

Cyber cover factsheet

Automatically included and providing bodies corporate with protection against social engineering.

What is social engineering?

A type of cyberfraud, social engineering involves a third party impersonating a trusted contact to trick a body corporate member into authorising payment to the wrong account.

CHU's new Cyber cover protects against loss or damage arising from social engineering fraud, provided the event relates to the body corporate's usual activities.

Who is protected by CHU's Cyber cover?

Members of the body corporate, including office bearers and committee members, and lot/unit owners.

Where in the Product Disclosure Statement (PDS) can I read more about Cyber cover?

Section 4 – Fidelity Guarantee of CHU's Residential Strata Insurance Plan has now been expanded to Section 4 – Fidelity Guarantee and Cyber.

What limits of cover are available?

Cyber cover is automatically included up to \$50,000 for any one loss during the Period of Insurance.

Is there any excess payable in the event of a claim?

If an Excess has been applied to Section 4 – Fidelity Guarantee and Cyber, this will be shown on your Policy Schedule and deducted from any claim.

Claim scenarios examples

Example 1:

A strata managing agent receives a monthly gardening invoice from ABC Building Services for a building it manages. The invoice lodged on this occasion has different bank account details from those used for historical payments.

The strata manager telephones the supplier at the contact number shown on the invoice, and the supplier confirms that the bank details are correct. Payment is made.

Sometime later, ABC Building Services chases up payment, and it becomes apparent the invoice had been intercepted by a third party, who had misdirected the funds by changing both the bank account number and contact details.

As the strata manager had established authentication procedures, the body corporate was able to make a claim under the Cyber section of CHU's insurance policy.

Example 2:

A lot owner, as per usual, receives their quarterly strata levies by email.

The lot owner manually pays their strata levies via electronic funds transfer, but doesn't notice that the bank account number has changed from the one used for previous payments.

Six weeks later, the lot owner receives a follow-up notice from the body corporate advising that their levies are overdue. They contact the strata manager to discuss, and it is discovered that the funds were transferred to an alternative account.

The lot owner has been a victim of a hacker who intercepted the strata levy notice and changed the bank account details.

The lot owner was able to make a claim on CHU's Cyber policy section.

The purpose of this document is to provide some additional information about the automatic inclusion of cyber insurance in our Residential Strata Insurance Plan PDS QM562-0526.

This document does not form part of any insurance policy and is not used in the assessment of insurance claims. Any insurance claim will be assessed against the PDS and Policy Wording policy terms and conditions and applicable law.

Please read the current PDS and Policy Wording, and Policy Schedule for full details of the terms, conditions and exclusions.

If you have any questions about these changes, please contact us at 1300 361 263 or info@chu.com.au.