Huntsman®
Defence-Grade Cyber Security

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

Topic 4

Systematic measurement of cyber controls

FOR CONTINUED INSURANCE COVER

▶ Verifiable proof

One of the key learnings coming out of the Australian Banking Royal Commission for Directors, Executives, and staff who report up to the Board, centred around the need for the governance-layer of an organisation to see verifiable proof of compliance across the organisation, and not just to assume that existing policies and processes imply alignment and fulfilment. This is equally relevant for cyber security.

This is not a "set and forget" mindset toward results and activity, this represents an active engagement with actual results that can be tracked and reviewed at any point in time, as well as trend-analysed over longer periods. Are the current policies and procedures achieving the strategic objectives?

The expectation of verifiable proof of your organisation's cyber security health and wellbeing should take the same approach too, as it has emerged as another vital component of risk management and business continuity planning.

▶ Productive paranoia

In his book Great by Choice, business leader Jim Collins notes that good leaders continually ask "What if?". By preparing ahead of time, building reserves, preserving a margin of safety, bounding risk, and honing their disciplines in good times and bad, they handle disruptions from a point of strength and flexibility.

This is not just wise advice from a researcher who focusses on business stability and growth, it's likely the kind of risk-management thinking that has already prompted your organisation to choose to invest in insurance cover, amongst other mitigation strategies, since its inception.

As cyber-risk has now become a regular discussion item under the risk agenda of small and large organisations, the question to ask is whether your organisation has cyber-attack prevention, containment and recovery thinking embedded in how it measures this type of risk, and whether your executives and board have a regular line of sight to this information? In fact, in its November 2021 Insight publication *Improving Cyber Resilience*, the Australian prudential regulator recommends that directors review and challenge [the quality of] the cyber information they receive from management to assist mutual understanding.

Whether you are based in the APAC region, in the UK or USA, ideally, you should be expecting regular governance-level proof that your cyber security measures are strong (or proof that there are methods in place to identify gaps, and then apply a fix). No doubt, as your team add this to their daily and weekly agenda, they'd appreciate a management process that minimises added costs and disruption, that still produces high fidelity in reporting.

The good, the bad, and the hopeful news around your cyber insurance renewal process

If your executive, board and staff already have a culture that reflects sound risk management and business continuity thinking, you're already ahead of the game when it comes to insurance renewal time.

Unless you've been off-grid for the last 12-months, you'll know that globally there was an 105% increase in ransomware attacks from 2020 to 2021, that included double and triple attacks, according to the 2022 SonicWall Cyber Threat Report. Right now, we're experiencing a slight hiatus in this trend but just as extreme weather conditions and natural disasters have an impact on the cost of insurance, cyber security effectiveness and coverage face the same rules.

Cyber insurance cover and renewal has become harder, but it is possible to navigate, by utilising cyber insurance renewal tools, that also have the side-benefit of strengthening your risk readiness and organisation's cyber maturity.

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

> “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**”

Essential 8 Auditor 5.7

Essential 8 Auditor
Executes a Cyber Risk Audit

Welcome to the Huntsman Essential 8 Auditor

Version 5.7

Copyright © 2022 Tier-3 Pty Ltd, All rights reserved

What are underwriters / insurers looking for with respect to cyber security maturity?

Returning to the concept of 'proof', we know that it needs to be something that is supported with real data. We know underwriters and insurers more generally are seeking to improve their loss ratios, and better-quality cyber security risk information is a key part of that. Knowing the effectiveness of the risks covered greatly assists in understanding the remaining or residual risk yet to be mitigated. In the reality of busy workplaces — the limitations on finding skilled staff in this tight job market and when organisations now need to account for every device (that might include legacy machines that lie forgotten in an office) — automation of data collection is a key enabler to what can be an unending task.

With the Huntsman Security Essential 8 Auditor or SmartCheck option, organisations are finding that because it is benchmarked against the ACSC Essential Eight framework or the NCSC Ransomware mitigation guidance, it provides accurate and timely cyber maturity measurement. As a result, it provides underwriters and insurers with an evidence-based measure of the state of your security controls and the residual risks to be underwritten. In the event of an insurance claim (the driving reason behind why organisations cover their risks with insurance), insurers are increasingly seeking to verify that the agreed mitigation activities were exercised as part of the ongoing operations of the business.

They will often look for:

- Legitimacy of quantitative vs qualitative measurement, and to know how required changes are identified, and the resulting informed security response;
- Quantitative metrics and proof of mitigation measures and ongoing maintenance of cyber risks – to support future claim eligibility;
- Automated benchmarking and cyber maturity scoring – the value of an approach that replaces sampling and estimation with hard verifiable data that informs effective security decision making;
- The value your organisation places on regular cyber vulnerability and maturity assessment in a changing threat environment;
- The quality of the security information, to effectively manage any exposure to security risks.

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