Cyber Security Self-Assessment Questionnaire

1				
Statement	Sometimes scammers can target you or your staff directly via email. These email addresses will look like legitimate business emails and contain vaguely specific details often containing clickable links within the email body.			
Question	Do you have a training program or process to train and educate your staff on how to identify such emails?	Yes	No	Unsure

2				
Statement	Regular backups of important data and systems is essential for minimizing downtime while maintaining customer confidence. Testing of recovery procedures is equally vital.			
Question	Does your business have complete backups regularly?	Yes	No	Unsure
Question	Does your business have recovery plans documented and tested?	Yes	No	Unsure

3				
Statement	Collecting and storing customer data securely is crucial to protecting customer privacy.			
Question	Do you request and retain any customer data for business purposes? (Customer names, addresses, mobile numbers, DOB)	Yes	No	Unsure
Question	Do you know where this information is stored?	Yes	No	Unsure

4				
Statement	Security software is vital for businesses to detect, prevent and respond to cyber threats.			
Question	Do you have security software for: • Devices/Servers	Yes	No	Unsure
	• Email	Yes	No	Unsure
	• Cloud	Yes	No	Unsure
	• Firewalls	Yes	No	Unsure

5				
Statement	Cyber criminals are known to exploit vulnerabilities in outdated software and systems, applying security patches reduces this risk significantly.			
Question	Do you regularly apply updates to critical software and systems required to run your business?	Yes	No	Unsure

6		
Statement	Cyber security incidents happen, and having adequate people, processes, and technology to detect these events is vital to business continuity.	
Question	Could you detect a cyber incident in your business?	Yes No Unsure
Question	Do you have a documented incident response plan or know what you would do if a cyber incident happened?	Yes No Unsure

7		
Statement	Multi Factor Authentication is the concept of something you know; like a password and something you have; like a token. It is crucial for enhanced second layer of security to protect against credential theft and unauthorised access.	
Question	Do you have multi factor authentication enabled for critical business applications?	Yes No Unsure

8		
Statement	Secured business connectivity is vital to protect data, prevent cyber incidents, safeguard intellectual property, and defend against cyber threats.	
Question	Have you secured your business Internet and WIFI / network connectivity?	Yes No Unsure

9		
Statement	Allowing non-business devices to connect to the business network could allow infection/malware into your business inadvertently.	
Question	Do you allow non business devices to connect to your business internet or WIFI?	Yes No Unsure

10		
Statement	Cybersecurity insurance is important because it offers financial protection for businesses in the event of a cyber attack or data breach, covering costs related to recovery, legal liabilities, customer notification, reputation management, and regulatory fines.	
Question	Do you have cyber security insurance in place?	Yes No Unsure

If you need more advice on cyber security for your business, please fill in the form on **one.nz/partner** and attach this self-assessment to book in a free security assessment.*

Your Name		
Company Name		
Company Address		
Contact Phone		
Contact Email		
Size of Company		
Type of Company		
Number of Mobile phone users		
Number of PC or Laptop users		
Are you a One NZ customer?	Yes	No

*One NZ will allocate your business a local IT Partner. Offer available to small to medium sized businesses up to 100 FTE. Free security assessment capped at four hours of allocated IT Partner's time with further hours billed to the customer by IT Partner. A quote will be provided prior to assessment commencing. Offer available to One NZ customers only. Business account owner authority may need to support the switch to services to One NZ. Only one offer available per business. Any additional products and ongoing support that may be required are not included.