Huntsman®
Defence-Grade Cyber Security

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

Topic 3

Cyber gap measurement & evidence

THE NEW STANDARD OF QUANTIFIABLE INTERNAL ASSESSMENT

As much as we invest into our people and culture, human error is inevitable. In a recent Notifiable Data Breaches Report, from the Office of the Australian Information Commissioner, for the 6-month period from July to December 2021, Health Services noted 47% of breaches resulted from human error, the Finance Sector noted 48% and Education a significant 75%.

The above 'human error' sources of a breach, and the cyber incident breaches from external threats combine to present a daunting prospect for organisations when it comes to cyber awareness training and risk mitigation efforts. That's why the ability to automatically measure or identify a breach - whether it is because of human error or not - is vital to internal assessment.

▶ The quantitative v qualitative debate

The reality of 'human error' is one part of the reason why quantitative, rather than self-assessment-based reporting is so important for organisations reporting on the health of their cyber security posture. Improvements in cyber security staff training and awareness will obviously assist in pre-emptively limiting the likelihood of a human error - but the real question is 'how will you know when that error has occurred'? That's where quantitative, data-driven scoring assists, by providing an objective and relative measure of the scale of the risk. Changes in qualitative measurement, particularly small ones, can sometimes be difficult to discern but objective measurement, when based on verifiable data, reflects any relative change in performance over time. It's no different measuring the cyber security and the cyber maturity of your organisation.

As we support our clients to manage their risks and controls, we also improve the quality of the information necessary for insurance underwriters to more accurately price risk. This means the best possible insurance renewal terms for an organisation, with underwriters increasingly equipped with a simple report that verifies client statements about their cyber controls and posture.

The reality is that human-nature influences qualitative assessments, making them subjective and often unreliable. Alternately, security controls that are systematically measured against a relevant benchmark, enable your SOC or ICT team to know where to start their mitigation efforts; and your prospective insurer to be more informed about the risk they are being asked to take on.

▶ An established measure that's ready for you to access

The Australian Government's Australian Cyber Security Centre (ACSC), established a framework of mitigation strategies to make it harder for attackers to gain access to your IT assets and systems – the Essential Eight – that incorporates a quantitative benchmark for measurement. The key to mitigation of cyber risks – whether from human error or external breaches - still lies in the detection of the correct implementation of your cyber risk controls and the demonstrable measurement that shows your current posture, on an ongoing basis.

The UK Government's National Cyber Security Centre provides similar guidance for both public and private sector organisations looking to protect themselves from malware and ransomware attack. The mitigating malware and ransomware attacks guidance provides advice on the appropriate security controls to limit the: (i) likelihood of infection, (ii) its spread across the organisation; and (iii) the impact of the infection. Prevention, containment and recovery mitigation strategies are universal themes.

As ransomware and cyber risk increase, organisations are encountering the longer lifecycle of insurance renewals and the need to demonstrate better management of security controls and their effectiveness. The upside, is that by better managing your security controls, you can better influence the price of risk and the cost of your premiums.

The insurance industry is looking closely at ways to improve the quality of the security risk information they receive. Improved risk information means the better pricing of risk and proven tools, like Huntsman Security's Essential 8 Auditor or SmartCheck to measure and verify an organisation's cyber security posture, and:

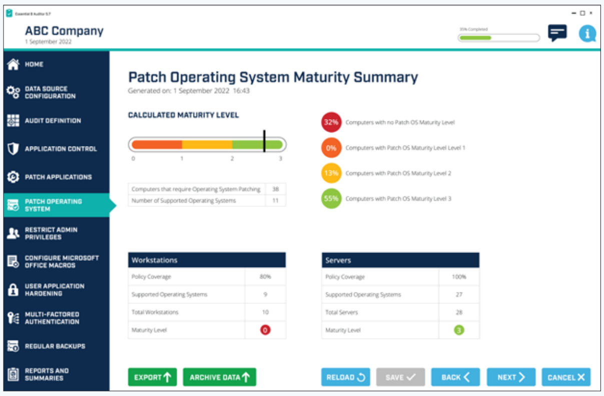
- Visualise & measure the cyber risk controls that will affect your insurance terms and eligibility for cover
- Understand your cyber posture with a data-driven application designed to measure your cyber resilience across detection, containment and recovery
- Use these changing insurance requirements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

What attestations and metrics should your Executives & Directors and Risk & Security teams be looking at?

1. **On-demand cyber security maturity rating, measured against the ACSC Essential Eight framework or NCSC & NIST guidance for malware and ransomware mitigation** – Whether you review your cyber risk weekly, monthly, or quarterly, you should have access to a quantitative number that gives you a score and maturity rating – across each of the prevention, containment and recovery safeguards.

2. **Data-driven reporting and analysis** - Quantitative based analysis and reporting is the most accurate way of measuring compliance. Data-driven reports provide certainty and allow your organisation to confidently use the results as a measure of performance in your official attestation of your cyber security assessment.

3. **Benchmarks for security improvement and a roadmap to remediate gaps** – Automatic identification and classification of each security issue found should be something your SOC or ICT teams have access to. An actionable report will support the remediation and the re-run of your maturity assessment as part of any uplift effort. These reports then form the basis of your own cyber maturity journey, and are a useful aide memoire for attestation to your internal cyber risk management activities.



Patch Operating System Maturity Summary
Generated on: 1 September 2022 16:43

CALCULATED MATURITY LEVEL

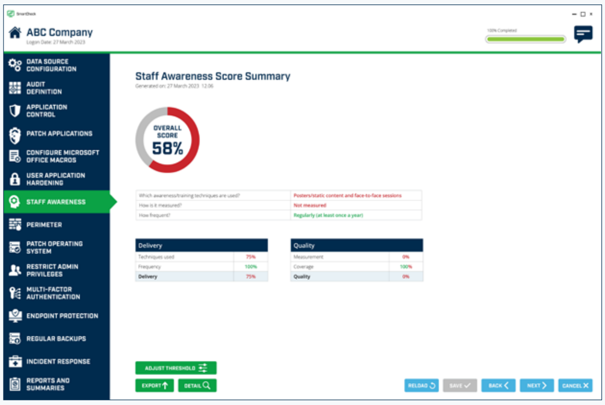
Computers that require Operating System Patching	38
Number of Supported Operating Systems	11

32% Computers with no Patch OS Maturity Level
0% Computers with Patch OS Maturity Level Level 1
13% Computers with Patch OS Maturity Level 2
55% Computers with Patch OS Maturity Level 3

Workstations	
Policy Coverage	80%
Supported Operating Systems	9
Total Workstations	10
Maturity Level	0

Servers	
Policy Coverage	100%
Supported Operating Systems	27
Total Servers	28
Maturity Level	3

Essential 8 Auditor – Patch Operating System Maturity Summary



Staff Awareness Score Summary
Generated on: 27 March 2023 12:06

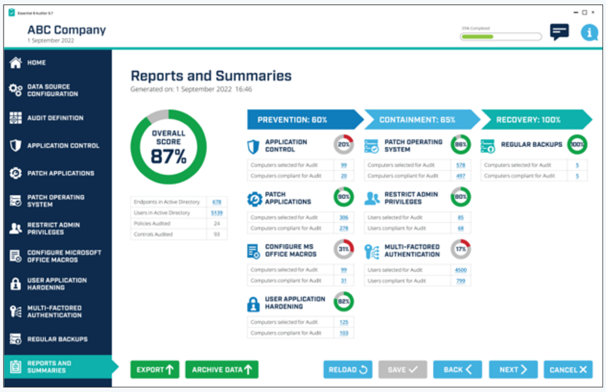
OVERALL SCORE 58%

Which awareness/training techniques are used?	Posters/static content and face-to-face sessions
How is it measured?	Not measured
How frequent?	Regularly (at least once a year)

Delivery	
Techniques used	75%
Frequency	100%
Delivery	75%

Quality	
Measurement	0%
Coverage	100%
Quality	0%

Smartcheck – Staff Awareness Score Summary



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

Essential 8 Auditor – Reports & Summaries

The World Economic Forum published recommendations and considerations for boards to follow, in their publication: Principles for Board Governance of Cyber Risk.

Principle 2.2 encourages boards and leadership to continually examine comparative measurements and metrics for cyber risk. The paper states: "Industry-accepted frameworks and reporting can guide data-driven decisions, aligning risk appetite with organizational goals and strategy."

Cyber risks can change overnight, with new external threats emerging or simply through new connections, devices, staff and systems. Organisations need to have visibility of those changes for ongoing risk awareness and mitigation, and at insurance renewal time – they are an important validation of their cyber risk management efforts.

Talk to your broker today about starting the preliminary stage of your cyber insurance renewal process and build more confidence in your cyber risk management by using risk-based measurement to improve the process now and into the future.

Your risk profile is the single most important factor in informing re-insurance success. Huntsman Security's Essential 8 Auditor or SmartCheck software applications strengthen your internal capacity to address these emerging cyber risk areas, support renewal of your cyber insurance, and manage your broader cyber security needs.

Start the Preliminary Stage of your Cyber Insurance Renewal process by activating the Insurance Renewal Initial Report driven by one of the following applications:

▶ 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].

▶ SmartCheck

Measure your cyber risk

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 WITH GUIDELINES FROM THE UK'S NATIONAL CYBER SECURITY CENTRE (NCSC) AND THE US DEPARTMENT OF COMMERCE'S NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST). [from £7,500].

Contact Us e: info@huntsmansecurity.com

Huntsman®
huntsmansecurity.com