THE EIGHT KEY AREAS TO HELP SECURE YOUR BUSINESS

By understanding the 8 key cybersecurity risks that pose a threat to Australian businesses, you can assess how prepared you are to face them. Use our Business Maturity Matrix Indicator to identify, summarise and track potential issues that might be compromising the security of your business. By working through the Business Essential 8 and highlighting where your business sits in each category (high, medium or low) you can identify the maturity and cyber risk level of your business.

CSOGROUP
SECURING AUSTRALIAN BUSINESS

MATURITY MODEL MATRIX INDICATOR

Essential Business 8		Maturity Level		
		Low	Medium	High
Risk Management	Cyber and Information Security has just as much impact (if not more) than any other risk to your business, so it needs to be treated with the same level of importance. The flow on effects of a breach can go further than you might think.	No business related cybersecurity risks have been identified and aligned to your business operations.	Some business risks have been identified, but are not aligned to the operational impacts. The risks are tracked through a risk management framework.	Business risks related to cybersecurity threats have been identified and aligned to business operations and owners assigned. The risks are managed through a risk management plan and reported to the board as a high priority agenda item.
People & Security Culture	Create a culture of cyber safety that speaks to the whole business - it’s not just for the IT team to worry about. Make everyone aware of their responsibility when it comes to Cyber and Information security, because lack of policy, processes and general awareness create the greatest vulnerabilities to any business.	There is little or no training, awareness or plan to build a cybersecurity culture.	Cybersecurity training and awareness is being conducted. However, no cultural change plan has been considered or identified.	All departments and lines of business have a cybersecurity plan that aligns to the objective of developing a cybersecurity aware culture. HR are actively driving a change program to embed cybersecurity safety culture throughout the organisation.
Cloud Adoption and Innovation	Taking your business into the cloud is the next step in innovation, but making the move to digital also needs a security strategy of its own, as you leverage off the advantages and differentiation the cloud provides.	Your organisation is consuming cloud services with little or no strategy or processes supporting the secure use of the cloud. You could also be lacking knowledge of how many cloud systems are being used within the organisation.	Your organisation is consuming cloud services and has processes to manage the use of these systems, data access and storage of known systems. However, there’s no validation of all services that could be used within the organisation.	Your organisation has developed a security strategy that addresses the usage of cloud systems that is supported by policies, controls and security tools to manage the policies within the cloud.
Measure, Benchmark and Report	Everyone wants to see a return on investment as well as the improvements in your security shield, so setup a baseline to track your progress and report back to stakeholders regularly. You want to ensure progress is visible and continues to be endorsed by showing the value provided to the organisation.	There is little or no vulnerability or maturity assessment established to determine the state of cybersecurity within the business.	A vulnerability assessment has been conducted against the defined cybersecurity risks identified within the business risk management plan, which is reviewed on an ad-hoc basis.	Regular vulnerability and maturity assessments aligned to the business risks are conducted. This is tracked and reviewed through a defined governance framework.

MATURITY MODEL MATRIX INDICATOR

Essential Business 8		Maturity Level		
		Low	Medium	High
Governance & Strategy	Organisation structures and governance frameworks are critical for the management of the security risk, as there are many different departments that play in the cyber network. These key players need to know what they're accountable for and how they contribute, as their awareness and engagement are key to success of the overall strategy.	Your organisation has no cybersecurity risk committee in place and there is no formalised reporting into organisational risk management processes. The only security reporting for the business is provided by IT functions and there is no clear evidence that a cybersecurity strategy is in place.	There is a risk committee that reviews cybersecurity as a regular management function. A technology cybersecurity strategy has been developed but it is not tracked or reviewed and IT (either CIO or IT Manager) is responsible for cybersecurity.	A business focused cybersecurity strategy is in place, aligned to the risk management plan and supporting processes, controls, tools and education have been implemented. A dedicated senior security officer (CSO) has been appointed and reports into risk and security committees are attended by all business departments. The board of directors review monthly reporting on cybersecurity.
Operations	Have an effective operating model showing how things should actually be working. Without it, any gains or improvements will quickly degrade and benefits and outcomes will not be obvious or implemented.	Your business operating model has not been assessed in identifying cybersecurity risk areas. No operating model is defined and any/all cybersecurity activities are managed by the IT department only. Your cybersecurity operating functionality is ad-hoc and relies solely on the IT department to administer and maintain.	The business' operating model has been assessed for threats with a few policies and controls. The service and control model and its responsibility is largely placed with the IT department to detect, assess and respond.	Your operating model includes all departments and their accountabilities are defined. The business' supply chain has also been assessed and mapped effectively under a responsibility assignment matrix (RACI) across the organisation. These are regularly being tracked and reported.
Regulation and compliance	Establish a strong compliance framework as part of your risk management plan. Keep in mind that this will continue to change and increase for the foreseeable future both locally and internationally, as will the penalties if the framework isn't adhered to.	There is little or no awareness of the mandatory disclosure laws within the Privacy Act or GDPR exposure or implications for your business and customers. There are no current plans to establish ISO27001 compliance/ certification.	You've assessed the compliance and regulatory requirements of the business and have some controls and a reporting framework in place. There is currently no ISO 27001 or equivalent certification and no requirement for suppliers to comply to policies or standards.	From the board down, the organisation is tracking and reporting its compliance exposures and obligations actively. You have ISO 27001 certification or equivalent standards in place and the business supports its suppliers or requires supplier compliance to policies and certification to conduct business with you.
Data & Information Management	Your data is important and it's your obligation to manage it efficiently. Take steps to categorise it, know what is sensitive and what isn't and treat it accordingly. Your responsibility of managing, retaining, removing and accessing data is serious and if not done correctly, holds significant consequences.	There is little or no understanding or awareness within your organisation as to where the organisations' sensitive, IP and/or critical data resides. There is also little or no awareness as to the responsibility of the organisation in regards to storing data.	The business understands its obligations as to what is required to obtain, store and remove data, however effective controls and processes are not evident or understood. Knowledge of sensitive and critical data locations are documented, although effective controls to monitor and maintain the data are not in place.	The organisation has mapped, classified and documented its data within its organisation and supply chain. Processes, systems and controls are in place to ensure the security, retention and discarding is performed consistently and accurately.

MATURITY MODEL MATRIX INDICATOR

CSOGROUP
SECURING AUSTRALIAN BUSINESS

WALK

LOW	**Your maturity level shows a lack of awareness and controls to manage the business' cybersecurity risk factors.** Assistance is needed to build a stronger defence. This matrix outlines potential risk factors requiring consideration. A more comprehensive assessment is required to break down the threats, demonstrate how they relate to your business functions and show you how effective management and strategy can mitigate many of the risks you're currently facing.
MEDIUM	**Your maturity level suggests there are some awareness and risk controls in place... however there are material gaps that need addressing.** More is required to provide the levels of security required by your business. We've outlined some areas which we recommend be placed on the agenda in the immediate future to drastically reduce the risk of cybercrime affecting operations.
HIGH	**Your maturity level suggests you currently have adequate control of your cybersecurity risks.** Your organisation is recognising cybersecurity as a serious business risk, not defaulting to an IT. Each business is different, and with the ever changing cybersecurity landscape, including the development of millions of new forms of malware and threat vectors being developed annually. It is recommended that regular health checks are conducted to maintain an effective level of protection.