Cyber Security for Finance Professionals in the Cloud

Protecting Your Business, Your Clients, and Your Reputation

INSTITUTE OF FINANCIAL PROFESSIONALS AUSTRALIA

Harvey Norman
TECHNOLOGY FOR BUSINESS

Making Enterprise-Grade IT Solutions Affordable For Small Business

What We Will Cover Today

Today's 45-Minute Session

- Why finance professionals are a key target for cyber crime
- How cyber threats impact your cloud-based practice
- Current compliance and security expectations
- Practical steps to protect your business and clients
- How Harvey Norman Technology for Business can help

Designed for finance professionals – no jargon, no unnecessary complexity.

Why Finance Professionals Are Targeted

The Cloud-Dependent Advisory Practice

Your tax, planning and SMSF work runs in the cloud:

- Xero Tax, Class, BGL, XPLAN
- ATO portals and SMSF compliance platforms
- Cloud document storage and sharing
- Email and collaboration platforms
- Remote access from anywhere

Cloud platforms bring convenience and efficiency but they also expand your exposure to cyber threats.

What Makes Advisers a Target

Attackers target advisers because you hold:

- Access to multiple client financial systems
- Bank account and payment details
- Tax file numbers and personal data
- ATO portal credentials
- Trusted relationships with clients

One compromised advisory practice can expose dozens of client businesses and funds.

The Data You Hold

Your clients trust you with:

- Financial records and bank statements
- Personal identification information
- Business activity statements
- Superannuation and SMSF fund data
- Tax returns and lodgement records

A single breach impacts:

- Their business operations
- Their regulatory compliance
- Their trust in you

Data protection equals client retention.

The Cost of a Breach

The average cost of cybercrime for Australian small businesses now exceeds $56,000[1] per incident.

Beyond the financial cost:

- Loss of client trust and reputation damage
- Regulatory penalties and TPB consequences
- Operational downtime and disruption
- Legal liability and notification obligations

Cyber security is not an IT issue it is a business risk Issue.

Source: Australian Signals Directorate Annual Cyber Threat Report 2024-25

The Cyber Threat Landscape

ASD Annual Cyber Threat Report 2024-25

Key findings:

- Over 87,400 cybercrime reports in 2024-25
- Cybercrime cost Global economy $10 trillion annually
- Ransomware and data breaches increasing in frequency
- Small businesses remain high-value, low-defence targets
- Identity compromise is the primary attack path

Source: Australian Signals Directorate Annual Cyber Threat Report 2024-25

Top Attacks Affecting Advisers

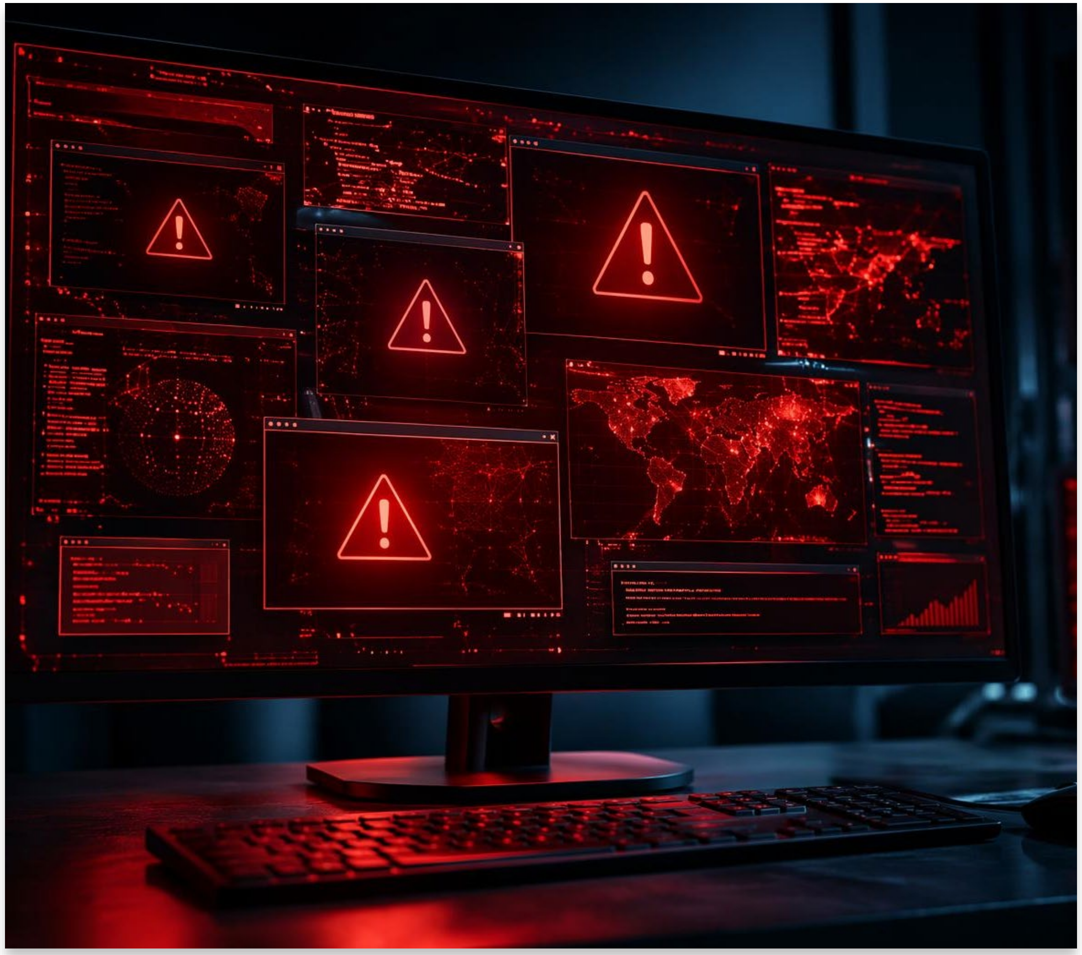
Account Compromise – Stolen credentials used to access email, cloud services, and client portals

Business Email Compromise – Fake emails impersonating clients, suppliers, or the ATO to redirect payments

Data Breaches – Unauthorised access exposing sensitive client information

Ransomware – Malicious software that locks your files until a ransom is paid

Phishing – Deceptive emails designed to steal your login credentials



Phishing and Business Email Compromise

How it works:

- Emails impersonating the ATO, banks, or clients
- Fake invoices requesting payment to new bank details
- Urgent requests to update payment or bank information
- Links to fake login pages that steal credentials

Most cyber fraud starts with human error, not system failure.

Account Compromise and Credential Theft

What happens:

- Attackers steal or guess your login credentials
- Access your email, cloud accounting, or ATO portal
- Escalate access to client data and systems
- Send fraudulent emails from your account

Identity is now the primary attack path in cloud environments.

Ransomware

The numbers:

- 69% of Australian businesses hit by ransomware in the past 5 years
- 84% of those affected paid the ransom
- Average ransom payment: $1.35 million
- Small businesses are seen as easy targets

Impact on advisory practices:

- Loss of access to all client files
- Inability to meet lodgement and SMSF reporting deadlines
- Potential liability for client data loss

Cloud-Specific Risks

Cloud platforms introduce unique risks:

- Misconfigured sharing and access permissions
- Weak or reused passwords across platforms
- Unmonitored third-party application access
- Data stored in overseas jurisdictions
- Shadow IT: unapproved tools and integrations

Cloud does not mean the provider handles all your security. You share the responsibility.

Compliance and Expectations

Legal and Regulatory Expectations

Cyber security is now a legal expectation across regulators:

- **ASIC** – AFS licensees must actively manage cyber risk and resilience
- **APRA** – CPS 234 mandates information security for super funds and regulated entities
- **TPB** – tax practitioners must use verified cyber security to protect client data
- **OAIC** – the Notifiable Data Breaches scheme requires securing and reporting on personal data

In Plain English:

Regulators now treat cyber security as a legal duty (not an option) with penalties, license conditions, and personal liability for falling short.

The Essential Eight Framework

What is it?

A set of eight cyber security strategies developed by the Australian Signals Directorate (ASD) to protect against common cyber threats.

Why it matters for advisers:

- Increasingly expected by cyber insurers
- Referenced in government procurement
- Demonstrates due diligence to clients
- Aligns with TPB compliance expectations

The Essential Eight is the minimum baseline that would prevent the vast majority of cyber attacks.

The Eight Strategies

Prevent attacks:

1. Application Control
2. Patch Applications
3. Configure Microsoft Office Macros
4. User Application Hardening

Limit impact of attacks:

5. Restrict Administrative Privileges
6. Patch Operating Systems
7. Multi-Factor Authentication

Recover data and availability:

8. Regular Backups

Maturity Levels Explained

Three maturity levels:

Level 1: Protection against opportunistic attacks

Level 2: Protection against targeted and deliberate attacks

Level 3: Protection against sophisticated, advanced threats

For advisers:

Maturity Level 2 is the minimum sensible target for any business handling sensitive client data.

What Maturity Level 2 Looks Like

At Level 2, your business:

- Can withstand targeted phishing attempts
- Can recover from ransomware attacks
- Has visibility of suspicious activity
- Has strong baseline cyber hygiene
- Meets growing compliance expectations

Level 2 significantly reduces financial fraud, data breaches, and operational disruption.

Practical Steps to Protect Your Practice

Multi-Factor Authentication

Enable MFA on everything:

- Advisory software (Xero Tax, Class, BGL, XPLAN)
- Email and Microsoft 365 / Google Workspace
- ATO portals and government services
- Banking and payment platforms
- Remote access and VPN connections

In Plain English:

A password alone is not enough. MFA means even if someone steals your password, they still cannot get in.

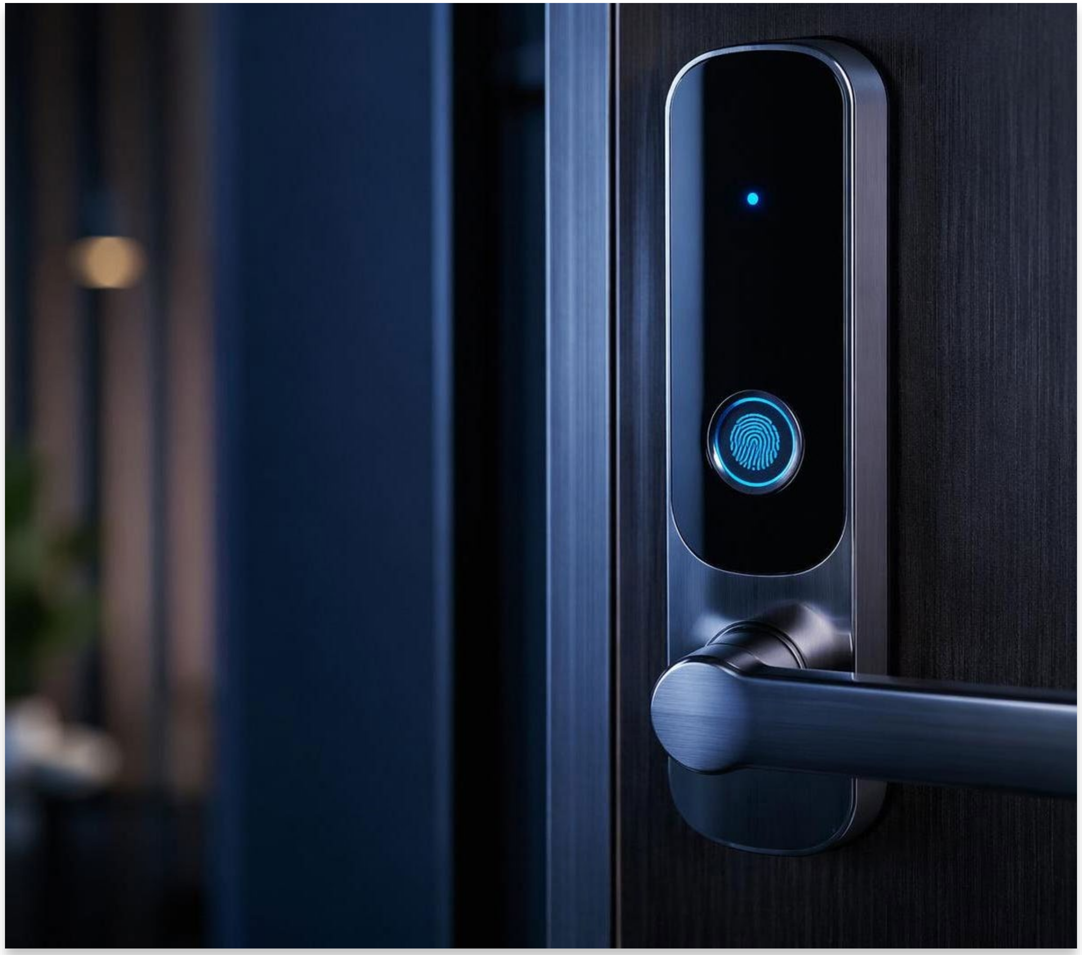
Passwords and Access Control

Password best practices:

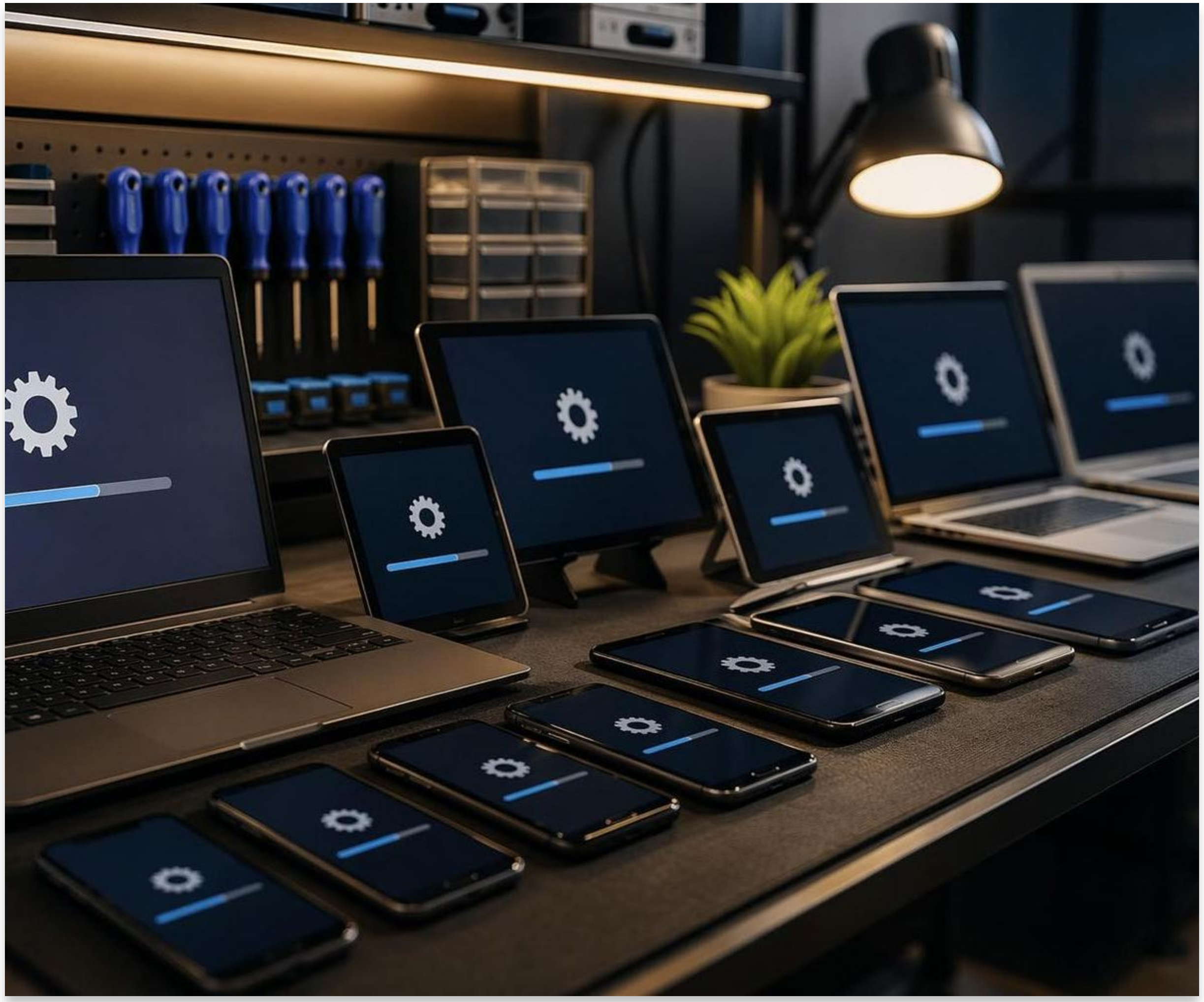
- Use a password manager for unique, complex passwords
- Never reuse passwords across platforms
- Change passwords immediately if a breach is suspected

Access control:

- Limit user access to only what each person needs
- Use separate admin and everyday accounts
- Review and remove access when staff leave
- Disable unused accounts promptly



Patch and Update Everything



Keep everything up to date:

- Operating systems (Windows, macOS)
- Web browsers and email applications
- Accounting and business software
- Security and antivirus tools
- Routers, firewalls, and network devices

In Plain English:

Updates fix known security holes. Delaying patches gives attackers an open door.

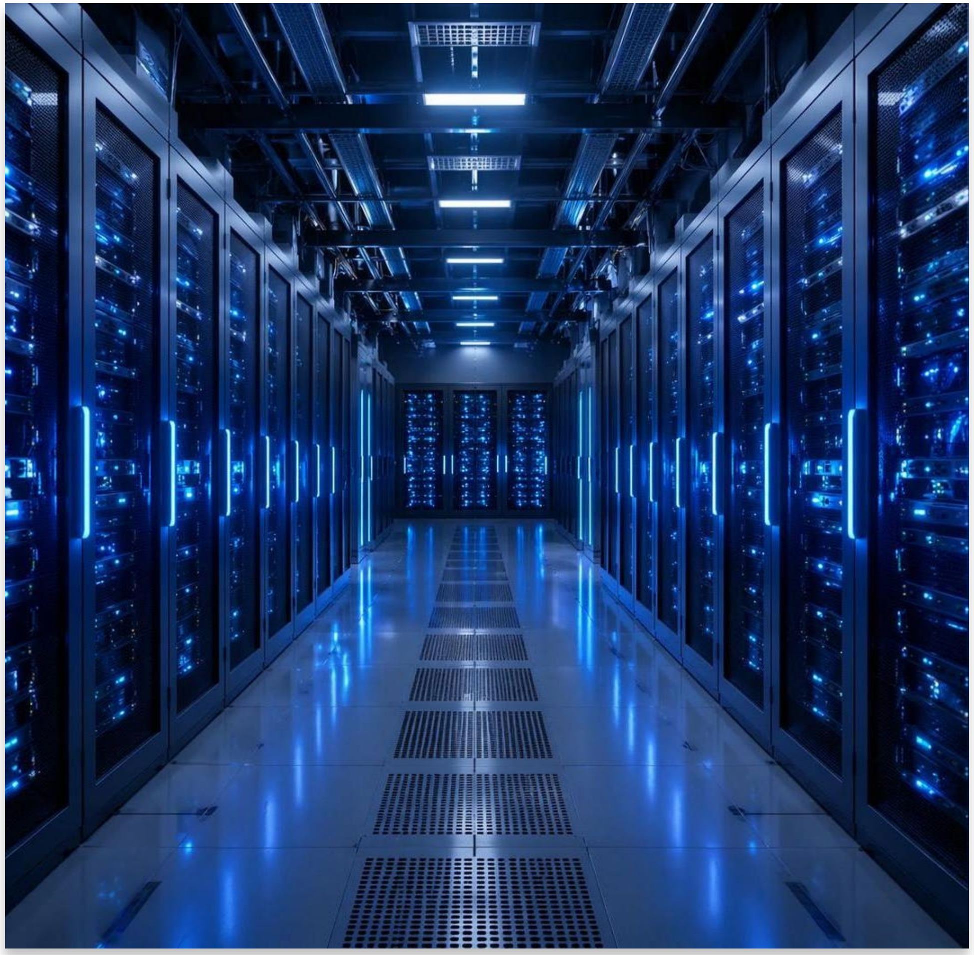
Backup Strategy

The 3-2-1 backup rule:

- 3 copies of your data
- 2 different storage types
- 1 copy stored offsite or in the cloud

Best practices:

- Automate backups, do not rely on manual processes
- Test restoration regularly
- Ensure backups cannot be deleted by ransomware
- Include client data, applications, and settings



Staff Awareness and Incident Response

Build a security culture:

- Train staff to recognise phishing emails
- Verify payment and bank detail changes verbally
- Question emails that feel urgent or unusual
- Report suspicious activity immediately

Have an incident response plan:

- Know who to contact if something goes wrong
- Document steps to contain and recover from a breach
- Understand your notification obligations under the NDB scheme

Your Cyber Security Checklist

- ✓ Enable MFA on all accounts and systems
- ✓ Use a password manager with unique passwords
- ✓ Keep all software and devices updated
- ✓ Back up data securely and test restoration
- ✓ Train staff to recognise phishing and scams
- ✓ Restrict access based on roles
- ✓ Have an incident response plan
- ✓ Review your cyber security posture regularly

Start with what you can do today. Every improvement counts.

Harvey Norman Technology for Business

About Harvey Norman Technology for Business

Your Business IT and Cyber Security Partner

- Enterprise-grade IT solutions at small business prices
- 24/7/365 cyber security monitoring and response
- Dedicated team of certified security experts
- Over 30 years supporting Australian small businesses
- Proactive management to reduce risk and downtime

Let Harvey Norman Technology for Business be your IT department.

Services and Solutions

What we provide:

- **Cyber Security**
  24/7 monitoring, threat detection and response, layered security framework
- **Business IT Support**
  Help desk support, proactive management, device and network administration
- **Backup and Recovery**
  Automated cloud backup, disaster recovery, regular restoration testing
- **Compliance Support**
  Essential Eight alignment, security training, phishing simulations

Packages and Pricing

Affordable packages for every business:

- **Foundation**
  Managed IT environment with baseline protection
- **Essentials**
  24/7 monitoring, backup and recovery, help desk
- **Standard**
  Extra security layers, staff training, phishing testing
- **Premium**
  Stringent security standards for financial and regulated sectors

Free Cyber Security Risk Assessment

Find out where you stand:

- Comprehensive review of your current security posture
- Identification of vulnerabilities and risk areas
- Practical recommendations tailored to your practice
- No obligation, no cost

Book your free assessment:

harveynormanbusiness.com.au

1300 781 865

harveynormanbusiness.com.au/pages/ifpa

Key Takeaways

1. Advisers are a prime target – your access and data make you valuable to attackers
2. Cloud convenience comes with shared security responsibility
3. Compliance expectations are rising. The TPB now requires cyber security measures
4. The Essential Eight provides a clear, practical framework
5. Start with MFA, passwords, patching, and backups
6. You do not have to do this alone, partner with experts

Dedicated Resources

- Latest insight articles on cyber security, best practices, compliance and more.
- Watch past webinars
- Helpful guides and resources.

https://www.harveynormanbusiness.com.au/pages/ifa

Other Resources

Harvey Norman Technology for Business

harveynormanbusiness.com.au

Australian Cyber Security Centre

cyber.gov.au

Cyber Wardens

cyberwardens.com.au

Office of the Australian Information Commissioner

oaic.gov.au

Small Business Cyber Resilience Service

business.gov.au/expertise-and-advice/small-business-cyber-resilience-service

Questions and Answers

Thank You

For more information, visit **harveynormanbusiness.com.au**