Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

SMALL BUSINESS CLOUD SECURITY GUIDES

EXECUTIVE OVERVIEW

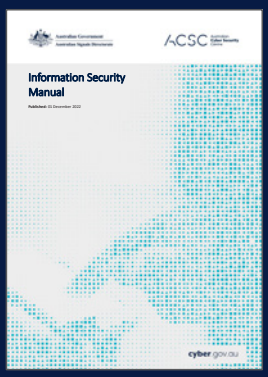
cyber.gov.au

Small Business: Cloud Security Guides - Executive Overview

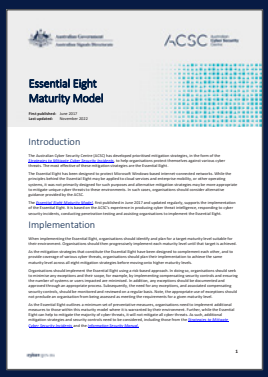
For more cyber security advice

For more information on how to improve your cyber security, see our other guides at **cyber.gov.au**

Small Business Cyber Security Guide



Information Security Manual



Essential Eight Maturity Model

Strategies to Mitigate Cyber Security Incidents

Table of Contents

Introduction

Cyber security incidents can affect any organisation at any time. The ACSC Annual Cyber Threat Report 2022 found that the average cyber security incident costs small businesses sting in their cyber security. In recognition of the increasing prevalence of cloud computing, the Australian Cyber Security Centre (ACSC) has published the Small Business Cloud Security Guides. These guides are designed to provide advice to protect against cyber incidents while remaining accessible to organisations which may not have the resources to implement a more sophisticated strategy.

The ACSC's Small Business Cloud Security Guides provide technical examples organisations can use as a reference point when designing their own cyber security approach. The examples demonstrate how the business can securely configure their Microsoft 365 tenancy.

Why invest in cyber security?

Cybercriminals and state-sponsored actors are using sophisticated techniques to compromise Australian organisations. The ACSC responds to attacks against Australian organisations every day, with the biggest threats including:

- ransomware
- exploitation of security vulnerabilities
- software supply chain compromises
- business email compromise.

Simply installing the latest technology in your organisation is not good enough, cyber security thinking needs to evolve. Failing to invest in your organisation's cyber security could lead to costly attacks, interruptions to operations, loss of data, reputational damage, legal liabilities and more. Implementing the Small Business Cloud Security Guides will help protect your organisation by making it much harder for cyber incidents to impact your office productivity capabilities.

[1] www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

Case Study

The Federal Court rules on managing cyber security risks.

In 2021, the Federal Court delivered a landmark ruling that highlights the obligations organisations hold to manage their cyber security risks.

The ruling related to an Australian Financial Services licensee which suffered several cyber attacks over a six year period. As a result of these attacks, the Federal Court found that the organisation had breached its obligations as an Australian financial services licensee.

In their judgement, the Federal Court noted a number of inadequate risk management practices across the organisation's network. This included some of its authorised representatives failing to have up-to-date anti virus software, system backups, email filtering or quarantining, and poor password practices. They were ordered to engage a cyber security expert to improve their cyber risk management and pay $750,000 towards the Australian Securities & Investments Commission costs.

While this judgment related to obligations as an Australian financial services licensee, it should put organisations of all sectors on notice. Managing cyber risks cannot be an afterthought or an optional extra. It is increasingly being recognised as an essential responsibility of all organisations.

How to use the guides

The ACSC's Small Business Cloud Security Guides are made up of a series of technical examples which use strategies aligned with ACSC's Essential Eight.[2] They're not designed for organisations looking to meet a specific Essential Eight maturity level. Instead, they have been designed as an easy way for organisations to protect against cyber threats and increase cyber security. These guides should be used as a reference only. Organisations should apply appropriate risk management when implementing the advice, with consideration for their unique operational needs and environment.

All organisations should implement cyber security mitigation strategies that are proportionate to their risk profile and risk appetite. The Small Business Cloud Security Guides are a good starting point for most small and medium sized Australian organisations that use a Microsoft 365 software as a service environment and have devices configured with Microsoft Intune. To find out more about which ACSC guidance is the best fit for your organisation, read the ACSC Business Guidance Breakdown. [3]

Resourcing considerations

Protecting your organisation from cyber incidents will require a financial and human resources investment and should be a priority for all organisations. Investing in preventative measures is typically far less expensive than responding to a cyber security incident.

The Small Business Cyber Security Guides will require a resourcing commitment from your staff or IT managed service provider to implement and maintain. It may be appropriate to train staff on how to administer your Software as a Service suite. Many vendors provide free training on how to use their products.

The ACSC has endeavoured to use low cost or free solutions in these guides where possible, however, many security configuration options are unavailable in entry level Microsoft 365 subscriptions. To follow these guides, and increase opportunities to protect against cyber threats, organisations will need a Microsoft 365 Business Premium subscription (or equivalent). Employees that require administrator roles will also need an Azure Active Directory Premium P2 subscription.

[2]www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight

[3]www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security/small-business-cloud-security-guide/small-business-cloud-security-guides-introduction

The eight mitigation strategies

The Small Business Cloud Security Guides apply the principles of the Essential Eight. The Essential Eight are the eight most effective and highest priority strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents[4] to protect against cyber threats. The strategies are underpinned by the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents and conducting penetration testing. Table 1, over the page, summarises each of the mitigation strategies including their benefits and costs.

Next steps

There are actions your IT team need to take before your organisation implements the Small Business Cloud Security Guides. These are outlined in the introduction to the guide on cyber.gov.au. After completing these actions, your IT staff or IT managed service provider will be ready to review each technical example and adapt it to your organisation's needs.

Also consider joining our Partnership Program. The ACSC Partnership Program enables Australian organisations and individuals to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy[5].

[4] www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents
[5] www.cyber.gov.au/resources-business-and-government/become-acsc-partner

Table 1 – Mitigation strategies, benefits and costs

Mitigation strategies	Benefits			Impost on organisation
	Protect against malware	Limit the extent of cyber incidents	Recover from a cyber incident	
Application control Reduces the risk of executing malicious programs.	✓			Users can only install applications that are deemed secure by Microsoft's Intelligent Security Graph.
Patch applications Fixes application security vulnerabilities.	✓			IT administrators must manage regular patching. If users rely on unsupported applications, the organisation may need to invest in upgrades or secure alternatives.
Configure Microsoft Office macro settings Reduces the risk of running malicious macros.	✓			Users cannot run macros without demonstrating a business requirement. IT administrators must manage macro permissions.
User application hardening Restricts the use of application functionality that is insecure.	✓			IT administrators must configure application settings. Users cannot use application functions that are deemed insecure.
Restrict administrative privileges Reduces the risk that accounts with special privileges are compromised or used inappropriately.		✓		Users must request approval to temporarily activate administrator roles when required. IT administrators must manage activation of administrator roles. Administrators are prevented from performing higher risk actions when logged into administrator accounts. A limited number of Azure Active Directory Premium P2 licenses are required.
Patch operating systems Fixes operating system security vulnerabilities.		✓		IT administrators must manage regular patching. If the organisation relies on unsupported operating systems, it may need to invest in upgrades or secure alternatives.
Multi-factor authentication Prevents unauthorised access to systems and accounts.		✓		Users are required to provide at least two factors of authentication when certain conditions are met.
Regular backups Allows restoration of data and settings after an incident.			✓	IT administrators must manage regular backups. The organisation may choose to purchase a commercial backup solution.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2023
With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre