An Introduction to Silent Cyber - Fact Sheet

An Introduction to Silent Cyber

We have recently updated our commercial business package policy wordings to set out our position on whether cover for cyber-related incidents and personal data exposure is included. Our new wordings are available as part of our quote or renewal process.

Our definitions help set out the cover for (or exclusions in respect of) cyber- and personal data-related incidents under each of our commercial business package policy wordings.

Current Insurances and Silent Cyber

Cyber risk is one of the most dynamic challenges facing the insurance and reinsurance industry.

Silent cyber refers to potential cyber-related losses stemming from traditional property and liability and small business insurance policies that were not initially specifically designed to cover cyber risk.

Unlike the specialist standalone cyber insurance products that are available in the market today, traditional liability policies were not designed with cyber exposures in mind and therefore may not implicitly include or exclude cyber risks.

This coverage ambiguity can result in a silent cyber scenario, whereby an insurer may have to pay claims for cyber losses off a policy not designed for that purpose.

The lack of clarity in some standard business package property and casualty policies can also lead to confusion or misunderstanding about coverage for cyber risks.

The Insurance industry refers to this coverage ambiguity as 'silent cyber' because it is neither explicitly included on an insurance policy, nor explicitly excluded.

What Cyber changes are the Insurance Industry making?

Insurers are taking steps to address this issue, some required by regulators, to clarify their coverage intent regarding cyber. Some insurers have clarified their coverage intent by defining cyber risk and then excluding it from non-cyber policies. Some are introducing new policy language and underwriting guidelines. We have taken the stance to expressly exclude cyber risks in all our small business package policy wordings.

Growing Cyber risk exposures

The insurance market now offers risk transfer solutions for cyber risk that address both ever-evolving technology risk and the recent retreat of traditional insurance products from adequately addressing small business evolving cyber-risk profile.

Cyber insurance begins with the premise that all business technology-driven risk should be insurable. These risks include both the direct loss that a small business can suffer in terms of lost revenue or assets, as well as the liability that can arise from a data breach or failure to comply with the myriad of new domestic and international regulations.

How to manage and protect your Small Business Cyber exposures

The following links provide some suggested good practices that enable small business entities to operate highly adaptive and responsive cyber resilience processes. We encourage all small business entities to consider their application to improve their own cyber resilience preparedness.

Cyber resilience good practices | ASIC - Australian Securities and Investments Commission

Cyber security and resilience is essential to all small business' operating in the digital economy.

Cyber resilience is the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations.

We also encourage you to visit the Australian Cyber Security Centre (ACSC) and register to receive their alerts. The ACSC has a range of resources for small and medium businesses and large organisations, including useful tips, guides and assessment tools:

Small & medium businesses | Cyber.gov.au

Small Business Cyber Security Guide | Cyber.gov.au

Step-by-step guides | Cyber.gov.au

Cyber Security Assessment Tool | Cyber.gov.au

Cyber Exclusions

Insurers have responded to the issue by expressly excluding cyber from traditional coverages to mitigate any ambiguity.

Expressly excluding cyber on small business commercial package non-cyber policies is a good step towards making sure that both insurer and insured understand each other's expectations of coverage.

Our Claims approach

Each claim is different. Whether or not the policy affords cover will be determined by the particular circumstances of the claim and the specific terms and conditions set out in your business policy wording (PDS).

The following are examples of cyber- or personal data-related claim scenarios and are provided as a guide only to the types of incidents that our policies may, or may not, typically respond to.

Claims example1: Buildings, contents and other property wordings

Our intent is not to provide cover for damage to any item that is directly caused by a cyber incident, or where damage spreads digitally from one item to the next. However, we do cover subsequent damage to other covered property that arises as a result of the initial incident.

For example, this scenario would typically be covered:

Your digitally activated fire suppression system (e.g. water mist or deluge sprinkler), was hacked and turned on, causing damage to your building or contents. The damage to the buildings and contents would be covered, although we would not cover damage to the fire suppression system itself caused by the hack.

For example, this scenario would not be covered:

Your digital device no longer works following a cyber-attack, hack or other related issue.

Claims example 2: Public liability (PL)

Our intent has never been to provide cover for a cyber-related incident under a PL policy.

For example, these scenarios would not be covered:

- Following a data breach, your businesses customer data was lost, and you or your employees suffered mental anguish as a result;
- Your customer's laptop was infected with a virus when connected to your business network, whilst in for repairs.

Cyber Insurance

Cyber insurance is a type of liability insurance that protects your business against cybercrime.

A specialised **Cyber Liability** policy is the best way to protect your small business against the many risks associated with cyber-attacks.

Cyber liability is designed to cover losses suffered by third parties, but instead of covering physical damage or injury it covers losses relating to cyber incidents.

As with all insurance policies, there are exclusions that are important to understand.

Cyber Insurance policies generally, do not cover:

- potential future lost profits;
- loss of value due to theft of your intellectual property; and
- the cost to improve internal technology systems, including any software or security upgrades after a cyber event

Disclaimer: This is a summary only. For full details of the covers, limitations, exclusions and conditions contained within your policy, please read the PDS.

A03810 27/10/22 A

LUCKY YOU'RE WITH AAMI