Huntsman®
Defence-Grade Cyber Security

FOR GOVERNMENT

- Risk & Audit Team
- Executive Team
- Directors

Agency resilience, compliance & reputation:

a cyber governance perspective

The Australian Signals Directorate's (ASD) recent publication of their Cyber Threat Report 2022-2023 unearthed a range of areas for concern for government departments and critical infrastructure entities at local, State and Federal level.

The pressure for leaders – with and without a specific information technology or security reference in their job title - is to manage the increasing accountability that leadership roles have with regards to cyber-risk oversight of department data, systems, and assets from both internal and external cyber-attack.

This summary aims to equip your leadership roles – especially those without a technology or security title – to stay current with the latest findings, and access short- and long-term solutions to improve cyber governance.

Key cyber pressures to be aware of that will impact government departments in 2024

1. **Government departments at all levels, and Critical Infrastructure organisations, face ongoing cyber-attack targeting by state actors (and organised crime)**
   - 20% of all critical vulnerabilities are exploited before patches are even installed[1]
   - 40% of vulnerabilities were exploited more than a month after a patch is released[2]
   - The updates to the Essential Eight Maturity Model announced in late November 2023 place an increasing priority on the frequency of risk assessments and mitigation. Critical patching regardless of the Maturity Level of the environment, for example, is now required to be completed within 48 hours of a priority vulnerability being identified.[3]

Malicious cyber incidents grew by 50% in 2022-23. The ASD encourages the sector to report anomalous activities early and not wait until thresholds for mandatory reporting are reached, because the immediacy of reporting is vital to containment and recovery activities.

[1] https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023
[2] ibid
[3] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

2. AUKUS is likely to generate added attention from those seeking to disrupt capabilities or steal sensitive information

- As Australia increases its voice and visibility through security partnerships with the United States, the UK and others, the profile of critical domestic entities is also raised.
- The benefits of closer ties to like-minded nations is clear but it is important to realise that with that comes an attractive and expanded attack surface to tempt threat actors operating from inside and outside an agency's physical and digital environments.

3. The interconnected nature of critical infrastructure (CI) and government entities means an increased systemic risk of attack

- We are about to see the preparedness of all critical infrastructure related organisations revealed when the new CIRMP Rules under Part 2A of the Security of Critical Infrastructure Act 2018 (SOCI Act) come into play, which require CI entities to have implemented and complied with their selected cyber security framework by 24th August 2024. CI organisations captured under Part 2A of the SOCI Act are also required to submit their first annual report to authorities no later than 28th September 2024.
- There is still a time window, between now and August 2024, for CI organisations to adopt a security framework and implement an effective cyber governance regime.
- International cyber security agencies continue to confirm that CI assets remain attractive targets. Their sensitive customer information, provision of essential services, and a high level of interconnectedness place them at the commercial, economic and social centre of our community.

> “International cyber security agencies continue to confirm that CI assets remain attractive targets. Their sensitive customer information, provision of essential services, and a high level of interconnectedness place them at the commercial, economic and social centre of our community”

The Commonwealth Cyber Security Posture in 2023 Report identified a range of cyber insights across all corporate and non-corporate Commonwealth entities.

CYBER SECURITY POSTURE ACROSS ENTITIES

Essential 8 (E8) maturity is improving but still low

17% of entities have reached E8 Maturity Level 2 (up from 11% last year)

25% had reached E8 Maturity Level 2 (up from 19% last year) when self- assessed compensating controls included

Patching performance continued to be poor in 2023

SECURITY INCIDENT RESPONSE PLAN

18% had no security incident response plan

42% reported 50% of incidents to ASD

LEADERSHIP AND PLANNING

27% had no cyber strategy (28% in 2022)

12% have joined Cyber Threat Intel sharing (up from 2% in 2022)

The responsibility and burden of guarding Personal Information

Alongside malicious threat actors, sits the localised risk that threatens your cyber security – human error. It is being constantly tested by increasingly genuine looking phishing emails as well as the problem of staying aware. Culture building and cyber awareness programs need continuous revitalisation and reinforcement with teams. While training and education programmes are essential within an organisation, they are far from being the fail-safe defence. Humans can make mistakes, maybe in your department or one of your supply chain partners. In either circumstance, a "portfolio" of defence-in-depth mitigation strategies is the best way forward.

2023 alone, has seen health, justice, telecommunications, and education data breaches[4], amongst others, that have impacted many in the community, and indirectly the government as well. The Office of the Australian Information Commissioner (OAIC) has been important in facilitating compliance and early reporting of breaches for organisations covered under the Privacy Act 1988.[5]

The legislation helps keep organisations accountable and ensures that individuals, whose information has been disclosed, are informed of their risks and remedial options as soon as possible. Beyond protecting stakeholder information, leaders in government agencies can equally be directly and indirectly responsible for:

- Loss of intellectual property
- Cost of down-time
- Impact on safety or health and wellbeing of staff or customers
- Cost of re-establishment of services or productivity
- Reputational risk costs (short, medium and long term)
- Additional resourcing required (including IT support, public relations advice, and legal)
- Administration overhead
- Impact on financial stability

Solutions with short- and long-term prevention/ containment/recovery benefits

Ensuring cyber risk visibility for your risk management and leadership teams

Building cyber resilience, especially within government agencies and critical infrastructure, is vital. For some, positive cyber security obligations already exist. As the cornerstone of our economy - and because so many of our vital digital assets are held within those entities – Government entities and CI providers are pivotal in driving cyber posture improvements and operational resilience across the broader economy. Especially as leaders need to ensure they remain informed, ideally with clear visibility of cyber security and other non-financial risks, that will inform their decisions and the performance of their duties.[6]

At a recent cyber security conference in Sydney, the Chairman of the Australian Securities and Investment Commission (ASIC) warned that "if boards do not give cybersecurity and cyber resilience sufficient priority, [it will] create[s] a foreseeable risk of harm to the company and thereby exposes the directors to potential enforcement action by ASIC based on the directors not acting with reasonable care and diligence"

https://www.smh.com.au/business/companies/watchdog-takes-aim-at-company-directors-over-cybersecurity-20230918-p5e5h9.html

[4] https://www.webberinsurance.com.au/data-breaches-list#twentythree
[5] https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities#WhoHasResponsibilitiesUnderPrivacyAct
[6] https://asic.gov.au/regulatory-resources/find-a-document/reports/corporate-governance-taskforce-director-and-officer-oversight-of-non-financial-risk-report//information-flows

Data-driven cyber-risk information

If you are not aware of the extent to which data-driven collection and analysis of empirical cyber security information can assist the timeliness and reliability of your decision making, now is the time to ask. Without an understanding of the sources and accuracy of the information that underpins your cyber reporting, you are at risk of making uninformed decisions.

Whether for risk management or strategic purposes, risk leaders, executive, and even board level, need to have confidence in the information that forms the basis of their decision-making. Clear evidence-based information that systematically captures the metrics relevant to your reporting and oversight obligations, will help ensure that your agency is not left exposed by an incomplete or inconsistent governance efforts.

In their efforts to simplify the translation of technical information into business or management reporting, IT teams can sometimes resort to abridged and even anecdotal reporting. In a strengthening legislative environment where senior executives and directors need evidence-based reporting that balances clarity and context, this is no longer acceptable. The security information needs to be in a clear and consistent format that enables decision makers to understand and meet their management and statutory responsibilities.

Automated cyber risk summaries for monthly review

If there is one trend for sure, it is that the cyber threat environment is continuing to become more dangerous. So, as you seek better evidence to support your decision making; it's important to remember the dark side is not standing still either. You should be asking how your SOC or IT teams are managing to collate and analyse enough relevant security data in such a rapidly changing environment. Especially on top of their business-as-usual cyber monitoring and response activities. How accurate and reliable is the data?

Collecting and analysing the appropriate and relevant data to assess the state of the dynamic threat environment is absolutely challenging. With its randomness, it is important to shrink the measurement intervals to limit the range and variability of the data being captured – measure more frequently.

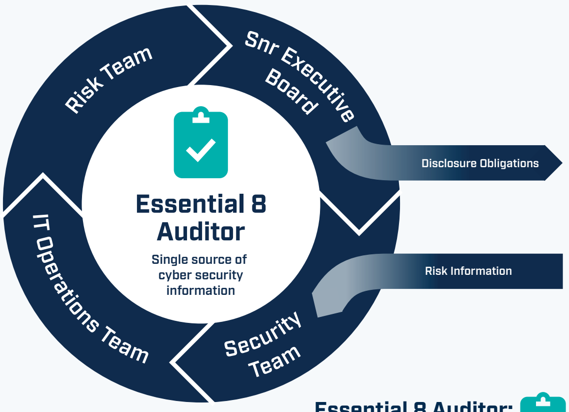
Effective cyber security is all about managing the detail within all the noise. Systems are complex, skilled staff are hard to attract and retain, data volumes are growing and you're looking to protect every last potential point of unauthorised access. Gaps are a problem, and current cyber security practices are not a guarantee of your ongoing cyber resilience – especially if they are built on subjective judgments or imprecise standards.

https://huntsmansecurity.com/blog/gaps-are-evident-in-australias-cyber-security-readiness/

Huntsman

Data-driven Cyber Security Measurement

A Single Source of Truth for Risk Management Stakeholders



One application to fulfil your cyber risk management obligations and boost operational resilience for you and 3rd parties

Essential 8 Auditor: Find out more

This turns out to be consistent with the latest recommendations of security agencies. More frequent collection of evidence-based observations, reduces the quantum and unpredictability of events and so dials down the uncertainty. Complexity too, whether it's the multiplicity of potential threat vectors at the threat surface or simply the complication and scale of current network architecture, will be reduced with more frequent measurement.[7]

At this point in any department or agency's digital journey, there should be a move toward automation of cyber-risk data. This is a problem happening at machine-speed and security teams can't keep up, yet security agencies are asking for more frequent risk assessments. To support your staff and enable them to focus on higher value activities, automated identification, assessment, and reporting can get them on top of your cyber resilience efforts - without every team member needing to be a cyber security specialist.

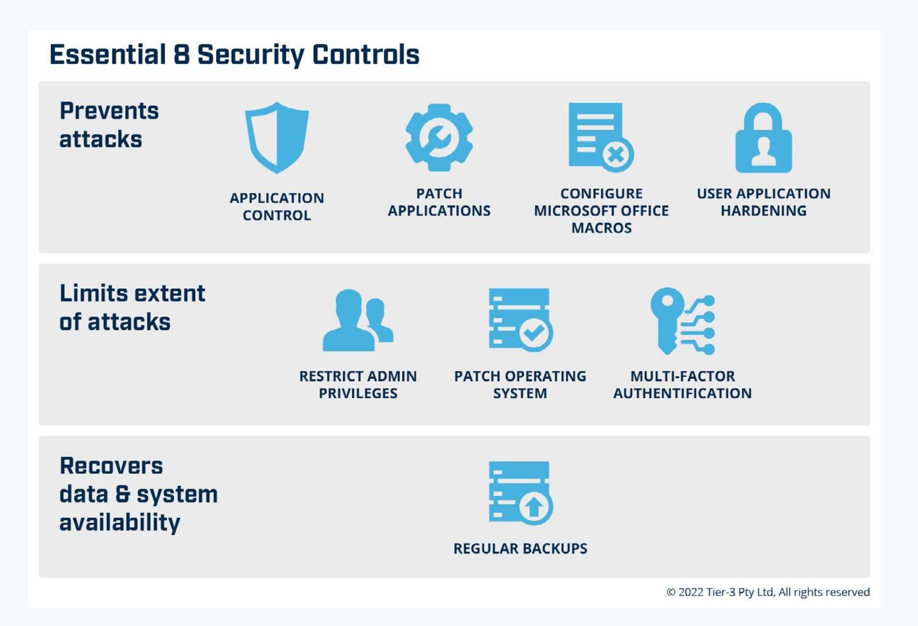
And it shouldn't be an enormous overhead or multi-year project – you should be able to access this information by your next board meeting, and easily within your delegation limits.

> “It shouldn't be an enormous overhead or multi-year project – you should be able to access this information by your next board meeting, and easily within your delegation limits”

The ease of using the ACSC's Essential Eight Framework

The Australia Cyber Security Centre (ACSC) and Australian Signals Directorate (ASD) Essential Eight Framework is a baseline for cyber security that is used across local government, State departments, and Federal agencies in Australia.

Utilising eight mitigation and cyber-risk management strategies, the Essential Eight Framework prioritises protection, containment, and recovery controls to protect your systems against adversaries and cyber theat.


Essential 8 Security Controls
Prevents attacks
APPLICATION CONTROL
PATCH APPLICATIONS
CONFIGURE MICROSOFT OFFICE MACROS
USER APPLICATION HARDENING
Limits extent of attacks
RESTRICT ADMIN PRIVILEGES
PATCH OPERATING SYSTEM
MULTI-FACTOR AUTHENTIFICATION
Recovers data & system availability
REGULAR BACKUPS

© 2022 Tier-3 Pty Ltd, All rights reserved

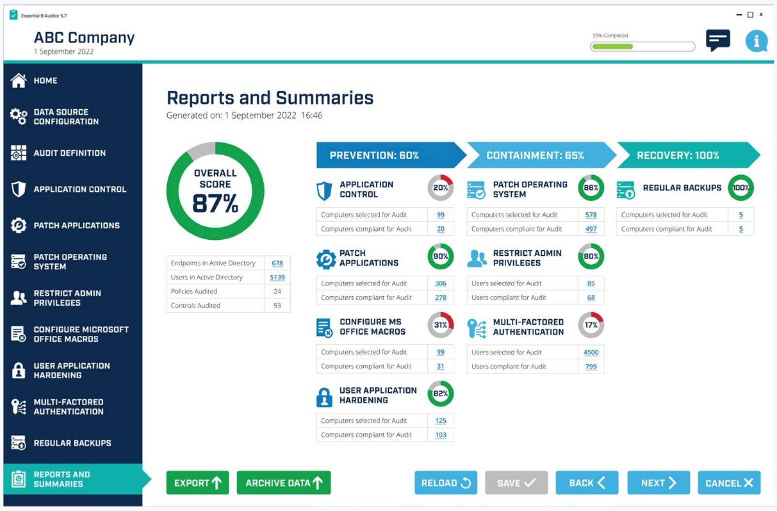
The Australian Cyber Security Centre's (ACSC) Essential Eight risk management framework is a prioritised list of eight mitigation strategies (security controls) organisations can implement to protect their systems against a range of cyber attacks.

[7] https://huntsmansecurity.com/blog/active-management-for-operational-and-cyber-resilience/

Next steps?

Your department or agency can reduce your attack surface by securing systems with the Essential Eight Framework or using one of the other alternate frameworks recommended in the CIRMP Rules[8] to maintain an asset registry, protect sensitive data and employ security by design.

Although operational activities may sit with others, your role still has an expectation of oversight of cyber risk. As you navigate digital transformation, and face upcoming cyber reporting and legislative requirements, consider Huntsman Security's **Essential 8 Auditor** or **Essential 8 Scorecard** applications.



ABC Company

1 September 2022

Reports and Summaries

Generated on: 1 September 2022 16:46

OVERALL SCORE 87%

Endpoints in Active Directory	678
Users in Active Directory	5139
Policies Audited	24
Controls Audited	93

PREVENTION: 60%

APPLICATION CONTROL 20%

Computers selected for Audit	99
Computers compliant for Audit	20

PATCH APPLICATIONS 90%

Computers selected for Audit	306
Computers compliant for Audit	278

CONFIGURE MS OFFICE MACROS 31%

Computers selected for Audit	99
Computers compliant for Audit	31

USER APPLICATION HARDENING 82%

Computers selected for Audit	125
Computers compliant for Audit	103

CONTAINMENT: 65%

PATCH OPERATING SYSTEM 86%

Computers selected for Audit	578
Computers compliant for Audit	497

RESTRICT ADMIN PRIVILEGES 80%

Users selected for Audit	85
Users compliant for Audit	68

MULTI-FACTORED AUTHENTICATION 17%

Users selected for Audit	4500
Users compliant for Audit	799

RECOVERY: 100%

REGULAR BACKUPS 100%

Computers selected for Audit	5
Computers compliant for Audit	5

Cyber security measurement and reporting system – available to you before the next board meeting

Huntsman Security's Essential 8 Auditor and Essential 8 Scorecard boost your cyber risk management and corporate governance oversight with automated and data-driven cyber security measurement and maturity level reporting – giving you daily, weekly or monthly visibility of your cyber controls and their performance against the Essential Eight.

The effectiveness of each security control is measured to inform both your security and management teams of any mitigations necessary in the operation of the key security controls. In parallel, the measured score reliably provides clear visibility to the executive, board, and risk managers, of the state of your current security posture to inform risk management oversight and regulatory reporting.

Benchmarked against the ACSC Essential Eight, the Essential 8 Auditor and Essential 8 Scorecard equip you and your organisation with a recognised evidence-based framework to identify and mitigate cyber security hazards – and support compliance with CIRMP review and reporting requirements utilising the ACSC Essential Eight Maturity Model.

Talk to our team

Request a demo

[8] *Section 8.4.b* https://www.legislation.gov.au/Details/F2023L00112

e: info@huntsmansecurity.com

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman

Huntsman®
Defence-Grade Cyber Security