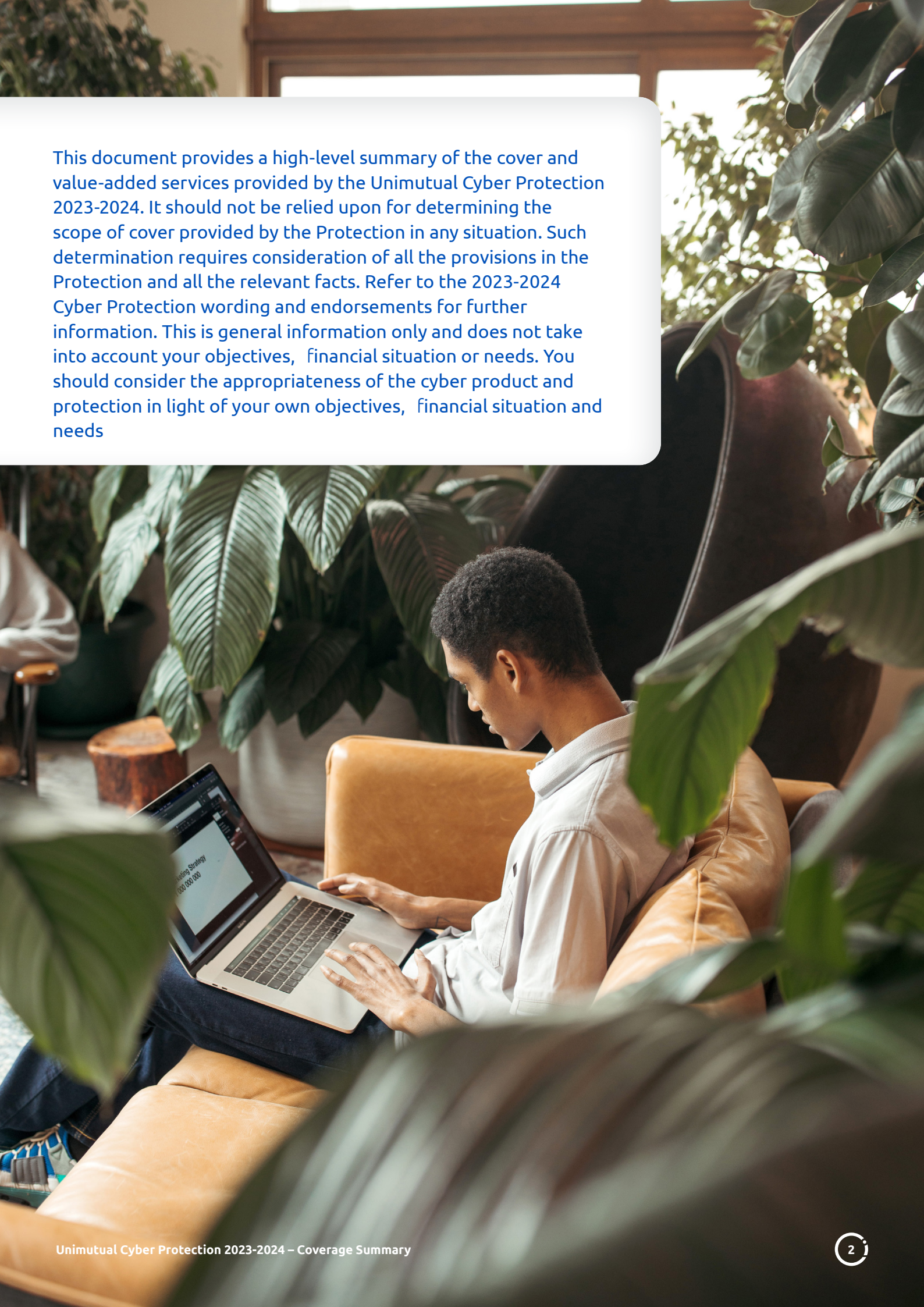
Unimutual Cyber Protection 2023-2024

COVERAGE SUMMARY

This document provides a high-level summary of the cover and value-added services provided by the Unimutual Cyber Protection 2023-2024. It should not be relied upon for determining the scope of cover provided by the Protection in any situation. Such determination requires consideration of all the provisions in the Protection and all the relevant facts. Refer to the 2023-2024 Cyber Protection wording and endorsements for further information. This is general information only and does not take into account your objectives, financial situation or needs. You should consider the appropriateness of the cyber product and protection in light of your own objectives, financial situation and needs



THIRD PARTY LIABILITY COVERAGES

1.1 **Media –** legal liability and defence costs incurred by you resulting from a claim alleging you have committed a media wrongful act (as defined in clause 7.38).

1.2 **Privacy and Security –** legal liability and defence costs incurred by you resulting from a claim alleging you have committed a privacy and security wrongful act (as defined in clause 7.54).

1.3 **Payment Card Industry Data Security Standard Liability –** fines and costs payable by you resulting from a claim alleging you have committed a PCIDSS wrongful act (as defined in clause 7.47) which has resulted in the unauthorised acquisition of cardholder data. Cover is capped at an aggregate sub-limit of $1,000,000.

1.4 **Regulatory Defence and Fines –** defence costs and regulatory fines incurred by you resulting from a regulatory investigation into a third-party wrongful act (as defined in clause 7.69) or a first party event (as defined in clause 7.30).

FIRST PARTY LOSS COVERAGES

2.1 Privacy Notification and Crisis Management Costs – reasonable and necessary costs charged by an incident response provider and incurred by you with the prior written consent of Unimutual in responding to a first party event (refer to Definition 7.53).

2.2 Betterment Costs – reasonable and necessary costs incurred by you in responding to a first party event to enhance or improve a computer system or data to the extent any increase in performance or functionality is an unavoidable consequence of restoring or replacing the computer system or data (refer to Definition 7.4).

2.3 Bricking Costs – reasonable and necessary costs incurred by you to repair or replace a computer device or IoT device which has been rendered non-functional by a first party event (refer to Definition 7.5).

2.4 Business Interruption Loss – loss of profit incurred by you for up to 365 days resulting from a network compromise which disrupts your business operations (refer to Definition 7.7).

2.5 Consequential Reputational Loss – loss of profit incurred by you for up to 365 days resulting from adverse publicity regarding an actual or alleged first party event (refer to Definition 7.14). Cover is capped at an aggregate sub-limit of $2,000,000.

2.6 Contingent Business Interruption Loss – loss of profit incurred by you for up to 365 days resulting from the computer system of your technology services provider experiencing a network compromise which disrupts your business operations (refer to Definition 7.15).

2.7 Data Recovery Costs – reasonable and necessary costs charged by a response provider and incurred by you with the prior written consent of Unimutual in restoring data that has been lost or damaged as a result of a first party event (refer to Definition 7.18).

2.8 Dependent System Failure Business Interruption Loss – loss of profit incurred by you for up to 365 days resulting from your technology services provider experiencing an unintentional and unplanned outage or failure which disrupts your business operations (refer to Definition 7.22).

2.9 Loss Mitigation Costs – costs incurred by you with the prior written consent of Unimutual in taking action to prevent or mitigate a third-party claim which could reasonably be expected to give rise to a loss covered under your Cyber Protection if such action is not taken (refer to Definition 7.34).

2.10 Operational Expenses – reasonable and necessary expenses incurred by you to reduce or avoid loss of profit resulting from a first party event which disrupts your business operations (refer to Definition 7.44).

2.11 System Failure Business Interruption Loss – loss of profit incurred by you for up to 365 days resulting from your computer system experiencing any unintentional and unplanned outage or failure which disrupts your business operations (refer to Definition 7.67).

2.12 Voluntary Shutdown Business Interruption Loss – loss of profit incurred by you for up to 365 days resulting from action taken by you to shut down your computer system to mitigate the effects of a first party event (refer to Definition 7.74).

2.13 Extortion Expenses – reasonable and necessary costs and expenses incurred by you (including costs charged by an incident response provider) in responding to an extortion demand including the reimbursement of extortion money, if legally permissible (refer to Definition 7.28).

2.14 Ransomware Event Loss – all loss, costs, fees and expenses incurred by you in connection with a ransomware event (refer to Definition 7.57). Cover is subject to the Ransomware Event Limit of Liability prescribed in your Protection Schedule.

PRE-INCIDENT SERVICES & CYBERSECURITY SOFTWARE TOOLS – NEW OFFERING

As part of our ongoing commitment to provide Members with industry leading service, Unimutual and AXA XL have partnered with expert vendors to offer Members access to discounted rates for the pre-incident services and cybersecurity software tools described below. More information about this offering, including vendor contact details and indicative pricing will be provided in due course.

Pre-Incident Services	Service Providers	
Cyber Incident & Data Breach Response Plans	Clyde & Co	Wotton + Kearney
Cybersecurity & Privacy Health Check	Clyde & Co	Wotton + Kearney
Tabletop Training	Clyde & Co	Wotton + Kearney
Data Retention & Destruction Policy	Clyde & Co	Wotton + Kearney
Communication Playbooks	Clyde & Co	Wotton + Kearney
Ransomware Decision Making Frameworks	Clyde & Co	Wotton + Kearney

Cybersecurity Software Tools	Service Provider
Extended Threat Detection and Response	Secureworks
Managed Detection and Response	Secureworks
Vulnerability Detection and Response	Secureworks
Active Directory Security Assessment	Secureworks
Threat Hunting Assessment	Secureworks
Threat Briefing	Secureworks
Penetration Testing	Secureworks
Office 365 Control Review	Secureworks

POST-INCIDENT RESPONSE SERVICES

A key benefit of your Unimutual Cyber Protection is access to an incident response service, provided by pre-approved expert service providers at discounted rates.

If you are experiencing a cyber incident, you are able to contact the **AXA XL Cyber Incident Breach Response Service on 1800 466 380** which is monitored 24/7 by Crawford & Company. Crawford will act as your incident response manager putting you in touch with service providers who will assist you in responding to the incident and getting your business back up and running as quickly as possible.

Refer to the protection endorsements for more details about this service including a list of the service providers. The cost of this service is covered under your Unimutual Cyber Protection. The available services include:

- IT forensics
- Incident response
- Legal advice and support
- Regulatory notifications
- Forensic accountancy
- Cyber extortion management and payment
- Public relations
- Identity protection and credit monitoring
- Public notifications including call centre operations

UNIMUTUAL BENEFITS & SERVICES

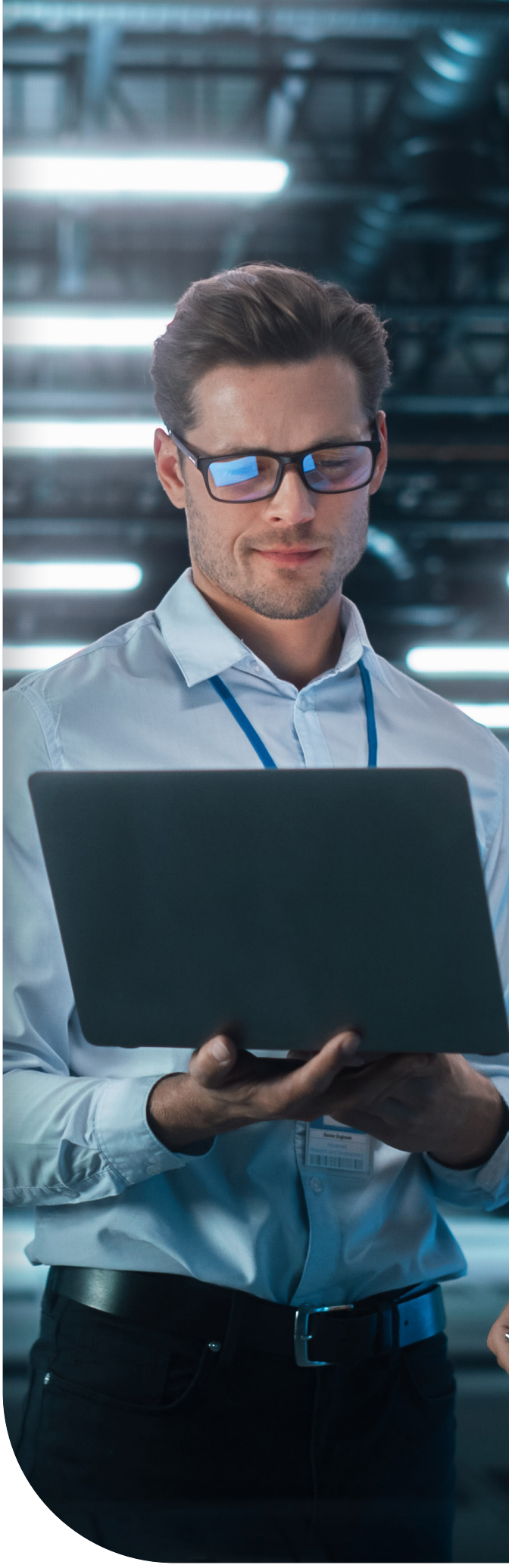
What makes the Unimutual Cyber Protection different?

The Unimutual Cyber Protection provides market leading coverage including some areas of cover that are not generally available from the market such as:

- **Multiple triggers** for business interruption loss including:
  - computer system failure of a technology service provider
  - computer system compromise of a technology service provider
  - voluntary computer system shutdown
- All business interruption covers apply for up to 365 days.
- **Betterment –** enhancements and improvements of computer systems to the extent an increase in performance is an unavoidable consequence of recovery.
- **Bricking –** costs of repairing or replacing damaged hardware.
- **Loss Mitigation –** costs incurred in taking action for the sole purpose of avoiding or mitigating a third-party claim that would be covered under the Protection.
- **Ransomware –** full limit cover provided you have the minimum level of controls.
- **Reputational loss –** $2.,000,000 of cover for loss of profit caused by adverse publicity.
- **Broad privacy and security coverage** which includes confidential business information in addition to personally identifiable information and protected health information.
- **Broad privacy regulatory coverage**, including fines and penalties where insurable by law, arising from a privacy or security wrongful act, media wrongful act or PCIDSS wrongful act.

In addition to this market leading coverage, the Unimutual Cyber Protection provides Members with access to:

- **Pre-Incident Services & Cybersecurity Software Tools** provided by best-in-class service providers at discounted rates (as described above).
- **Post-Incident Response Services** provided by best-in-class service providers at discounted rates (as described above).



Unimutual Limited
Suite 11.02, Level 11,
56 Pitt Street, Sydney NSW 2000

Phone: (02) 9169 6600
Email: service@unimutual.com.au
Website: www.unimutual.com

ABN: 45 106 564 372
AFS Licence No: 241142

ADMKR-000321_UCP23.02