Australian Government
Department of Finance

Comcover Information Sheet
Cyber risk

December 2022

Cyber risk

Summary

Fund Members may be exposed to legal liability and other losses associated with cyber risks. Comcover does not have a specific cyber risk policy, however the Statement of Cover may respond to some first and third party losses arising from a cyber security event.

First Party Losses

These are losses suffered by the Fund Member directly, and include:

- physical loss or damage to the network or system, resulting in business interruption and/or loss of revenue;
- loss or damage to hardware;
- loss or damage to data and/or records; and
- additional costs resulting from business interruption, for example, costs for the temporary hire of IT hardware or the costs of using a cloud data storage service while network hardware is being restored.

Depending on the particular circumstances of the loss, coverage for first party losses may be provided under Chapter 4 - Property.

The value of electronic data and records should be included in the Contents column on the Fund Member's Assets Schedule located in the Comcover Gateway. Contact your Comcover Relationship Manager if you would like assistance with reporting this information in the Comcover Gateway.

Comcover will not cover the following first party losses:

- denial of service attacks, including ransomware and malware;
- unlawful use of data where this results in a breach of privacy; and
- any losses caused directly or indirectly by erasure or corruption of information on computer systems or other records arising from a Fund Member's incorrect programming, punching, labelling, insertion or cancellation.

Third Party Losses

These are losses where a Fund Member is held liable to another party for losses arising from a cyber event. Examples include:

- 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; and
- 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.

Comcover will not cover the following third party losses:

- fines, penalties, or multiple, punitive, exemplary or aggravated damages;
- 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;
- liability of your employees or officers arising from their deliberate disregard of the need to take all reasonable steps to prevent losses; and
- 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.

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; and
- assist Comcover in handling the claim.

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

Commercial insurance cover

If your entity requires specific cyber security insurance, you may wish to arrange cover through the commercial insurance market for cyber risk exposures that do not fit within the Comcover scheme. Fund Members can access the services of Comcover's contracted insurance broker, Arthur J. Gallagher. Please refer to 'Comcover Information Sheet – Insurance Broking Services' for more information.

Cyber Security Policy and Guidance

The Australian Cyber Security Centre (ACSC), which operates from within the Australian Signals Directorate, is responsible for providing security advice and assistance to Australian Government entities. Information in relation to ACSC is available at www.cyber.gov.au. The ACSC publishes the Australian Government Information Security Manual (ISM), which outlines a cyber security framework that entities can apply to protect their systems and information from cyber threats. The ISM is available from ACSC's website at www.cyber.gov.au/ism/using-the-australian-government-information-security-manual.

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 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 coverage for cyber risks, please contact your Relationship Manager directly.

If you do not know the Relationship Manager assigned to your entity, please call 1800 651 540 - Option 3 or email comcover@comcover.com.au.