Let our experts audit and fine tune your **cybersecurity defences**

Scope

Tell us the purpose of your audit and we can help define the right scope to match your desired outcome.

Low Friction

We work with your preferred IT provider or in house IT Manager to identify areas of concern.

Recommendations

You get a report that identifies any areas of concern and recommended a remedial course of action.

Get In Touch With Us.

Call Chris
0438 855 884
chris.karapetcoff@computingaustralia.group

The Essential Eight

The cornerstone of any cybersecurity review is an Essential Eight assessment.

We can then determine what additional steps need to be taken to strengthen your business security.

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight. The Essential Eight are designed to protect Microsoft Windows-based internet-connected networks.

It is therefore accepted as the gateway to reviewing a business from a security perspective. Based on the outcome of an Essential Eight review, it may be determined to take additional steps to strengthen your business IT systems.

What to expect from

an Essential Eight audit

We like to start all security reviews with an Essential Eight audit because it is the best benchmark for assessing cyber-readiness.

Depending on your IT management model, this could involve us working with your existing IT company or an in-house staff member. We ask a lot of questions but nothing that an average user with basic knowledge of your system can't handle. If you take a look at the chart we added to the next page, you will see the criteria we target.

Essential Eight / Cyber Security Audits are design to be non-confrontational and we don't advise using them to assign blame. The intention is to identify risks to your business and take remedial action to increase the resilience of your IT systems. We want everyone on board, from management down. Cyber security impacts the whole organisation, so encouraging all staff to contribute will always lead to better organisation wide outcomes. When people all think the same way, you can foster a change in mind set that leads to a more secure IT system and security driven culture.

At the conclusion of an audit, we will compile a detailed report that gives you a risk profile and often, a series of recommendations on what fixes are required. You can either engage with our technical team or your own IT support to take the steps provided.

Most businesses need to take out Cyber Security insurance these days, but it is important to understand that insurance companies are unlikely to pay our claims where they can materially prove deficiencies in your IT systems.

Most insurance companies are requesting that you answer a number of key questions prior to being granted cover. Be careful not to just tick boxes, because if you have a cyber event that warrants insurance, they are going to do a deeper forensic examination before they award the cover.

Legislatively, the amendments to the SOCI Act require that specific critical infrastructure assets must report certain types of cyber security incidents. If you become aware that a critical cyber security incident has occurred, or is occurring, and the incident has had, or is having, a significant impact on the availability of your asset, you must notify the Australian Cyber Security Centre (ACSC) within 12 hours after you become aware of the incident.

If you do nothing else this year in terms of IT, we recommend that you do an Essential Eight audit.

To book an Essential Eight audit

Please contact Chris on 0438 855 884

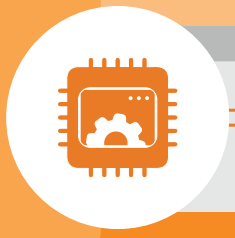
Or email sales@computingaustralia.group

1 APPLICATION WHITELISTING

Application whitelisting to control the execution of unauthorised software

2 PATCHING APPLICATIONS

Patching applications to remediate known security vulnerabilities



3 CONFIGURE MACROS

Configuring Microsoft Office macro settings to block untrusted macros

4 APPLICATION HARDENING

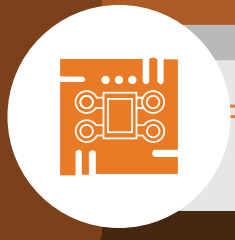
Application hardening to protect against vulnerable functionality

5 RESTRICT ADMIN PRIVILEGES

Restricting administrative privileges to limit powerful access to systems

6 PATCHING OPERATING SYSTEMS

Patching operating systems to remediate known security vulnerabilities



7 MULTI-FACTOR AUTHENTICATION

Multi-factor authentication to protect against unauthorised access

8 DAILY BACKUP

Daily data backup to maintain the availability of critical data

Call Chris on 0438 855 884 or email sales@computingaustralia.group