Australian Government
Department of Finance

How the Comcover Statement of Cover responds to cyber security events

(current as at August 2017)

Summary

This Fact Sheet provides a summary in relation to how the *Comcover Statement of Cover 2017-18* (the Statement of Cover) may respond to cyber security related losses.

While there is no specific Cyber security section under the Statement of Cover, first and third party losses arising from an event may be covered, subject always to the terms and conditions of therein. A summary follows:

First Party Losses

A Fund Member may suffer a loss of its property as a result of a cyber security event. The following property losses may be incurred:

- loss or damage to the network, or system failure, resulting in business interruption and/or loss of revenue
- loss or damage to software or hardware
- loss or damage to data and/or records
- additional costs resulting from Business Interruption.

Depending on the particular circumstances of the property loss, coverage for first party losses may be provided under Chapter 4 'Property' (e.g. under section 8 or 11).

The value of electronic data and records should be included in the Contents column on the Fund Member's Asset Schedule located in the Gateway, which is shown on the Fund Member's Schedule of Cover.

Comcover will not cover the following first party property losses:

- denial of service attacks, including ransomware and malware
- unlawful use of data where this results in a breach of privacy.

In addition, as outlined in section 18(6) under Chapter 7 'General Exclusions' of the Statement of Cover, any losses caused directly or indirectly by erasure or corruption

of information on computer systems or other records arising from incorrect programming, punching, labelling, insertion or cancellation are not covered.

Third Party Losses

Third party losses relate to being held liable to another party for losses arising from a cyber event. For example:

- disclosure of personal information, including financial information
- disclosure of commercial information
- unauthorised disclosure of information
- defamation and infringement of intellectual property
- physical injury and/or property damage
- virus transmission.

Depending on the particular circumstances of the loss, coverage for any action taken by a third party against a Fund Member may be provided under Chapter 3 Liability (e.g. under section 6) of the Statement of Cover.

However, some exclusions may apply under the Statement of Cover, such as the following examples:

- Section 18(2)(e) under Chapter 7 ' General Exclusions' outlines that losses resulting from fines, penalties, or multiple, punitive, exemplary or aggravated damages are not covered.
- Section 18(2)(f) under Chapter 7 'General Exclusions' outlines that losses for any liability arising out of liquidated damages clauses or similar penalty clauses in contracts except to the extent that liability would have attached in the absence of such clauses are not covered.
- Section 18(2)(h) under Chapter 7 'General Exclusions' outlines that liability of your employees or officers arising from their deliberate disregard of the need to take all reasonable steps to prevent losses is not covered.
- Section 18(6) under Chapter 7 'General Exclusions' outlines that losses caused directly or indirectly by erasure or corruption of information on computer systems or other records arising from your incorrect programming, punching, labelling, insertion or cancellation are not covered.

Claims

If a Fund Member experiences a potential loss, or receives a demand for compensation from a third party as a result of a cyber security breach, it is important the Fund Member:

- take all reasonable steps to minimise any identified loss
- provide written details to Comcover as soon as possible
- not admit liability, or enter into any settlement negotiations, or incur any costs in connection with any breach without the prior written consent of Comcover
- assist Comcover in handling the claim.

For more information on claims, please refer to the Comcover website at www.finance.gov.au/comcover/claims.html.

Cyber Security Policy and Guidance

The Department of Prime Minister and Cabinet (PM&C) is responsible for leading the development of cyber security policy for the Australian Government. Information in relation to PM&C and cyber security is available at www.dpmc.gov.au/cyber-security. Fund Members are responsible for protecting their assets and information from cyber attacks. Fund Members are also responsible for ensuring their employees and officers are aware of the need to take steps to mitigate potential losses from cyber attacks, and to implement relevant policies and procedures.

The Attorney-General's Department is responsible for administering the Protective Security Policy Framework (PSPF), which provides policy, guidance and better practice advice relating to information security for Australian Government entities. Information in relation to the requirements under the PSPF is available at www.protectivesecurity.gov.au. The Department of Finance provides guidance to Commonwealth entities on cyber security requirements for business cases, available at www.finance.gov.au/policy-guides-procurement/cyber-security.

The Office of the Australian Information Commissioner (OAIC) issues guidelines to assist entities to comply with the *Privacy Act 1988*. This includes the 'Data breach notification guide: A guide to handling personal information security breaches'. Information in relation to the role of the OAIC and the guidelines issued by the OAIC are available at www.oaic.gov.au/.

Questions about Cover?

If you have any questions in relation to a claim relating to a cyber security event, please contact claims@comcover.com.au or phone the Comcover Claims Management Team on 1800 651 540 (option 1).