# Beyond the Basics of Cyber Security for Financial Professionals

Presented by Rutland Smith, May 2026

INSTITUTE OF FINANCIAL PROFESSIONALS AUSTRALIA

Harvey Norman
TECHNOLOGY FOR BUSINESS

Making Enterprise-Grade IT Solutions Affordable For Small Business

# Cyber Security is a Business Risk

Cyber security protects:

- Your revenue
- Your reputation
- Your clients
- Your operational continuity

It is a strategic investment, not an expense.

Cyber security is a business risk, not just an IT issue

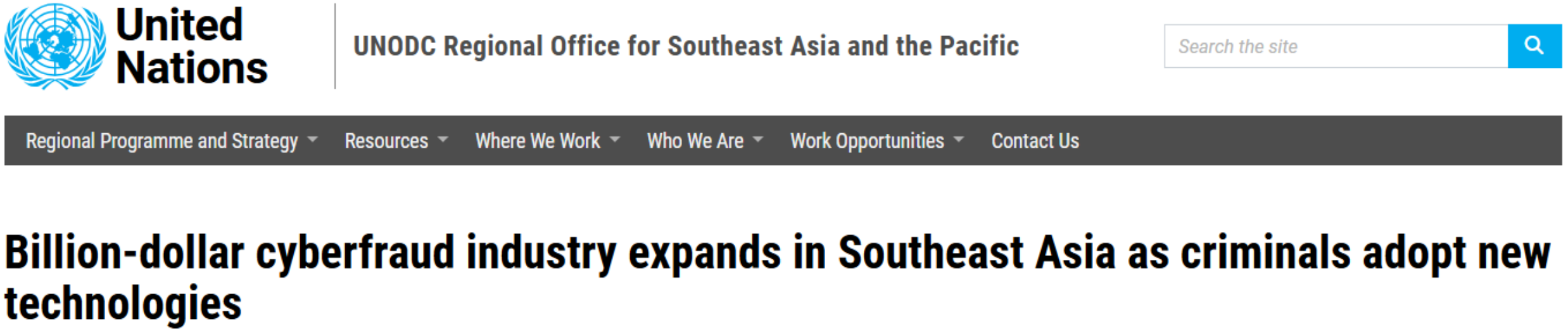
# Not IF But WHEN

> “Cyber Attacks Are Inevitable – So Stop Preparing For IF One Happens and Start Preparing For When One Will.”

Entrepreneur

*Written by Rakesh Soni, 26 July, 2024*
*Entrepreneur Media, LLC*

# Cyber Criminals are Sophisticated



# Compliance and Legal Obligations

# Obligations | **Financial Services**

- Australian Privacy Act 1988 (Cth)
- Corporations Act 2001 (Cth)
- ASIC Cybersecurity Expectations
- ASIC Regulatory Guide
- Cyber Security Act 2024
- APRA CPS 234 (where applicable)
- Industry Codes of Conduct
- Notifiable Data Breaches Scheme (Privacy Act Amendment)

# The industry is buzzing


## Multimillion-dollar FIIG penalty a 'clear warning to all financial organisations', expert says

## Australian company fined $2.5 million for cyber failures

First-ever penalties after 'thousands' put at risk.

By Leonard Bernardone on Feb 10 2026 01:30 PM

Home › News › Technology › Security

## FIIG penalised $2.5m for cyber security failures

# ASIC Open Letter

"Too often cyber-attacks are successful because known vulnerabilities are exploited. ASIC's expects regulated entities to actively prepare for cyber incidents, respond promptly and effectively when they occur, and recover in a way that restores critical services, minimises harm, and strengthens future resilience"

# ASIC Open Letter

“We encourage you to take the following steps now:

- Reassess your cyber plans and refocus efforts on the most critical risks
- Confirm your cyber risk, governance and overall risk and decision-making frameworks, consider the cumulative impact of interrelated vulnerabilities, and facilitate clear decision-making and escalation at the pace necessary to manage risk.
- Identify and protect critical assets and systems, with a clear understanding of what matters most to your business and customers.
- Strengthen cyber security fundamentals by regularly reviewing and validating core controls.
- Minimise attack surfaces by reducing exposure of systems and services to untrusted networks.
- Regularly review user access and reassess privileges, to protect against unauthorised access. Insider threats are increasing and entities should monitor for warning signs and act to restrict access where concerns are identified. “

# ASIC Open Letter

- “Patch systems promptly, recognising that AI is accelerating vulnerability, discovery, and exploitation.
- Review and strengthen patch management processes, considering challenges daily patching may present to identification, testing, and governance of critical updates.
- Implement layered, defence-in-depth architectures that assume breach and restrict lateral movement.
- Prepare for incident response by maintaining and exercising incident response plans and playbooks including business continuity plans and identification of highest priority services, channels and platforms.
- Actively manage third-party risks, particularly where services introduce concentration or systemic exposure.
- Use AI for defensive purposes, where appropriate, including identifying vulnerabilities and securing software before release. ”

# The Essential Eight – Risk Mitigation Framework

| Strategy | What It Means | Why It Matters |
|---|---|---|
| **Application Control** | Only allow approved apps and programs to run on your systems. | Stops malware from running in the first place. |
| **Patch Applications** | Regularly update your software (e.g. browsers, Microsoft Office, PDF readers). | Fixes security holes that hackers can exploit. |
| **Configure Microsoft Office Macro Settings** | Blocks risky macros from running in documents. | Macros are a common way for viruses to get in. |
| **User Application Hardening** | Disable unnecessary features in apps (like Flash, ads, and Java). | Reduces the number of ways hackers get in. |
| **Restrict Admin Privileges** | Only IT/admin staff should have full access to systems. Regular users get only what they need. | Limits damage if someone's account is hacked. |
| **Patch Operating Systems** | Keep Windows, macOS, or other operating systems updated. | Prevents known security flaws from being used against you. |
| **Multi-Factor Authentication** | Requires users to enter a second code (e.g. from an app or via SMS) when logging in. | Makes it much harder for hackers to break into accounts. |
| **Regular Backups** | Automatically backup data and test restoring it. | Essential if hit by ransomware. |

# Recognising and Responding to Cyber Security Red Flags

# Identifying Suspicious Emails and Phishing Attempts

**Recognise Phishing Emails**

Phishing emails imitate trusted contacts to trick users into revealing sensitive information or installing malware.

**Check Sender Addresses**

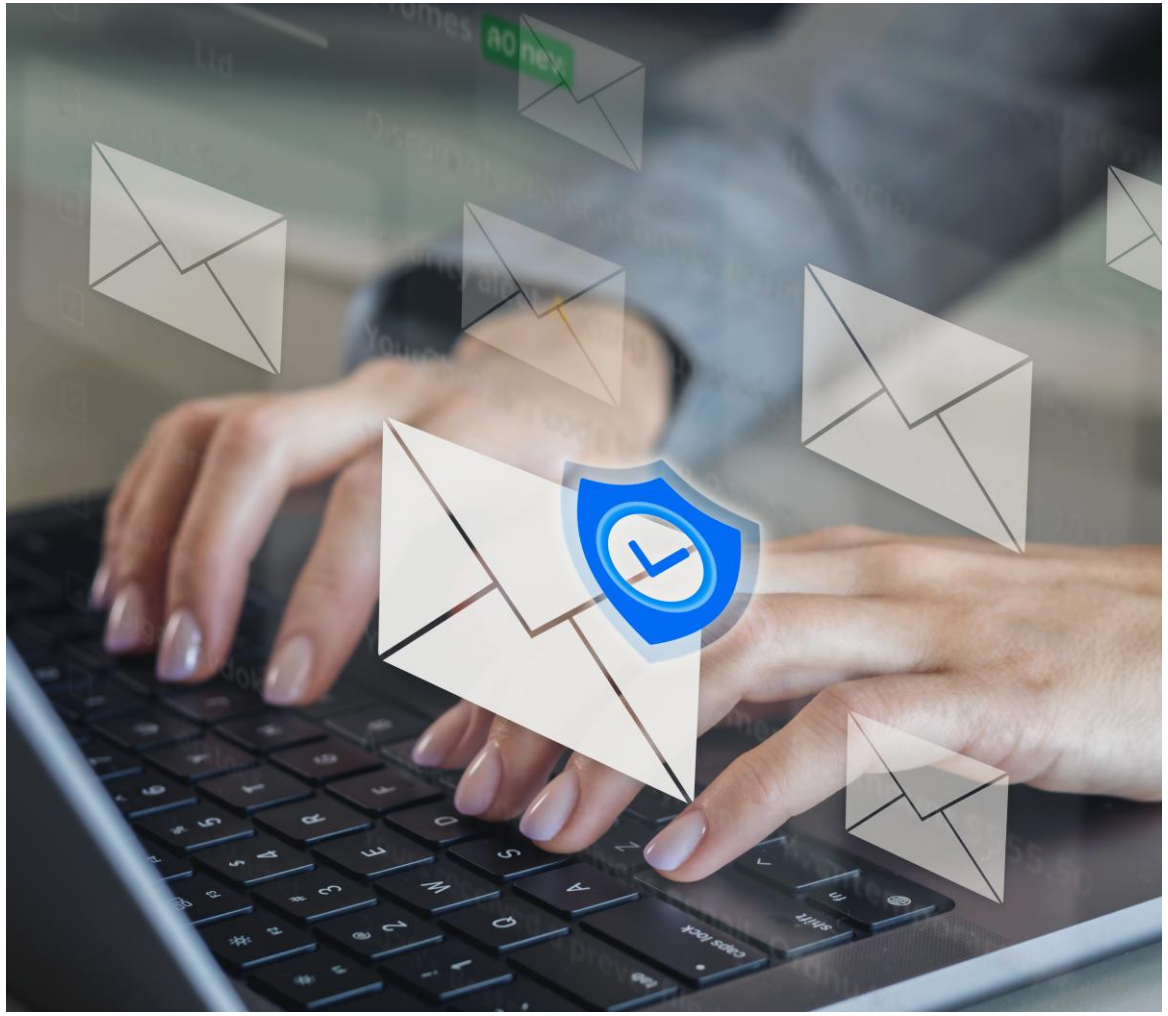
Unusual or slightly altered sender addresses can indicate fraudulent emails posing as trusted sources.

**Identify Urgent Requests**

Phishing emails often create urgency to pressure recipients into immediate action without verification.

**Beware Suspicious Links**

Links or attachments in phishing emails may be malicious and should be checked carefully before clicking.



# Recognising Client Interactions and Social Engineering

**Impersonation Risks**

Cybercriminals often impersonate clients or colleagues to steal sensitive information.

**Verify Identities**

Always confirm identities before sharing sensitive or financial information.

**Cautious with Requests**

Be cautious of unexpected, unusual or urgent requests, especially involving financial transactions.

# Advanced Email Filtering

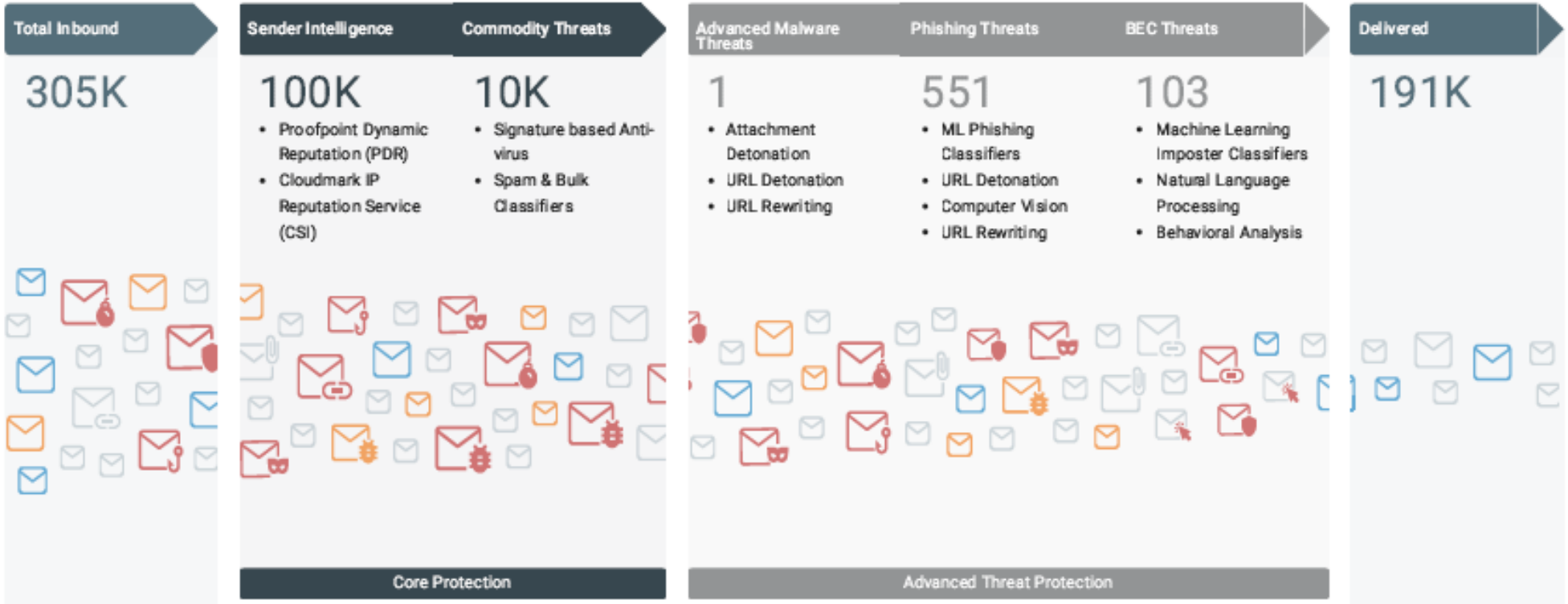
- Improves detection of phishing and spam emails significantly.
- Machine learning algorithms adapt to new threats for enhanced security.
- Email filtering reduces the risk of malware and ransomware infections.
- Filters minimise false positives while increasing threat detection accuracy.
- Integration with other security tools enhances overall cyber defence.
- Regular updates ensure filters stay effective against evolving attack methods.

# Effectiveness of Advanced Email Filtering

## Inbound Email Protection Breakdown: **All Customers**

The **All Customers Inbound Email Protection Report** provides a summary of the different types of malicious inbound emails sent to your customers that were blocked by Proofpoint.

Report generated: 5/1/2026




**110K Threats Blocked**

**655 Threats Blocked**

Message counts for **Advanced Malware, Phishing and BEC Threats** are aggregated across all your customers

# Access Control & Privilege Management

- Remove unnecessary admin access
- Disable dormant accounts
- Restrict data access by role
- Secure remote access properly

Least privilege = reduced risk.

# Device Management and System Security

# Best Practices for Securing Laptops and Desktop Computers

**Use Updated Antivirus Software**

Keep antivirus software updated to protect devices from malware and security threats effectively.

**Enable Firewalls**

Activate firewalls to monitor and block unauthorised network access, enhancing device security.

**Maintain Strong Passphrasess**

Use strong, unique passphrases to prevent unauthorised access to devices and accounts.

**Install Software Updates**

Regularly update software to patch vulnerabilities and improve security features.

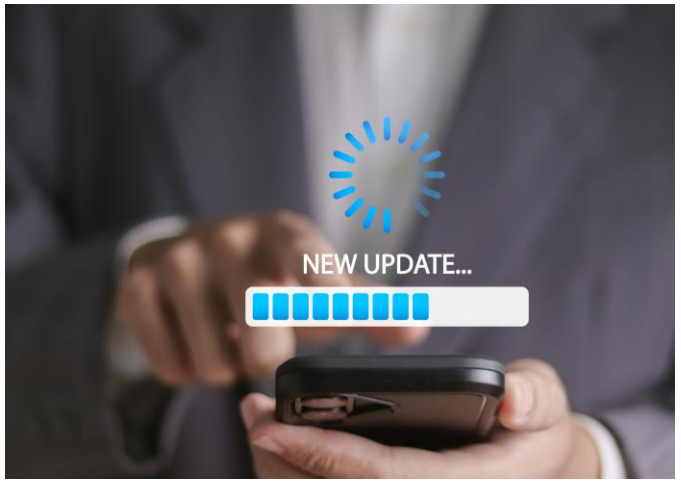
# Best Practices for Securing Laptops and Desktop Computers


- Restricted administrative privileges
- Multi Factor Authentication.
- Proven backup and recovery process and tools
- Compliance with encryption standards is essential.
- Application Control
- Restrict Microsoft Macros
- Locked down security policies

# Protecting Mobile Phones and Tablets

**Device Security Features**
Use screen locks, encryption, and remote wipe to secure mobile devices against unauthorised access and data loss.

**Public Wi-Fi Risks**
Avoid using public Wi-Fi networks for sensitive tasks to prevent data interception and cyber attacks.




**Keep Software Updated**
Regularly update operating systems and apps to patch security vulnerabilities and enhance protection.

# Incident Response: What to Do in the Event of a Breach

# Step-by-Step Breach Response Procedures

**System Isolation**

Quickly isolate affected systems to prevent further spread of the security breach and limit damage.

**Scope Assessment**

Evaluate the extent and impact of the breach to understand affected data and systems.

**Evidence Preservation**

Secure and preserve all evidence to support forensic investigation and legal processes.

**Recovery Protocols**

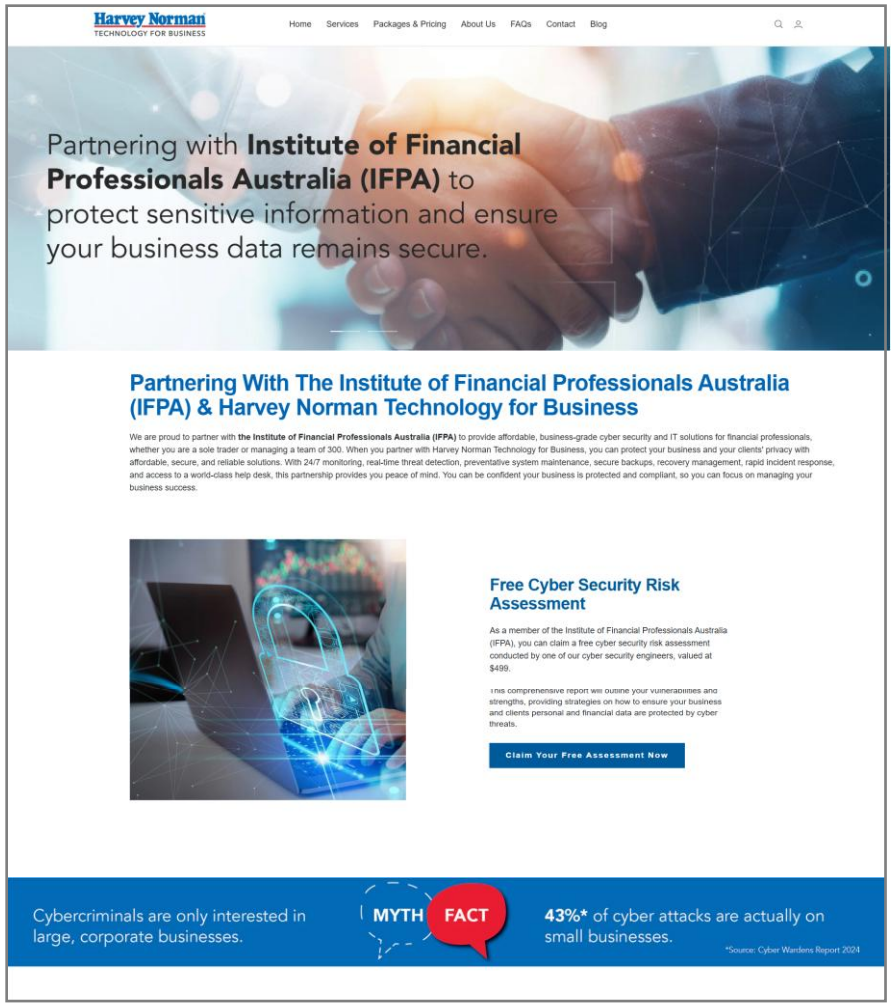
Initiate recovery steps to remediate the breach and restore affected systems to normal operation.

# Incident Response Plans: Legal Necessity and Practical Essential

- Incident response planning is mandated by various cybersecurity regulations and standards.
- A well-structured plan enables quick, coordinated actions during security breaches.
- Legal obligations require timely breach notifications and evidence preservation.
- Effective response plans minimize damage and reduce financial and reputational losses.
- Incident response plans ensure compliance and demonstrate due diligence to regulators.

# About Harvey Norman Technology for Business

# Dedicated Resources




- Latest insight articles on cyber security, best practices, compliance and more.
- Helpful guides and resources.
- Book your free cyber security risk assessment.

**https://www.harveynormanbusiness.com.au/pages/ifpa**

# Free Cyber Security Risk Assessment

## CURRENT COMPLIANCE SCORE (SCALE OF 5)

### OVERALL COMPLIANCE SCORE - 2.92

| MITIGATION STRATEGY | SCORE | IS COMPLIANT |
|---|---|---|
| Patch Applications | 3.18 | No |
| Patch OS | 3.48 | No |
| Multi-Factor Authentication | 5.00 | Yes |
| Restrict Admin Privileges | 5.00 | Yes |
| Application Control | 0.00 | No |
| Restrict MS Macros | 0.00 | No |
| User Application Hardening | 0.00 | No |
| Regular Backups | 5.00 | Yes |

## RECOMMENDED FIXES FOR FAILED CONTROLS

| SEVERITY | FIX RECOMMENDATION |
|---|---|
| CRITICAL | 1. Scan internet-facing device OS daily |
| CRITICAL | 2. Replace all OS for which support is not available |
| CRITICAL | 3. Security incidents must be reported to CISO and forwarded to ASD as soon as possible |
| HIGH | 4. Use an automated vulnerability scanner |
| HIGH | 5. Scan online services daily |
| HIGH | 6. Apply Application Control to ProfileTemp and Windows folders |
| HIGH | 7. Security incident response plan must be implemented immediately when an incident is recognized |
| HIGH | 8. Enable / Install Windows Defender Application Control on all workstations |
| HIGH | 9. Enable Application control on all internet facing devices |
| MEDIUM | 10. Remove online/email/browser/PDF applications for which support is not available |
| MEDIUM | 11. Use an automated asset discovery process |
| MEDIUM | 12. Application Control events must be centrally logged |
| MEDIUM | 13. Security/Event logs should be analyzed on a timely basis to identify suspicious activity |
| MEDIUM | 14. Apply Microsoft recommended application blocklist |
| MEDIUM | 15. Restrict creation/execution of executables to only approved set |

# In Summary

| | |
|---|---|
| **Recognising Cyber Threats** | Identifying cyber threats is crucial for preventing attacks and safeguarding sensitive client information. |
| **Securing Devices** | Implementing strong security measures on devices ensures protection from unauthorised access and malware. |
| **Effective Incident Response** | Responding promptly and effectively to security incidents minimises damage and restores system integrity. |
| **Understanding Compliance** | Awareness of compliance requirements helps maintain legal standards and protects client data privacy. |

# Thank You

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

Harvey Norman®
TECHNOLOGY FOR BUSINESS

Making Enterprise-Grade IT Solutions Affordable For Small Business