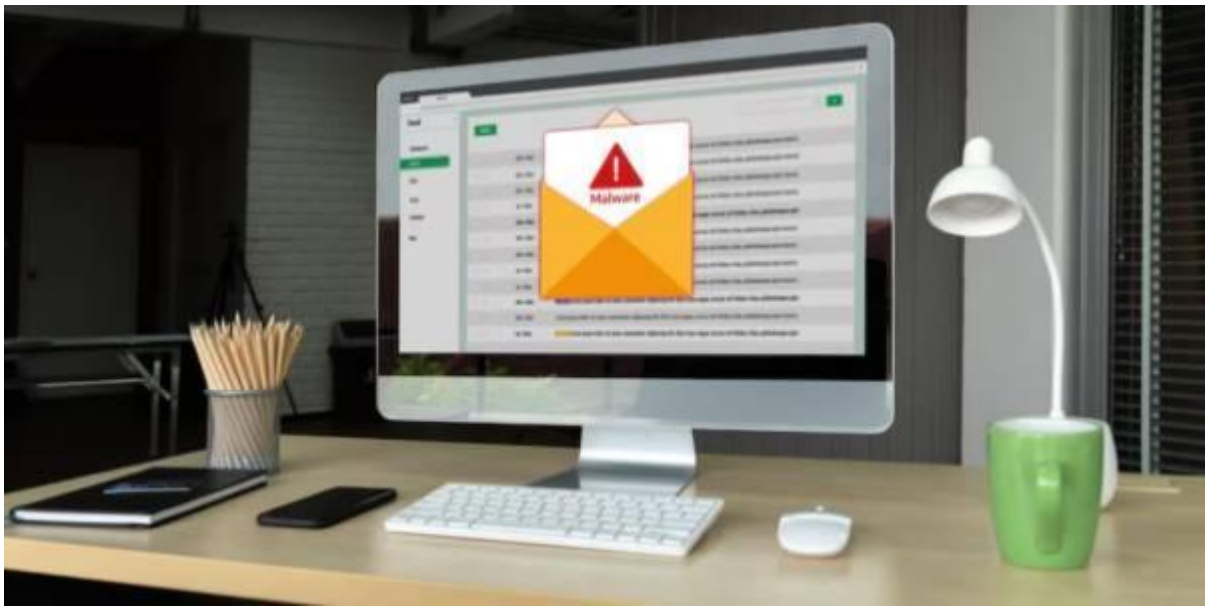
Digitisation was the first transformative step that made business data vulnerable. The advent of automation tools, the use of the Internet, and remote work arrangements have made it even more susceptible to theft. Cybercriminals target small businesses with a wicked intent to steal confidential data and demand ransom. Many immoral hackers penetrate reputed corporate networks to showcase their hacking abilities and gain fame. Some of them also have a political agenda or personal vendetta against a business.

While the big businesses have the necessary security features in place, the smaller ones become easy targets. They do not implement the required cybersecurity

measures, and their employees are unaware of the hacking tactics used by criminals. Small entities have a much higher rate of facing cyber attacks, and the number is growing every year. **Here is a list of the top ten cyber threats faced by Australian businesses** that should be known to all business people and employees to stay alert and aware.

1. Business Email Compromise
2. Malware
3. Ransomware
4. Data Breaches
5. SQL injection
6. Insider Threats
7. Denial of Service Attacks
8. Identity Theft
9. Password Attack
10. Quishing

1. Business Email Compromise



In the annual cyber threat report for 2023-24 by the Australian Signals Directorate, the topmost reported cybercrime was business email compromise. It is a phishing attack wherein hackers dupe employees by posing as a trusted individual associated

with the business. They send emails with fake bills to make financial gains or ask the employees for confidential business information that can be used for cybercrime. Sometimes they hack the email account of the CEO of the organisation and send emails to employees to make them look authentic. They also use hacked email accounts of business lawyers, partners or stakeholders to carry out the scam. They ensure to send emails to employees with the authority to purchase or provide information. It can lead to significant losses and the leaking of sensitive information.

2. Malware

Malware is malicious software widely used for cyber attacks and can damage or disrupt a computer, server or network. Various types of malware include viruses, Trojan, ransomware, spyware, adware, etc. It infects the system and renders it unusable to impact the business. Malware can also be used to steal information or get a ransom from the organisation. Individuals who plan to purchase a business for sale Brisbane should ensure they stay protected against this threat with anti-virus, network security, strong passwords and multi-factor authentication.

3. Ransomware

Ransomware is a common cyber threat that affects businesses. Hackers carry it out for financial gain. They catch hold of confidential business information and ask for money to stop it from getting leaked. The attack involves encrypting all the systems, files, and documents across devices to make the workforce helpless and create forced downtime until the ransom is paid. Businesses can protect themselves from this threat by creating offline data backups stored far from the office. They must adopt cyber security measures and install intrusion detection systems.

4. Data Breaches

Data breaches are becoming prevalent in the country, wherein hackers gain unauthorised access to business information. They can destroy, modify, steal or leak the information, which can be damaging to the business's reputation. Usually, businesses that store customer details like credit card information get targeted by cybercriminals. They can use this information to hack bank accounts. Entrepreneurs can stay safeguarded from this threat by training their employees to maintain data security. They must follow the customer data privacy protocols, coach remote workers and follow data encryption.

5. SQL injection

SQL injection is a hacking technique in which a malicious SQL query is injected into application's software. It allows cybercriminals to access confidential data, make changes to the information, modify transaction data, impersonate an employee, etc. Hackers use this attack to gather customers' credit card information and misuse it for financial gains. Individuals who plan to acquire businesses for sale in Brisbane must ensure their databases are secure and up-to-date to safeguard them from these threats.

6. Insider Threats

Insider threats can also affect a business significantly because employees have access to confidential data and can misuse it for personal vendetta. They may also leak sensitive information by mistake without ulterior motives because of carelessness. It can lead to fines, downtime, loss of credibility and financial deficits. The insider threat can be prevented by training employees about cyber security protocols and offering access to confidential data to only a limited number of employees with a reliable track record.

7. Denial of Service Attacks

DoS attacks are identified by crashing the website because of an onslaught of traffic that creates too much pressure on the network or server. It can badly impact e-commerce businesses due to loss of customers and trustworthiness. If the site is not up quickly, it can lead to a decline in revenue and negative publicity. The restoration of the site can also impact the business financially and pull it into debt. Entrepreneurs can stay protected by implementing intrusion detection and prevention systems that help to restrain malicious traffic, and they can also use traffic balancers to channel it across servers.

8. Identity Theft

Cybercriminals can take on the identity of a senior employee or the CEO to take out money from the business account or a loan from the bank. They can also steal vital information. It can be a challenging predicament for the individuals whose identity has been stolen because they may have to prove their real identity. It can make banks question their creditworthiness, which can affect funding in future for business growth. Thus, if an individual has a plan to acquire a business for sale in Brisbane, they must secure their personal identity documents

9. Password Attack

Password attacks are quite common and involve cracking the password of an authorised user to enter the system or network. These can be of different types including brute force, password spraying, dictionary attack, credential stuffing, etc. Most users create the same passwords for all logins and do not pay much attention to the strength of the passwords, which increases the vulnerability of the systems. This is why multi-factor authentication is a powerful protective shield against password attacks.

10. Quishing

Like phishing, quishing is a type of cyber threat that uses malicious QR codes to scam workers. Users scanning the QR code are made to divulge sensitive information or download a virus that impacts the business. Since most people trust QR codes, the probability of scanning them without verification is high. It can be used to replicate classified information or gain access to the system. Therefore, aspiring entrepreneurs planning to buy a Brisbane business for sale must train their employees to check the source of the code, use manual online transaction methods and avoid downloading apps or files using codes.

Cyber threats are a growing menace in the digitally connected world, where business information and financial transactions are stored on the network. It is vital to keep this secret information private using up-to-date cyber security measures that cannot be breached easily.

V. Keeping your business cyber secure

The free Cyber Wardens program helps you prepare your business to prevent cyber attacks. The program includes self-paced cyber security short courses, webinars and guides to help you protect your business and upskill your team.

Register for a free cyber security webinar.

Cyber security includes the tools, techniques and processes to protect IT data and systems from attacks, and the people who manage them.

All businesses need to be cyber secure, no matter the size or industry. For small businesses, even a minor incident can be devastating.

The average cost of cybercrime in Australia is:

- $49,600 for small businesses
- $62,800 for medium businesses
- $63,600 for large businesses.

Online threats and risks

Online threats and risks can target your IT systems, data and online assets causing:

- brand and reputational damage
- loss of confidential and sensitive data
- loss of business continuity
- fines if your business is found negligent.

The most common types of cyber threats to small business are:

- **scam messages** (phishing)—designed to trick recipients out of money and data
- **malicious software** (malware)—provides criminals with a way to access important information (e.g. bank or credit card numbers and passwords). It can also take control of or spy on a user's computer
- **ransomware** —a type of malware that locks down your computer or files until a ransom is paid.

Educate yourself and your team

Ensure your staff are well trained in good cyber security practices. Include cyber security in staff inductions and provide regular staff training. Learn more by:

- enrolling your team in the free Cyber Wardens program. This program makes it easier for you to increase your business's cyber readiness to prevent attacks and be resilient to them. The program includes a range of self-paced cyber security short courses, webinars and guides to help you better protect your business
- connecting with IDCARE's Small Business Cyber Resilience Service which is specifically designed to help you build cyber resilience and recover from cyber incidents. It's free for small businesses with 19 or less full-time equivalent staff and an active ABN
- watching cyber security webinars and reading related information sheets
- reading the Ask a mentor—cyber security mentor tips from our Mentoring for Growth program
- checking your business's cyber fitness by attending a Mentoring for Growth session.

How to protect your business from cybercrime

The Small business cyber security guide (PDF, 1.5MB) by the Australian Cyber Security Centre (ACSC), steps you through basic security measures.

As a starting point, the ACSC recommends the following 3 actions:

- turn on multi-factor authentication—a security measure that requires 2 or more proofs of identity to grant access to your accounts
- update your device and software—this can fix security flaws in your operating system and other software
- back up your information—learn how to back up your files and devices.

The guide may include measures that are not relevant to your business, or your business may have more complex needs.

After completing this guide, the ACSC recommends small businesses implement Maturity level one of the Essential eight.

Report cybercrime

If you are a victim of cybercrime, find out how to get help and how to report the crime. IDCARE can support eligible businesses with recovery from a cyber or privacy related incident.

Reporting suspicious online activities can help authorities to combat cybercrime and enable them to develop tools and awareness programs to protect businesses and individuals from attacks.

IT threat preparation

Protect your business by securing bank accounts and managing access to personal and financial information, using suitable IT system security, and consider purchasing insurance. Learn more about preparing, preventing, responding and recovering from an IT threat.

Working with IT professionals

If you have questions about this information or cyber security in general, we recommend you speak to an IT professional or trusted adviser. To improve your cyber security resilience, learn how to choose digital services and specialists.

Your legal obligations

If your business handles personal data (of employees, customers and suppliers) and financial information, you are responsible for meeting all legislative data-protection requirements. Know your legal obligations for online businesses, including storing and protecting privacy information.

CONCLUSION

In 2025, cybersecurity is a business priority, not just an IT concern. Organizations that adopt adaptive tools, strong policies, and ongoing training will better safeguard their systems and thrive in the digital future.

REFERENCES

Cyber security and your business | Business Government, Retrieved 23 September 2023 from https://business.gov.au/online-and-digital/cyber-security/cyber-security-and-your-business

By Peter | 10 Ways Cybercrime Impacts Business | Investopedia, Retrieved 20 February 2025 from https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx

By Jerry | How Cyber Risk Management Should Evolve With The Threat Landscape | Forbes, Retrieved 12 March 2025 from https://www.forbes.com/councils/forbesbusinesscouncil/2025/03/12/how-cyber-risk-management-should-evolve-with-the-threat-landscape/

By Liam Walker | Top 10 Cyber Threats Facing Australian Businesses | Busines2Sell, Retrieved 17 December 2024 from https://www.business2sell.com.au/blogs/evaluation/top-10-cyber-threats-facing-australian-businesses

By Vikki | Top 10 threat detection tools for cybersecurity | Cyber Magazine, Retrieved 14 April 2023 from https://cybermagazine.com/articles/top-10-threat-detection-tools