PRIORITY networking

Accountant's Cyber Security Checklist

2023-24

A self-guided self-assessment checklist for accountants

Greg Gardiner
Co-Founder
Priority Networking

greg.gardiner@pnet.com.au
1300 718 076

Cyber security and cyber resilience are some of the most pressing challenges faced by accounting practices.

By the nature of the information accountants hold and manage, accounting practices are a prime target for cyber attack.

Accountants in public practice must satisfy cyber security requirements across multiple statutory and professional requirements. Practices must take "reasonable steps to protect client data they hold." But, what does that mean and how do you ensure that your practice has done exactly that?

Priority Networking has worked with numerous accounting practices over the last decade to secure their data, meet (or exceed) compliance requirements and, quite frankly, help their management teams sleep better at night.

That's why we've created this guide. It will help you understand what is required to create a compliant cyber security strategy that offers a comfortable balance between protection, flexibility, and cost-effectiveness.

The first part of this guide explores the requirements of the most common statutory requirements, helping you understand what you need to do to achieve compliance.

The second part of this guide is a checklist that explores cyber security strategies and tactics, that, when implemented, help you satisfy these compliance requirements.

Here's how to use this checklist:

1. **Give yourself an honest score for each item.**
   You get a score of "1" if you are currently implementing the item, and a score of "0" if you're not. Then, tally up your score at the bottom of each page.
2. **Total your scores and assess your performance.**
   This will give you a concrete idea of your strengths and areas that require improvement.

I hope this guide creates a more secure future for your practice. If you need support to identify and implement your practice's cyber security and cyber resilience strategy, contact a Priority Networking specialist on 1300 718 076 or email support@pnet.com.au.

Welcome to your journey towards better cyber security.

Best wishes,

Greg

Greg Gardiner

Accounting Practice Cyber Security Requirements

"How do I know my accounting practice's cyber security and cyber resilience measures meet the minimum statutory requirements?"

Part 1

1. Cyber Security Requirements of the Privacy Act

There is a common misconception that small accounting practices with an annual turnover under $3m are exempt from the Privacy Act 1988 ("Privacy Act"). This is incorrect.

If your accounting practice handles client Tax File Numbers (TFNs), you must comply with Privacy Act requirements, regardless of your annual turnover.

What does the Privacy Act require?

The Australian Privacy Principle 11 requires your practice to "take such steps as are reasonable in the circumstances to protect the information:

- from misuse, interference and loss; and
- from unauthorised access, modification or disclosure."

And, the Privacy (Tax File Number) Rule 2015 imposes a higher level of obligation on practices handling TFNs. Under the TFN Rule, you must safeguard TFNs from loss, unauthorised access, use, modification, disclosure or other misuse. This means appropriately managing, documenting, reviewing and updating your practice's TFN management practices and protecting them against risk.

What are the data breach requirements?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. A data breach occurs when, "personal information that an entity holds is subject to unauthorised access or disclosure, or is lost." Examples include:

- Loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- Unauthorised access to personal information by an employee
- Inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- Disclosure of an individual's personal information to a scammer, because of inadequate identity verification procedures.

Assuming your practice can identify if a data breach has occurred, and this is questionable for many, the question is whether the breach is reportable under the notifiable data breach scheme. A reportable breach is one that, on assessment, is likely to result in serious harm.

How do I implement cyber security measures that satisfy these requirements?

It's impossible to reduce cyber security risk to zero but your practice can reduce the risk to acceptable levels.

See Part 2 of this guide where we explain 20 strategies and tactics you can implement to improve your accounting practice's cyber security and satisfy your statutory and ethical requirements.

Need support?

Do you need help identifying and implementing your practice's cyber security policies and procedures? Contact a Priority Networking specialist on 1300 718 076 or email support@pnet.com.au.

2. Cyber Security Requirements for Tax Agents

The obligations of Tax Agents go further than protecting personal information. Tax Agents have a professional and ethical obligation to take reasonable steps to protect the client data they hold.

The statutory obligations derive from the:

- Tax Agents Services Act 2009, particularly Code 6 of the Code of Professional Conduct
- The Privacy Act 1988
- The Privacy (Tax File Number) Rule 2015, and
- Tax Administration Act 1953

The Tax Practitioners Board provides some practical guidance on these obligations:

- TPB(PN) 4/2021 Use and disclosure of a client's TFN and TFN information in email communications
- TPB(PN) 3/2019 Letters of engagement
- TPB(PN) 1/2017 Cloud computing and the Code of Professional Conduct
- TPB(PN) 2/2018 Outsourcing and offshoring of tax services - Code of Professional Conduct considerations
- TPB(PN) 5/2022 Proof of identity requirements for client verification
- TPB(EP) 03/2010 Professional indemnity insurance requirements for tax and BAS agents

From a cyber security perspective, you must ensure that:

- You take reasonable steps to protect the data of individuals held by your practice; and
- If a breach occurs, your practice must be able to limit the risk and respond to the breach.
- If the breach is significant, adhere to the requirements of the

How do I implement cyber security measures that satisfy these requirements?

It's impossible to reduce cyber security risk to zero but your practice can reduce the risk to acceptable levels.

See Part 2 of this guide where we explain 20 strategies and tactics you can implement to improve your accounting practice's cyber security and satisfy your statutory and ethical requirements.

Need support?

Do you need help identifying and implementing your practice's cyber security policies and procedures? Contact a Priority Networking specialist on 1300 718 076 or email support@pnet.com.au.

3. Cyber Security Requirements for Financial Advice Practices

Accounting practices that offer financial services have an additional layer of obligation imposed by the conditions of your Australian financial services licence (AFSL) and by extension, its authorised representatives.

By its nature, the provision of financial advice and the data and information managed on behalf of clients, carries with it a higher level of risk. This data is often very valuable to cyber criminals.

Financial services providers are required to reduce cyber security risk to an acceptable level through adequate cyber security systems, documentation, and controls.

Section 912A(1)(a) of the Corporations Act 2001 requires an AFSL to "do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly". Failing to ensure that adequate cyber security measures are in place, the measures are adequately implemented, and implemented in a way that enables an efficient response, is a failure of this requirement.

Section 912A(1)(d) requires an AFSL to ensure that its "representatives are adequately trained", and section 912A(1)(h) requires an AFSL to "have adequate risk management systems" in place.

How do I implement cyber security measures that satisfy these requirements?

It's impossible to reduce cyber security risk to zero but your practice can reduce the risk to acceptable levels.

See Part 2 of this guide where we explain 20 strategies and tactics you can implement to improve your accounting practice's cyber security and satisfy your statutory and ethical requirements.

Need support?

Do you need help identifying and implementing your practice's cyber security policies and procedures? Contact a Priority Networking specialist on 1300 718 076 or email support@pnet.com.au.

Accounting Practice Cyber Security & Resilience Implementation

"What policies, strategies, and tools should I implement if I want to improve my practice's cyber security and meet statutory requirements?"

Part 2

#	Question	Solution	Add to your score
1	**Asset management register (both physical and digital)** Record one point for each of the following security controls: • You have an active register of data assets, such as client data systems • You conduct regular audits and updates of asset registers • You restrict access to authorised assets only, including management of Bring Your Own Device (BYOD) policies • You use automated discovery tools to track new assets (to avoid human error)	An 'asset management register' helps you understand exactly what digital and physical assets you own (and must protect from cyber incidents). It gives you the ability to systematically assess the health and protection layers for those assets. This layer of protection is likely to include third party tools, to both track and manage assets.	**+4**
2	**Software management and inventory register** Record one point for each of the following software maintenance controls: • You maintain a software register • You restrict software installation, and use authorised software only • Your software is currently supported by its vendor • Your software maintenance controls extend to web based apps accessible via browsers • Your software is patched monthly as a minimum • You have support/license update agreements in place and accessible • You have enabled the automatic discovery of newly installed software	A 'software management and inventory register' is similar to an asset management register. It helps you keep your software up to date. This strategy is important because hackers take advantage of commonly known software vulnerabilities within hours of them being released. Therefore, knowing what software you have, and what you must do to keep it up to date (and therefore as secure as possible), is a key security principle. Third party tools and platforms such as Microsoft 365 automate and centrally manage these controls.	**+7**
3	**Technical controls to maintain and restrict access to supported and authorised software** Record one point for each of the following technical controls: • Your application whitelisting is centrally managed from Microsoft's management platform • Admin privileges are restricted on local workstations • You prevent unknown scripts and executable files from being used on workstations • Your technical controls are reviewed bi-annually or more frequently	Technical controls help you secure access to your software. For example, if staff are tricked into clicking on malicious links that have made it through your spam filters, technical controls significantly reduce the risk of malware being installed. Over the last 24 months, the government has published these technical controls as the standard for Australian businesses. They can be set up as automatic policies via Microsoft 365 and will need to be reviewed and maintained on a regular basis by qualified IT personnel.	**+4**
		Enter your score for this page here:	

#	Question	Solution	Add to your score
4	**Establish and maintain data management processes and policies** Record one point for each of the following data management controls: • Your data access control is regularly reviewed and staff only have access to what they require • You use classification labels such as Microsoft sensitivity labels to encrypt and protect data • You have a data retention policy that includes the removal of client data no longer required • You conduct network based scanning via appliance and/or firewalls for the use of file share sites	Data management processes and policies help you control and monitor access to your accounting practice's sensitive data. With an increasing number of privacy breaches, the government has enacted legislation making data management and protection a central tenet of company and director duties. Microsoft's data classification labels, along with Data Loss Protection policies are useful for accountants. They alert you to a potential data breach, and prevent third parties from reading data that has accidentally been sent by staff in error. Mail filtering programs such as Avanan have also introduced similar reporting to identify potential data loss (leaks).	**+4**
5	**Encryption technologies across multiple layers** Record one point for each of the following use of encryption technologies across multiple layers: • You use encryption on all workstations (i.e. Windows BitLocker, Apple FileVault) • Classification labels are used on Microsoft and PDF documents • Password protection of sensitive documents is a standard process within your practice • Removable media i.e. USB drives are encrypted, or you restrict the use of USB Drives • You ensure backups of data are encrypted, and mandate the use of immutable technologies (i.e. is stored in a read only state)	Encryption technologies make your data unreadable to anyone, unless they have a "key" or similar password/access credentials. Encryption works at multiple levels for various scenarios. For example, Microsoft BitLocker can be set up to automatically encrypt laptop hard drives. This means that if a hard drive is lost or stolen, it is extremely difficult for a third party to read its data without the keys and/or password. The encryption of PDF files and other documents is also important, alongside the use of classification labels. When a mailbox is compromised, it is extremely common for there to be a search for all emails with attachments looking for personal information.	**+5**
6	**Screen saver and lock screen deployment** Record three points if all devices (including BYOD) are locked within a maximum of 15 minutes. Mobile devices should lock in less than 2 minutes.	Screen savers and screen locking is a long standing principle that protects against: • external threats when remote controlling devices; and • internal threats and breach of systems, or the disclosure of confidential information between staff For example, given the opportunity, hackers may be able to 'remote control' devices after hours in order to access sensitive systems. Or, internal staff may be able to access confidential information via their colleagues' unlocked devices, when they are away from their desk. Microsoft and other systems can deploy automated policies to force the activation of screen savers.	**+3**

Enter your score for this page here: ☐

#	Question	Solution	Add to your score
7	**Firewalls across multiple levels** Record three points if: • Managed firewalls are deployed at multiple levels including physical office-based network perimeters, servers and workstations; and • Your firewalls include controls/technologies such as Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)	Firewalls prevent unauthorised traffic (e.g. hackers and other cyber adversaries) from accessing your networks and data. Firewalls are highly recommended as they prevent and detect malicious activity, particularly when hackers can be hiding inside a system for months before they attack. When staff work from home, the effectiveness of firewalls can also be reduced. Firewalls with IPS/IDS are cost effective and a useful security layer to alert of potential threats. Fortinet FortiGate solutions are a good balance between cost and highly-rated security features.	**+3**
8	**Practice wide password management** Record one point for each of the following controls: • You use a password manager • You conduct corporate administration and monitoring of potentially breached passwords, and the use of weak passwords by staff • You enforce the minimal use of shared passwords but where shared passwords are used these are managed via a password manager (definitely no spreadsheets of passwords or formulated passwords such as Name, Month, Year.)	Password management involves the use of complex, unguessable passwords (from 20-40 characters in length) and password management platforms. With the development of computer processing power and AI technologies, hackers are finding it easier to guess passwords. Therefore, password management is important. Additionally, compromised passwords are readily available on the internet. Password management also ensures that your staff don't re-use a password that may be compromised. Keeper, Dash lane, Last Pass and Bitwarden are preferred password managers. These platforms include corporate controls that monitor the strength and potential compromised passwords of your staff.	**+3**
9	**User account management** Record one point for regular review and maintenance of each of the following user account management controls: • You regularly review administrator privileges including separate administrator accounts across all systems • You regularly review inactive accounts and remove accounts no longer being used • You centralise accounts where possible i.e., Single Sign On with systems such as Microsoft or Google (this maintains user accounts in one place where possible)	User account management ensures that your staff have the correct amount of access to certain systems and data. User account management utilises the principle of 'least privilege', which ensures that only the minimum level of access and authorisation is granted. In simple terms, staff should access data on a 'need to have' basis. Also, it's advisable not to use 'full administrator access' accounts as your daily-use accounts. If a staff member is compromised, the least privilege principle reduces the risk of all data / systems being compromised. This leads to a quicker recovery of systems and data. While these are consulting and administration practices, Microsoft and other platforms are starting to provide reporting and auditing in these control areas.	**+3**

Enter your score for this page here:

#	Question	Solution	Add to your score
10	**Multi factor authentication (MFA)** Require and enforce MFA for all applications, network and administrator access. Record one point for each of the following controls: • MFA is enforced and monitored across all accounts • You use security keys (hardware tokens) and/or biometrics as additional layers of authentication • You use passwords/PIN numbers as primary authentication	Multi Factor Authentication (MFA) is a simple layer of protection that makes it harder for hackers to compromise a system using leaked or hacked passwords. However, there are different types of MFA, with different degrees of security. Text messages are considered insecure because, if mobile devices are compromised, text messages can be easily extracted. Additionally, staff can still be tricked into providing MFA tokens. Security keys such as 'Yubi' keys are growing in popularity as a third layer of protection. Keeper password manager or Microsoft Authenticator are also preferred as MFA tools because they hide the authentication token.	**+3**
11	**Management of software vulnerabilities** Record one point for each of the following software vulnerability management controls: • You have a documented process to manage software vulnerabilities, and it is reviewed regularly • Your operating systems are automatically patched monthly or on a more frequent basis • Your critical patches are applied within 48 hours • Vulnerability scanners and information databases are used to escalate deployment of critical patches Note: software ranges from Operating System, Office Suite, Browsers, PDF readers and Line of Business applications	The management of software vulnerabilities requires you to update software as soon as the latest patch becomes available. This is important because the time between when a patch is announced, and the time a hacker exploits it, can be within days (if not hours). It is increasingly important to patch critical vulnerabilities as soon as possible. It is common for service providers to enable automatic patching for critical updates and controlled updates at least monthly. Microsoft systems functionality, including central management and monitoring, is a valuable tool to configure and utilise. Other third party products are also available.	**+4**
12	**Anti-spoofing email tools** Record three points if you have these three key email anti-spoofing tools: • Sender Policy Framework (SPF), • DomainKeys Identified Mail (DKIM), and • DMARC reporting tools.	Anti-spoofing email tools prevent hackers from 'faking' emails from you or your staff. These tools apply a digital signature to emails that publish where your emails are being sent from. Reporting and management tools instruct receiving email servers on what to do with unverified emails i.e., nothing, quarantine, or reject. SPF is a base control and quick to check / implement. DKIM is a valuable control to monitor and reduce the spoofing of your emails. DMARC reporting of both SPF and DKIM is also recommended (which can be via email reports). Products such as PowerDMARC are also extremely effective for monitoring and governance of these controls.	**+3**

Enter your score for this page here:

#	Question	Solution	Add to your score
13	**Third party email anti-malware and virus protection** Record four points if you employ additional third party email protection systems including anti-malware/virus and phishing features.	Anti-malware and virus protection protects your systems from malicious code. Microsoft and Google filtering is certainly improving. However, having multiple layers of protection for phishing, malware, and spam are superior for both blocking and managing email based threats. Avanan is a highly rated system that we recommend. Higher marks for this control as these solutions offer a significant reduction in potential phishing or spear phishing emails.	**+4**
14	**Backup and recovery controls** Record two points each for the following backup and recovery controls: • You conduct daily automated backups and more frequent back-ups for sensitive data • Your backups are immutable (read only) and are stored separately from key systems • Your data recovery is tested on a regular basis - at a minimum annually, but monthly sample testing is recommended	Recovering lost data is the final defence against cyber attack, errors, or disgruntled staff. However, recovering lost data can be much more complex than it seems. If data is encrypted or modified, you need to be able to track the changes or recover deleted content. We recommend that you know how to recover quickly. We also recommend that you regularly test your data recovery process. Don't solely rely on Microsoft's limited undelete functions, if you have access to this service. Datto, Cove, and Acronis are useful backup and recovery tools.	**+6**
15	**Host-based intrusion prevention deployed** Record six points if you have deployed a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. For example, use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	Host-based intrusion prevention detects and deters hackers and other unwanted traffic. This feature used to be handled by legacy anti-virus solutions, however these are no longer effective. You may want to consider Endpoint Detection and Response (EDR) tools that also include Managed Detect Respond (MDR) and Extended Detection and Response (XDR). Speak to us for more information about this. Sentinel One, CrowdStrike, and Deep Instinct are highly recommended solutions.	**+6**
16	**Staff security awareness training** Record one point each for the following security awareness program controls: • You conduct email phishing exercises, to train staff to recognise social engineering attacks • You conduct general awareness training, at least every 6 months • You conduct training for key roles with access to sensitive data and/or systems, and role specific staff on control procedures for authentication and electronic fund transfer protocols • You conduct training on authentication best practices and password management • You have data encryption policies in place, to prevent the transfer of personal information in unencrypted emails	Staff security awareness training teaches your team about cyber security practices and principles. This strategy is important because human error causes more than 70% of successful cyber attacks. Cyber insurance companies and government cyber security agencies highly recommend robust security awareness training for staff. This includes a whole spectrum of training, from general through to role-specific, on a regular basis. This maintains awareness and keeps staff alert. We also recommend monthly email phishing campaigns as an effective tool for awareness but also to measure and identify staff who require additional training. Common solutions include Breach Now and KnowBe4.	**+5**

Enter your score for this page here:

#	Question	Solution	Add to your score
17	**Service provider management** Record one point each for the following service provider management policies: • Your service providers meet minimum security requirements i.e., via service agreements • You undertake regular assessment and attestation from service providers	You must also ensure that your service providers employ strong cyber security principles, too. This involves monitoring service providers and sending them regular assessments to complete. This ensures they are conducting appropriate levels of security. Larger businesses will be certified in both SOC2 and ISO 270001 standards, which says they have been independently audited and have a security management framework in place. There are a number of basic surveys similar to this checklist that can be sent to them on an annual basis at a minimum.	**+2**
18	**Standard security hardening configuration** Record four points if you monitor and maintain standard security hardening configurations from application providers. i.e., A Microsoft Security Score of 75% or greater is recommended.	Some application providers show you exactly how to implement cyber security measures for certain platforms and environments. For example, Microsoft publishes their recommended security baseline configuration for others to follow. Microsoft also has a 'Security Score' for overall security that requires regular maintenance and improvement. It focusses on the hardening of both new and existing features. The government's 'Essential 8' framework also references key measures to undertake.	**+4**
19	**Establish, maintain and train staff on your cyber incident response plan** Record one point for each of the following elements of your cyber incident plan: • You have planned and documented your cyber incident handling and reporting procedures (internally and to authorities), and trained your staff • You have documented the cyber response roles and responsibilities of your staff, and your staff have been trained • You have planned and documented the remediation, recovery and root cause analyses of security incidents • You are conducting regular routine testing of incident response processes	A cyber incident response plan tells you and your team what to do in the case of a breach or other cyber incident. Raising staff awareness of who to report the incidents to, both internally and externally, as well as testing the recovery of key systems, is critical. The process of documenting and educating staff with tabletop (mock) cyber recovery exercises will reduce the impact of a real cyber incident on your practice. Incident response plan templates such as the Victorian Government template are easy to adopt and free to download.	**+4**
		Enter your score for this page here:	

#	Question	Solution	Add to your score
20	**People controls** Record one point for each of the following people controls: • You use onboarding/offboarding checklists • You conduct background checks for all staff, including police, certifications and reference checks • You have 'acceptable use' and 'remote working' policies in place (that include security considerations)	Many cyber incidents originate from the actions of internal team members. You must implement people controls to ensure that your team acts with integrity. Active policies will limit these internal threats. This includes both deterrents to security breaches, as well as mandating security requirements (many of which are documented in this checklist).	**+3**

Enter your score for this page here:

Calculate your cyber score

Tally your score from the previous pages, and assess your cyber security score against the chart below.

Your score range:	*Your score range:*	*Your score range:*
0-65	**66-72**	**73-80**
VERY INSECURE	**HIGH RISK**	**OK**
Your cyber security requires immediate attention. You are at very high risk of a cyber breach.	Your cyber security requires urgent attention. You are at high risk of a cyber breach.	Your cyber security is OK. Maintain your current cyber security strategy but stay vigilant for evolving threats.

If you scored between 0 and 65 you are at very high risk of a cyber attack

A score within this range indicates that your cyber security measures are significantly below recommended levels. Your practice is at a high risk of cyber attack creating the potential for loss of client data, disruption to business continuity, reputational damage, and civil penalties.

Immediate action is recommended to enhance your cyber security. We suggest a 360 Degree Cyber Security Audit, which will provide a thorough assessment of your current cyber security infrastructure and create a plan for improvement.

If you scored between 66 and 72 you are at high risk of a cyber attack

If your score is between 70 and 75, your cyber security measures are not adequate enough to satisfactorily reduce your risk of cyber attack. Within this score range, a significant cyber attack is likely, potentially leading to loss of client data, disruption to business continuity, reputational damage, and civil penalties.

It is recommended that you act promptly to improve your cyber security. A 360 Degree Cyber Security Audit will help identify weaknesses in your existing cyber security strategy and provide insights for necessary enhancements.

If you scored between 73 and 80 your cyber security is OK

Congratulations! A score within this range is indicative of a strong cyber security strategy. However, given the constantly evolving nature of cyber security threats, continuous evaluation and improvement are crucial. Even though your cyber security measures are robust, it may be beneficial to periodically review your strategy. An objective analysis can offer new insights for optimisation, which can further enhance operational efficiency while maintaining a strong defence against cyber threats.

In all cases, remember, cyber security is an ongoing journey, not a destination. Constant vigilance and regular reviews are crucial to maintaining the integrity and security of your systems in the face of evolving threats.

Improve your resilience by undertaking a

360 Degree Cyber Security Audit

Some of the common questions we are asked about cyber threats to accounting practices:

- Does my accounting practice meet (at least) the minimum statutory requirements? If not, what do we need to do?
- Are there any other obligations I must meet, to "take reasonable steps to prevent client data from misuse?"
- I have staff working remotely, what do we need to do to protect against cyber attack?
- Do I need to move my on-premise servers to the cloud, and if so, what is the best cloud system for accounting?
- Do we have the right IT systems in place to handle leave/employee management, debtors management, etc?
- Are we compliant with the "Essential 8", and are we protected against evolving threats?
- Are my offshore resources as efficient as they could be, and is there AI and other technology available that might remove the need for offshoring?
- Am I currently overpaying for my accounting practice's cyber security?

If you would like answers to these important questions, request a 360 Degree Cyber Security Audit where you will:

- Learn more about **cyber security strategies designed specifically for accountants,** including the latest cyber security frameworks recommended by major industry authorities (Essential 8 m1, ISO 27001, MS Score)
- **Receive a report and action plan** showing you how your cyber security can be improved, without restricting your operational efficiency or growth trajectory
- **Finally be able to relax** knowing that you are (a) up to speed with standards and (b) protected against cyber threats. You can also demonstrate due diligence, too.

Please note, this is not a sales pitch in disguise. You will receive actionable information that you can take away and implement yourself. If you would like help implementing our strategies, we can speak about those, too.

Request your 360 Degree Cyber Security Audit by clicking here, while you're thinking about it, and before busy accounting life gets in the way.


PRIORITY
networking
Visit our website to learn more
Priority Networking | www.pnet.com.au