huonit
A KYOCERA GROUP COMPANY

www.huonit.com.au

Security Guide

Protecting Your Business in the Digital Age

Your business is a potential target for cybercriminals

In today's interconnected world, organisations have embraced digital technologies to reach global markets, reduce costs, and create more productive workplaces. However, as your business becomes more mobile and connected, your systems, networks, and data face increasingly sophisticated cybersecurity risks.

According to the Australian Cyber Security Centre (ACSC), a cybercrime is now reported every six minutes in Australia, with self-reported losses totaling more than $2 billion. The average cost of a data breach for Australian businesses has reached $4.75 million in 2023, a 12.9% increase from the previous year.

The consequences extend far beyond financial impact. A data breach can severely impact your business, leading to operational downtime, loss of customers, brand reputation damage, identity theft, compliance and legal issues.

As your trusted IT security partner, Huon IT understands that effective data security is more critical than ever — especially in the era of hybrid work. Criminals, hackers, and scammers are becoming increasingly sophisticated, with their methods and technologies constantly evolving. The ACSC reports a 23% increase in cybersecurity incidents in the past year, with a notable rise in critical infrastructure attacks.

This guide will help you understand:

- The top cybersecurity threats facing Australian businesses
- How these threats can compromise your data and impact your business security
- How Huon IT can help improve your security posture with comprehensive protection strategies

What is phishing?

Phishing continues to be one of the most prevalent threats to Australian businesses, with losses reaching $58.9 million in 2023 according to Scamwatch. These attacks use deceptive emails, phone calls, text messages, and websites to trick recipients into providing sensitive information or downloading malicious software.

As your IT security partner, we've seen how these attacks can lead to serious data breaches, compromised systems, and significant financial losses. Particularly concerning is the 200% increase in SMS-based phishing ("smishing") attacks targeting Australian businesses.

How to recognise phishing emails

Fraudulent emails often use the same branding and logo as popular brands, such as banks, credit card companies, telephone companies, courier services, social media sites, or payment providers. Text messages will appear to come from a known company. The email or text message will ask you to verify your personal details, confirm a package delivery, claim a prize, or complete a survey.

The hacker may even pretend to be from a software company, internet service provider, or security firm informing you of 'suspicious activity' on your account.

3 ways to protect your business from phishing

With phishing scams on the rise in Australia, we implement comprehensive protection through:

1. Advanced Protection Technologies

Working with Huon IT ensures your business has enterprise-grade security solutions including advanced firewalls, spam filters, anti-virus, and anti-spyware software across all computers, devices, and servers. We manage regular updates and maintenance to ensure maximum protection against evolving threats.

2. Comprehensive Monitoring Services

Our security operations center provides complete visibility across your business information environment. We track website traffic, email communications, and network activities 24/7, quickly identifying and responding to potential threats.

3. Employee Security Training

We deliver comprehensive security awareness programs, including phishing simulations, security best practices, and clear incident response procedures. Our training ensures your staff becomes your first line of defense against cyber attacks.

What is ransomware?

Recent data shows that 76% of Australian organisations experienced a ransomware attack in 2023, with average ransom payments reaching $1.2 million according to Sophos State of Ransomware 2023. Healthcare has been particularly targeted, accounting for 22% of all attacks.

Ransomware restricts access to important files stored on a computer or server and has become one of Australia's fastest-growing and most damaging cyber threats.

How ransomware works

Ransomware typically begins by infecting an unprotected computer through a phishing email or fake website. The malware encrypts business data, making it inaccessible. Sometimes, it can lock users out of their computers entirely.

Once systems are infected, hackers threaten to release information publicly or destroy data unless demands are met. However, paying the ransom provides no guarantee of data recovery.

3 ways to safeguard your business from ransomware

We implement a comprehensive defense strategy:

1. System Protection and Maintenance

Our team ensures all your systems are regularly updated with the latest security patches and protection software. We manage firewalls, anti-virus, anti-spyware, and anti-malware programs across your entire network.

2. Robust Backup Solutions

We implement automated backup systems across multiple secure locations, ensuring business continuity even in the event of an attack. Regular testing validates your ability to recover quickly from any incident.

3. Security Culture Development

Our security awareness programs create a culture of vigilance across your organisation, ensuring everyone understands their role in preventing ransomware attacks.

What is the risk with malicious insiders?

According to recent studies, insider threats now account for 67% of data security incidents in APAC organisations, with the average cost reaching $15.4 million globally in 2023 (Proofpoint 2023).

Australian businesses face particular challenges with insider threats due to increasing remote work arrangements.

How Huon IT protects against insider threats

We implement comprehensive insider threat protection through:

1. Access Management control over system access, regular access reviews, and sophisticated user behavior analytics.

2. Data Protection Advanced Data Loss Prevention (DLP) solutions, document encryption, and secure file sharing systems.

3. Policy and Training on security policies, regular training, and established incident response procedures.

What is a document security breach?

A document security breach involves unauthorised access to sensitive information, including personal details, financial data, and intellectual property. The average cost of a data breach to an Australian business reached $4.75 million in 2023, with regulated industries facing additional compliance penalties.
The Australian Privacy Act now carries penalties of up to $50 million for serious breaches, making effective document security more critical than ever.

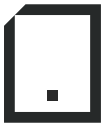
How to protect your business from document security breaches

1. Secure Infrastructure

We implement comprehensive security across all endpoints, including printers and multifunction devices, often overlooked as security vulnerabilities.

2. Document Management

Our solutions provide secure document storage, access tracking, and comprehensive audit capabilities.



3. Mobile Security

We implement robust mobile device management and security policies to protect data across all devices and locations.

4. Managed Print Services

Our managed print services include advanced security features, protecting sensitive documents throughout their lifecycle.

Conclusion

Your business data is one of your most valuable assets and must be protected. As your trusted IT security partner, Huon IT provides comprehensive protection against both traditional and emerging cyber threats. Our team of security experts are ready to help you:

- Assess your current security posture
- Identify and address vulnerabilities
- Implement comprehensive security solutions
- Maintain ongoing protection against evolving threats

Contact Huon IT today to learn how we can enhance your security posture and protect your business from modern cyber threats.

www.huonit.com.au **info@huonit.com.au** **1300 HUON IT**