Cyber security self-assessment

A checklist for small and medium-size enterprises

DOWNLOAD THE CYBER SECURITY PLAYBOOK FOR SMEs

CONTINUUM CYBER
Simple & safe

CHARTERED ACCOUNTANTS™
AUSTRALIA + NEW ZEALAND

DIFFERENCE MAKERS™

Cyber security self-assessment checklist

	Governance	Yes	No	Unsure	Hi/Med/Low	Recommendation
1	Do you have an information security policy approved by management and communicated to all employees?	○	○	◉	HIGH	Develop an information security policy to help with the coordination of security strategies across the business.
2	Do you have a process to review your information security policy at least annually?	○	○	◉	HIGH	Reviewing an information security policy annually and tracking the changes ensures the information is kept up-to-date.
3	Do you perform security threat and risk assessments on critical information systems using an industry-standard risk assessment methodology?	○	○	◉	HIGH	Determine which systems represent your 'crown jewels'. Review risk scenarios against these assets as part of your existing business risk management framework.
4	Do you have a system maintenance policy in place (including patch management, RACI, etc) reviewed regularly and updated?	○	○	◉	HIGH	Develop a policy to govern roles, responsibilities and timeframes for information system maintenance. This should include 'patch management', which covers patching vulnerabilities of your operating system, hardware and software.
5	Do you have a privacy policy that includes data retention and destruction?	○	○	◉	HIGH	In many industries, privacy has become a regulatory requirement. Ensure that your policy includes personal identifiable information (PII) - how it will be used, stored and destroyed.
	Asset management	**Yes**	**No**	**Unsure**	**Hi/Med/Low**	**Recommendation**
6	Do you have a list of all hardware and systems within the business?	○	○	◉	HIGH	You cannot protect it if you are unaware of what you own. Begin by developing a list with hardware and systems that contain sensitive information
7	Do you have a list of all applications used to support your business?	○	○	◉	HIGH	Each department of your business should create a master list of essential and optional applications. This will determine if the applications are still supported by the vendor, up-to-date with their patching and security, and compliant with any licensing requirements. Using a master list will help to develop role-based access, keeping higher risk applications under closer watch.
8	Do you have information classification rules established to address confidentiality requirements?	○	○	◉	MED/HIGH	Based on your industry, developing an information classification system (such as public, confidential, employee confidential, management restricted, private) will share security responsibility with all employees and allow you to protect files and documents commensurate with their value to your business.
9	Do you have a record of data flows between internal and external information systems?	○	○	◉	HIGH	If you know what information is typically moving around and outside your network, it will be easier to determine anomalies.

Cyber security self-assessment checklist (continued)

	Identity management, authentication and access control	Yes	No	Unsure	Hi/Med/Low	Recommendation
10	Have you recorded individuals with administrative privileges?	○	○	○	HIGH	Administrative privileges comes with greater responsibility and accountability for information security. Individuals should be granted admin access based on their role based access control (RBAC).
11	Are users' requirement for privileged accounts regularly revalidated?	○	○	○	HIGH	Regular reviews of access requirements ensures that individuals are able to do their job unimpeded without introducing extra risk.
12	Have Role-based access controls been instituted (i.e., role-based rather than by named user)?	○	○	○	MED/HIGH	Assign permissions to individuals based on their role within the business. It offers a simple, manageable approach to access management and is less prone to error than assigning permissions individually.
13	Is access to information systems approved by the asset owner?	○	○	○	MED/HIGH	This is a workflow issue - it's fundamental that access approval goes through the master administrator to ensure they need access to that information.
14	Are all accesses linked to unique user credentials?	○	●	○	HIGH	Every user should have their own login and password (a complex password or a passphrase) allowing for more accurate auditing and ensuring individuals do not have access to information beyond what they require.
15	Are access rights reviewed on a regular basis by the asset owners?	○	○	○	MED/HIGH	Your asset owner is responsible for the day-to-day management of your information systems and needs to be aware to whom they've granted access and for what purpose.
16	Do you use multi-factor authentication (MFA) for remote access to business data and e-mail accounts?	○	○	○	HIGH	Multi-factor authentication (MFA) is an authentication method that requires users to present two forms of verification to gain access to a resource. For accesses outside your physical network, MFA provides an extra layer of security to ensure the only person accessing your businesses information is the person you intend.
17	Do you use multi-factor authentication (MFA) for all administrative access to cloud services?	○	○	○	HIGH	As with remote access to your data, administrative access to your cloud service allows greater privilege and access. Multi-factor authentication (MFA) is a best practice to ensure the correct person is being granted access.
18	Do you ensure only administrative accounts can install or run new applications?	○	○	○	HIGH	As part of application whitelisting (one of the Australian Signals Directorate Essential 8 Principles) all new applications should be reviewed, tested and approved by your administrator before being installed. This ensures all applications meet minimum security standards and prevents users from creating open doors for cyber criminals.

Cyber security self-assessment checklist (continued)

	Human resources policies and training	Yes	No	Unsure	Hi/Med/Low	Recommendation
19	Does your hiring policy include background or screening checks commensurate with their access to sensitive information?	○	○	○	MED/HIGH	Follow the 3Cs of pre- or post-hiring screening checks to ensure you know who has access to your sensitive information: Company-wide, Consistent and Compliant
20	Do you have an Acceptable Use policy signed by all employees?	○	○	○	MED/HIGH	Creating an Acceptable Use policy for all corporate systems (hardware, Wi-Fi, etc.) keeps users away from websites and practices that weaken your security.
21	Do you conduct employee cyber security training relevant to their job function (at least annually)?	○	○	○	HIGH	Frequent cyber security training that includes details that are relevant to an employees job function should overall security awareness.
22	Do you conduct regular phishing simulations of your employees?	○	○	○	MED/HIGH	Phishing simulations can be used as a continuation of the training, rather than a test. Departments that do exceptionally well should be publicly commended rather than pointing to the ones that did not.
23	Is there a process in place to remove user accounts when employees leave?	○	○	○	HIGH	Just as accounting and HR departments have processes from the first to the last day, so too should information security. Ensure HR process includes a flag to your administrator, with formal processes to remove access and conduct an access review as necessary.

	Data security	Yes	No	Unsure	Hi/Med/Low	Recommendation
24	Do you have a process in place to ensure all hardware and media containing confidential data is encrypted?	○	○	○	HIGH	Ideally, every device used to access, store or transfer restricted, confidential or personal information (such as USB keys, laptops, tablets, cell phones and external hard drives) must be encrypted. The quality of your encryption tools should be commensurate with the information you are storing.
25	Do you have a policy and process to ensure the secure removal or destruction of devices containing confidential information?	○	○	○	HIGH	Creating a clear asset inventory policy that includes processes for the storage, removal and destruction of all hardware and removable media helps to ensure sensitive or confidential business information is secure.
26	Do you use data loss prevention (DLP) tools to detect or block potential unauthorised or unintentional transmission or removal of confidential data?	○	○	○	MEDIUM	Data Loss Prevention (DLP) tools monitors sensitive data while in use, motion or at rest. It can be set to further ensure reduce the chance of data breaches through purposeful or accidental action.

Cyber security self-assessment checklist (continued)

	Information protection processes and procedures	Yes	No	Unsure	Hi/Med/Low	Recommendation
27	Have you created or adopted network security baseline configurations for all systems?	○	○	○	HIGH	A network security baseline is the first layer of defence - your fundamental elements upon which you can build more advanced security. Start small if you have nothing and adopt an industry configuration guide that includes the key security elements to be implemented in phase one of a 'defence-in-depth' strategy.
28	Do you have an automated system for tracking any changes or deviations from that baseline?	○	○	○	HIGH	Automated configuration management tools allow you to see when changes are made to your security posture. Whether purposeful or accidental, you want to know if someone removes basic network security functions.
29	Are all configuration changes documented and reported?	○	○	○	HIGH	Ensure that changes are tested in a safe environment (a 'sandbox') and log changes in case you need to return to a previous version and improve training going forward.
30	Do you have a Bring Your Own Device (BYOD) or similar policy?	○	○	○	MED/HIGH	BYOD is becoming more common as employees are comfortable with their personal devices and organisations wish to save money by not purchasing corporate devices. In 2020, two-thirds of polled employees reported using their personal devices at work. Set standards for how they can be used, how organisational data can be stored or accessed on devices and decide how you want to be able to remove it if the need arises.
31	Do you have a segregated wireless network for personal and guest devices?	○	○	○	HIGH	Guest networks are convenient for clients and employees during breaks. A guest network may be more open to the public or extended business, as such, you should segregate it from other networks that can access confidential and sensitive data.
32	Do you have a formal backup and recovery plan?	○	○	○	HIGH	The best time to prepare for data recovery is before you need it. Establish a policy and process for backups. Be clear about the businesses Recovery Point Objective (RPO) and establish acceptable data loss to determine the frequency of backup and when backup media can be overwritten.
33	Do you have up-to-date anti-malware software installed and used on all applicable systems?	○	○	○	MED/HIGH	Not all anti-malware software is created equal, but software-based anti-malware is a relatively low cost and unobtrusive security measure to add a layer of protection.
34	Are new security patches tested and applied in a timely manner?	○	○	○	HIGH	Just as with applications, security patches should come signed from trusted partners. If your security team is able, test new patches in a safe environment to determine if there are any problems interacting with the rest of your systems.

Cyber security self-assessment checklist (continued)

	Physical security environment	Yes	No	Unsure	Hi/Med/Low	Recommendation
35	Do you have a physical security environment policy (e.g., emergency power and lighting, fire protection, water damage protection)?	○	○	○	HIGH	Many insurers require these policies and processes, while others may offer incentives. In any case, your policies should address worst case scenarios specific to your physical environment(s) and be consistent with your determined acceptable data loss.
36	Have you located and secured all information system components to minimize damage or loss?	○	○	○	MED/HIGH	The location of components should account for natural threats to data loss (i.e., fire, flood) and data security. The more important the information on the component, the more secure it should be.
	Protective technology	**Yes**	**No**	**Unsure**	**Hi/Med/Low**	**Recommendation**
37	Do you have a process in place to record, store and review audit logs for IT activity?	○	○	○	HIGH	In addition to logs being written, a process should exist for their review in reasonable terms.
38	Are these logs adequate to ensure they are not overwritten before reviewed in case of an incident?	○	○	○	HIGH	Both from acceptable data loss and forensic investigation positions, balance log size with cost and usefulness. Ensure your logs cover enough time to be meaningful in case of a breach.
39	Do you have a removable media policy and ensure that all removable media is encrypted?	○	○	○	HIGH	Establish rules for all removeable media - what can be used, to store what kind of data and where that data can be taken. USB drives can be quickly lost or stolen. A minimum security standard encryption makes the data unreadable without the key.
	Security monitoring	**Yes**	**No**	**Unsure**	**Hi/Med/Low**	**Recommendation**
40	Do you monitor user activity for potential security events?	○	○	○	HIGH	Alongside your Acceptable Use policy, automated triggers can be placed to alert your security team if activity occurs on your network outside of normal business practices.
41	Do you use automated software (e.g., anti-malware, phishing e-mail filters, intrusion detection systems) to verify against malicious activity?	○	○	○	MED/HIGH	The more security practices you can automate, the more time your IT and security teams can focus on incidents of greatest concern and preventative training.
42	Have you performed penetration tests in the last year?	○	○	○	MED/HIGH	Penetration tests (or Pen Tests) are often performed by outside consultants to give a snapshot of the security posture from a cyber criminal's perspective. Establish a security program that meets the standards you believe are necessary and then test it.

Cyber security self-assessment checklist (continued)

	Incident response	Yes	No	Unsure	Hi/Med/Low	Recommendation
43	Do your Incident Response and Business Continuity Plans account for a potential cyber incident?	○	○	○	HIGH	BCPs ensure critical business resource processes and outputs are protected and functional in and after a disaster. It goes beyond the physical space to account for data and systems too.
44	Are your Incident Response and Business Continuity Plans (BCP) regularly reviewed, tested and updated?	○	○	○	HIGH	Standards change, as do contact people and processes. Regularly review and test Incident Response and BCPs so that they are current and communicated ahead of an incident.
45	Do you have a process for forensic investigation and analysis to be performed after a security incident?	○	○	○	MED/HIGH	Whether you have trained staff within your business or a third party on retainer, establishing a plan before an incident will be less expensive and more effective.
46	Are all incidents recorded and tracked, regardless of a forensic investigation?	○	○	○	MED/HIGH	Tracking incidents provides important metrics: you can determine the effectiveness of your security controls, assess security awareness of staff and needs for your security team.
	Extended organisation risk management	**Yes**	**No**	**Unsure**	**Hi/Med/Low**	**Recommendation**
47	Do your contracts with vendors and suppliers include information security requirements?	○	○	○	HIGH	After spending time and money to secure your own network and systems, you should demand a minimum standard of those in your supply chain. There are many examples of organisations that have lost millions because cyber criminals got in through a trusted supplier.
48	Do you have a record of all vendors, suppliers and clients with access to your network?	○	○	○	HIGH	Just as you know which employees have access to your premises, so too should you know which members of your extended organisation have access to your data and network.
49	Do you have an agreement for notification if any vendor or supplier suffers a cyber security breach?	○	○	○	HIGH	If your supplier or vendor suffers a cyber security incident, it could quickly become your problem as well. Make sure that it's in your contract to be notified so that you can protect yourself early.
50	Do you have a review mechanism to ensure vendors and suppliers are meeting the agreed requirements?	○	○	○	MED/HIGH	When you sign an agreement, establish a plan for cyber security review. Your vendors – and the rest of your supply chain – will thank you for setting the tone and increasing the level of cyber resilience for everyone.