Huntsman®
Defence-Grade Cyber Security

Obtaining Cyber Insurance Cover, including Renewals, in 2022 – 2023

Topic 2

Australia's Essential Eight: Beyond Endpoint Control

FOR VISIBILITY OF CYBER-RISK PREVENTION, CONTAINMENT & RECOVERY

As a decision-maker within your organisation, you may be familiar with the set of cyber security and risk mitigation strategies that the Australian Government created to help organisations protect their systems against cyber threats. Known as the Australian Cyber Security Centre (ACSC) Essential Eight, this framework of strategies is recommended to all organisations as a set of cost-effective baseline cyber security controls.

If you've had to reset your password from your favourite phrase to a combination of letters, numbers and characters that are hard to remember, or if you are required to use an Authenticator app to gain access to files or parts of your system, then your team has potentially already implemented at least some of the suggested security mitigation strategies.

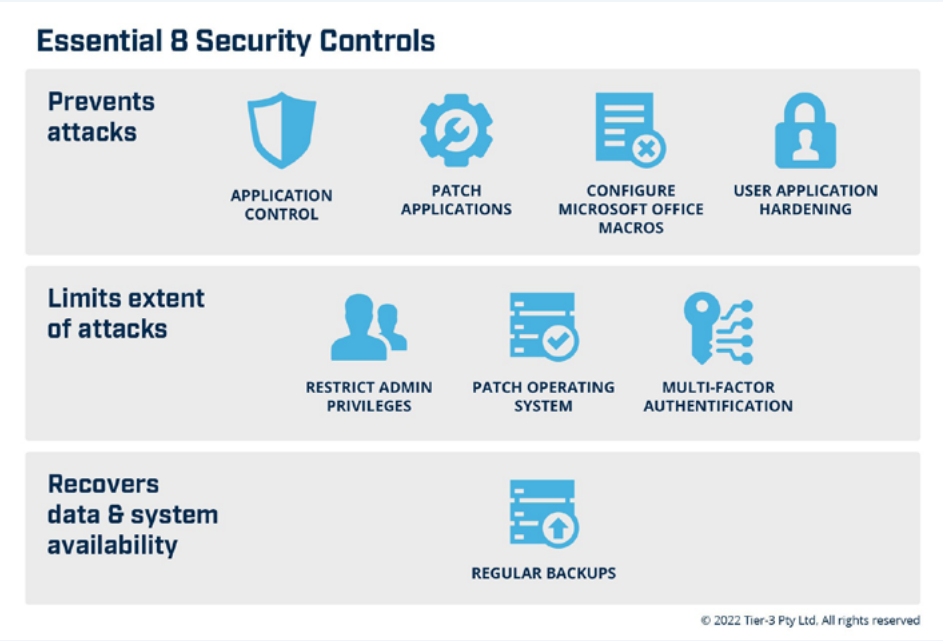
▶ Question 1

Have your teams implemented any or all of the eight strategies, to protect your Microsoft Windows-based connected networks and systems? How do you have ongoing assurance of this?

It might seem like a question for your IT team, but this question is now also directed to your executives, board, risk managers and any others involved in the in the renewal of your cyber-insurance policy in the coming 12 months.

The likelihood of cyber-attack in Australia and the potential costs to organisations associated with such an attack has risen considerably in the last little while, and the style of attack varies too. This means that organisations need to demonstrate a range of prevention, containment and recovery steps as a part of their risk controls.

The Australian Cyber Security Centre's (ACSC) Essential Eight risk management framework is a prioritised list of eight mitigation strategies (security controls) organisations can implement to protect their systems against a range of cyber attacks.



QUICK READ:
The Australian Government's recommended cyber risk measurement

Given the increased cyber risks to all facets of private and public organisations, the Australian Government, through its Australian Cyber Security Centre, established a framework – the Essential Eight – that defines a baseline set of mitigation strategies that aim to make it harder for attackers to gain access to your systems.

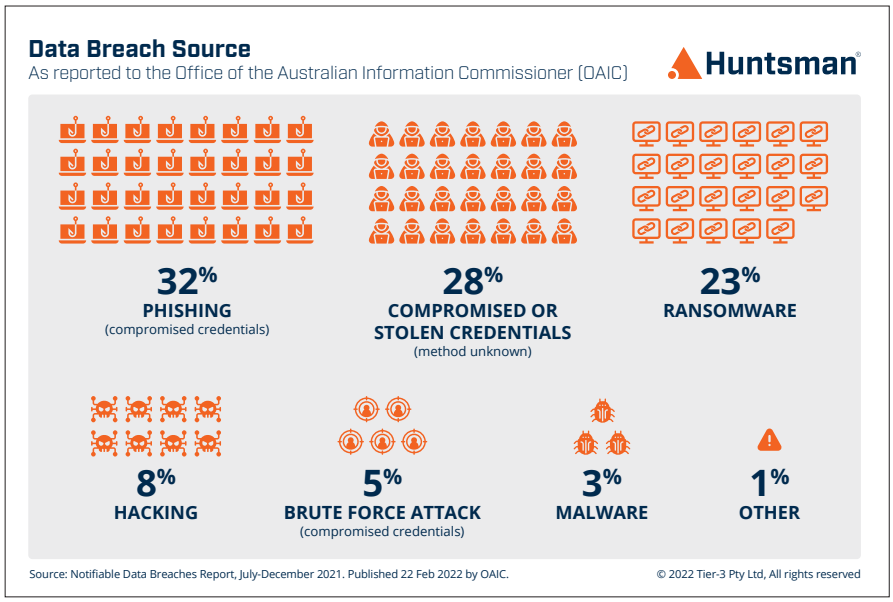
The Essential Eight Maturity Model is an implementable product of these strategies, it enables organisations of any size to measure the effectiveness of their cyber risk controls. Once an organisation establishes it security level objective, which can depend upon the nature of its business and the perceived associated IT security risks, it can measure its "compliance" with the Essential Eight framework to determine any gaps, which can then be mitigated as they are identified. It incorporates a key set of technical checks & balances which can be measured to support cyber security objectives. With an experienced and dedicated Security Operations Centre (SOC) or security specialists within your Information Communication Technology (ICT) team, the Essential Eight Maturity Model can be applied to measure the adequacy of your cyber risk mitigation efforts.

The effectiveness of each security control is measured as a score, that informs your ICT or SOC teams of any inadequacies in the operation of the key security controls. In parallel, these scores provide clear visibility to the executive, board, and risk managers, of the state of your current security posture and cyber risk readiness, highlighting any areas requiring particular risk management oversight.

A single point solution, such as Multi-Factor Authentication (MFA) or simply strengthening your password strategies is not enough. Because a single point solution can represent a single point of failure, frameworks like the ACSC Essential Eight seek to address the concept of Defence-in-Depth. By monitoring the effectiveness of multiple strategies, an Essential Eight risk assessment can provide significantly better visibility across the prevention, containment and recovery phases of a cyber-attack.

In looking at the Source of Cyber Incident Breakdowns results from the recent Office of the Australian Information Commissioner's report, it is evident that there are a range of ways that Australian organisations are being targeted, and there needs to be a more comprehensive approach taken to defend and protect your data and systems, and ultimately your product & service delivery to customers.

It's in the name - ***Essential*** Eight. The next steps for your executive, board, and risk teams are to firstly determine the extent to which you have implemented this powerful set of risk mitigation strategies, and secondly, to regularly assess the operating efficiency of each of those controls. Interestingly the ACSC no longer prioritises any single one of the controls above another – they acknowledge that all need to be in place.



OAIC Notifiable Data Breaches Report. July to December 2021. Published 22 Feb 2022

Question 2

Did you know that evidence of your organisation's implementation of the Essential Eight can support cyber insurance renewal, and is now a tool that underwriters are starting to look for to validate your cyber maturity?

As ransomware and cyber risks increase, it is recommended that organisations get ahead of the onerous reinsurance process – now starting 2 to 3 months before their current policy ends. Huntsman Security's Insurance Renewal Initial Report, driven by the Essential 8 Auditor software application, streamlines the process of IT risk assessment or posture measurement for organisations, as it aligns directly to the Essential Eight framework.

This data-driven application provides accurate cyber-risk measurement via a simple dashboard, and identifies vulnerabilities that might leave your entire organisation at risk.

With the gaps highlighted via the assessment, your in-house ICT team can remediate against the provided 'to do list', and then, if required, re-audit your entity to quantify and validate that your cyber posture is one that insurance providers can cover.

This new step in insurance coverage is valuable for any organisation that prioritises cyber insurance as a risk-control, and now seeks quantifiable data to verify its cyber posture, to:

- Visualise & measure the cyber risk controls that will affect your insurance terms and eligibility for cover
- Understand your cyber posture with a data-driven application designed to measure your cyber resilience across detection, containment and recovery
- Use these changing insurance requirements to improve your security controls and maintain your access to insurance as a risk management option

Your risk profile is the single most important factor in informing re-insurance success.

Huntsman Security's Essential 8 Auditor software application strengthens your internal capacity to address these emerging cyber risk areas, support renewal of your cyber insurance, and manage your broader cyber security needs.

Download the Essential 8 Auditor brochure

Download

Start the Preliminary Stage of your Cyber Insurance Renewal process with an Insurance Renewal Initial Report driven by:

Essential 8 Auditor

On-demand cyber vulnerability & maturity assessment

With on-going access to resilience reports, cyber maturity metrics, remediation "To-Do" Lists, and the ability to regularly 'Re-Audit' your environment for 12-months.

ALIGNED TO THE AUSTRALIAN CYBER SECURITY CENTRE'S (ACSC) ESSENTIAL EIGHT CONTROLS.
[from $7,500].

Contact Us e: info@huntsmansecurity.com

Huntsman®
huntsmansecurity.com