Pre Assessment Information

cyberturity®

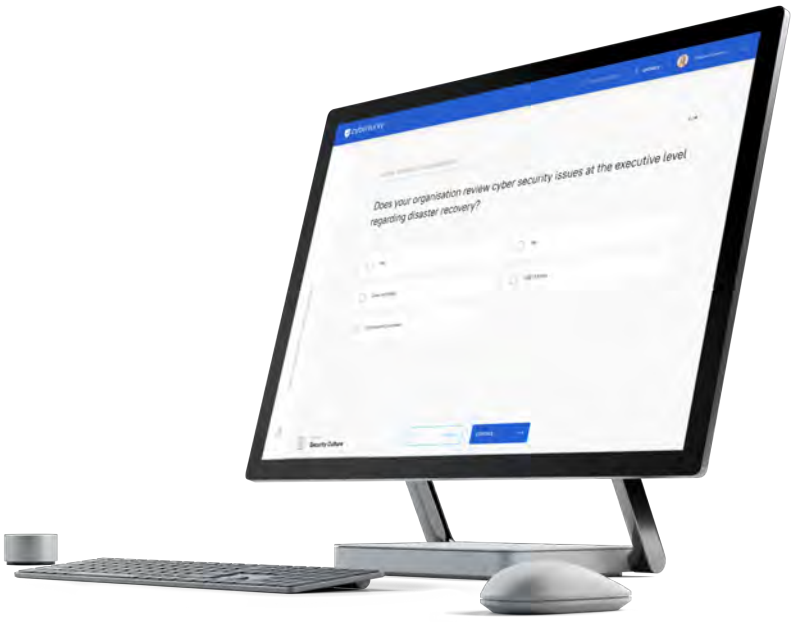
What is this all about?

In short, this is about helping you better understand and identify where you are strong and where you may have gaps in cyber securing your business.

Cyber risk management is a whole of business risk that has many parts to it. It's much more than having a firewall and antivirus installed, and it's not something your IT team or provider can solve on their own for you. Managing cyber risk involves every member of your business, the contractors you use as well as the partners you buy from and sell to.

Effective cyber risk management requires attention across multiple areas. One of the most common failures in businesses is over investing in one or a few areas, leaving other areas completely exposed. Being strong, or mature in only one or a few areas can leave your business seriously exposed to cyber-attacks. Hackers, or bad actors as we now call them, target these areas because they know most businesses aren't addressing them.

Conducting a whole of business cyber maturity assessment is one of the very best ways to get a broad view of how your cyber risk management is progressing. It's an effective way to identify areas that need additional focus or attention. It's also an excellent way to improve your understanding of cyber risk management and what's involved in becoming more cyber resilient.



Who should complete this assessment?

The Cyberturity® 360 assessment is a high level assessment specifically designed for the senior leaders of your business. Our recommendations are that you include as many senior leaders, and board members if you have them, when you are completing the assessment. It's a great opportunity to get everyone on the same page at one time. It also acts as a great cyber risk management education piece that is directly relevant to your business.

The most important person to have present when completing your assessment is the CEO, or managing director, or equivalent. No one is more important to the cyber security of your business than the person at the very top. They are the one that sets and drives the security culture.

Absolutely include your current cyber security team as part of the group. This may be your IT provider or your IT team, but they will only be able to help answer some of the more technically focused questions. There is very little chance they will be able to answer a majority of the questions in the assessment.

To get the most out of this process we suggest that you assemble a group and complete the assessment together either as an in-person workshop or remotely via video conference. Either option is just as good. You will need to allow 45 mins to 1 hour to complete the assessment.

The following list is our recommendation for who should be present when you complete your assessment in order of priority of attendance:

1. CEO / Managing Director
2. CISO, CRO & Board members (if applicable)
3. Cyber security team / CIO / Head of IT / IT provider
4. CFO / Accounts Manager
5. COO / Business Manager / General Manager

IMPORTANT! Cyberturity® 360 is not a technical assessment or compliance audit. Please do not send this assessment to your IT team or IT provider to complete by themselves.

What does the assessment cover?

The Cyberturity® 360 assessment covers 8 areas that address cyber risk management as a whole of business risk issue. Managing cyber risk requires more than IT intervention alone, and spans every aspect of your business as well as the partners you trade with.

Understanding these areas and how strong you are in them is critical to maximising your cyber security investments and developing real cyber resilience.

The 8 areas addressed in the Cyberturity® 360 assessment include:

Security Culture - Cyber security is a risk issue that spans all parts of an organisation. How much is cyber security part of the day-to-day, living, breathing fabric of your business.

Self Awareness - Every business, no matter the size or sector, has 'crown jewels' or digital assets of value to cyber criminals. How aware of your digital assets are you, and just what you have to lose?

External Awareness - The nature and purpose of cyber-attacks is constantly evolving. How well do you understand the cyber risk landscape – the scope, the threats, the reasons they attack?

Identifying your Digital Assets - Just like an inventory of hard assets for insurance, you should list your digital assets, who has access to them, and which are the most valuable.

Preparing to Protect - This is where most organisations focus. While technology alone can't deliver cyber security, it is a critical aspect. Do you have the right tools to protect your digital assets?

Ability to Detect Intrusion - Holistic cyber security doesn't stop with prevention. Even the biggest and best get breached. How well are you setup to detect an intrusion before it can cause serious damage or loss?

Ability to Respond - Reacting effectively to a breach can be the difference between going on or going under. How well are you set up to mitigate the threats and reduce the damage?

Ability to Recover - You've been breached! How do you go about rebuilding your business and your reputation? Who tells your clients and partners? What's your plan?

What does my score mean?

You won't find the traditional Green, Amber, Red in the Cyberturity® assessment. This isn't about identifying a business as "bad". Every business is on a different journey. They may be at the start, developing momentum, or a pioneering trailblazer. All are completely acceptable.

If you come across questions when you're completing the assessment that you don't know the answer to, that's ok. Make that your answer, "I don't know".

It will help ensure that you get access to the best information to help you on your journey. That is one of the most important outcomes from this process and the fastest and most cost effective ways to get better.

The Cyberturity® assessment has three levels of maturity scoring that aim to place your business at a certain stage of development in key areas and sub sections. The levels are as follows:

Low – Understand
You have uncovered an area that leaves your business highly vulnerable to cyber-attack. Before you invest time, money and resources to address this area, seek to fully understand the issue and which actions will give you the best results.

Moderate – Implement
You have identified an area with moderate levels of cyber security and resilience within your business. This result shows that you are aware of it and are already taking steps to improve. Seek to identify the most effective next steps and implement them as soon as possible.

High – Improve
This is an area where you are strong, putting your business in a good position to prevent or recover from a cyber-attack. The cyber-attack landscape is constantly changing so continually seek to assess and improve this area to remain well protected.

What is in my report?

Now you know where you stand, it's time to act and your Cyberturity® Maturity Assessment Report is that starting point. It's a plain English guide that gives you more detail about the specific areas of focus covered in the assessment, why they are important, our suggestions and what your current position is,

Your Cyberturity® Maturity Assessment Report will help you to prioritise your next steps and where you should focus your investments. This could include deeper investigation into specific areas of focus that have been identified as vulnerable, accessing training or education for you and your staff, or implementing additional IT or security controls.

Your report is really the starting point of a cyber risk management journey that you can use with your cyber security expert to help you develop your strategies and a roadmap to build strong cyber resilience and maturity. And if you don't have a cyber security expert then we suggest that you work with your existing IT provider. You may also find other trusted advisors such as your accountant or lawyer can be of assistance as they understand risk management. Remember, this is a whole of business risk issue, not just an IT one!

Appendix 1 – 8 Areas of Assessment

1. Security Culture

Security culture is best when it is top-down. What does that mean? It means that executives must lead cyber security initiatives in any organisation. Executives do not need to be involved with every detail of cyber security operations, but a mature organisation has executives involved in decision making for cyber security issues.

At the heart of security culture is the realisation that there are valuable digital assets within an organisation, as well as risks that threaten profit and even the total viability of an organisation. The mitigation of those risks is not just a technology issue, but also a process issue and ultimately requires a culture that is aligned towards security.

2. Self Awareness

You have valuable digital assets. This simple realisation is a first step towards being able to protect those assets. One of the reasons why organisations with immature cyber security posture believe they do not have valuable digital assets is because they look at those assets in isolation.

Your customer list may just be a set of names and emails, and potentially also their credentials. You might think that because the data does not include a credit card number, it is of minimal value to an attacker. Your data has large value to an attacker because these attackers piece together your data with other breached data.

In the age of 'big data', correlation of data vastly increases its value, to everyone, including for malicious purposes. Your data may look like a completely isolated inconsequential artefact in the hands of others, but this is simply not true. It is a puzzle piece to a much larger picture, and has value in a world where identity theft is rampant.

3. External Awareness

Obviously, we all need to have awareness of our risk against malicious attackers that we have no relation to, who simply want to steal the value of our digital assets. But what about the risks you face from competition, insider threats, human error or even just bugs in the software/systems you operate? It is vital to map out where all of your risks originate.

4. Identifying your Digital Assets

Just as in the 'Self Awareness' section, the National Institute of Standards and Technology's (NIST) cyber security framework calls for the identification of hard and soft IT assets, but also their relevance to governance and risk management. Identifying your current state is vital to be able to define your mitigation priorities. Keep in mind that this only works when all your stakeholders are also identified, and formal methods of communication are in place. Remember, cyber security is not just an IT issue. It involves the entire organisation.

5. Preparing to Protect

Once you have identified your digital assets, it's time to protect them. This is where most organisations start, but don't have a plan. Your plan should be based on your inventory and vision for the outcome of your organisation. Once you have done this it is time to consider access controls, awareness/training, data security, maintenance and other security technologies. Remember, there are no silver bullets, regardless of what security vendors tell you in their marketing.

6. Ability to Detect Intrusion

Detection of malicious cyber security activity is much more difficult than you might expect. Even large organisations struggle with this and almost all globally respected incident handling reports have reported that most organisations find out very late about being a victim of a cyber-attack.

Cyber-attacks are mostly silent to the average person, including to the average IT staff member. Detection of cyber-attacks is a rare skill, and therefore we must try to employ controls. The problem is that detection controls usually requires people with those rare skills, making this need for detection out of reach for most organisations especially small organisations. But we must try, and there are things we can do.

7. Ability to Respond

Malicious cyber security attacks are inevitable. Whether they succeed or not, is a function of your defence posture, but how you respond to them is a function of planning. Again this is not a function that should be given to IT, but should be reviewed by executive leadership and executed by someone who understands risk management. This could be a third party consultant or someone in your organisation with that skillset. Are you liable to Australian breach notification laws, or perhaps European General Data Protection Regulation (EU GDPR) ? Do you have a response and communication plan? Are you continually improving these plans and processes? Cyber security maturity in response is as important as all the work and procurement that goes into risk mitigation itself.

8. Ability to Recover

After all the work that has gone into risk inventory and awareness, mitigation controls, detection and response, now you have to be able to recover from a cyber security attack. You must have a plan and continually review and improve it. This plan should include communications planning as well as technology planning.