emergence

smarter cyber insurance

Summary of Key Changes - Cyber Event Protection Policy

Summary of Key Changes from EME CEP-003.1 to EME CEP-004

This document provides a brief summary of changes to the Emergence Cyber Event Protection policy. It follows the sectional layout of the policy. It is not an exhaustive summary, nor does it form part of the policy wording. Emergence policies are available on the Emergence website: **emergenceinsurance.com.au**

Please read the policy wording in its entirety for full details of cover and to ensure it meets your requirements.

Section A – Losses To Your Business

Policy Reference	Description
"Section A – Losses To Your Business"	*Additional coverage provided for preventative shutdown as follows* If a **preventative shutdown** happens during the **policy period**, **we** will pay **you** a **preventative shutdown allowance**.

Section D – Optional Covers

Policy Reference	Description
"Section D - Optional Covers – Contingent Business Interruption Cover"	*Contingent Business Interruption cover has now been split into "supplier outage" or "system failure" Additional coverage is now provided for "system failure".* *The waiting period has been shortened to 72 hours.* **We** will pay **you impact on business costs** caused by: a. **supplier outage**, or b. **system failure**. For the purpose of this Optional Cover – Contingent Business Interruption Cover only the words listed below have been given a specific meaning and the specific meanings apply: **cyber event** is extended to include a **cyber event** at **your** direct external supplier's business. **Impact on business costs** means: a. the amount that the **revenue you** earn during the **indemnity period** falls short of the **revenue you** ordinarily earn directly as a result of a **supplier outage** or a **system failure**, less any consequent savings, and

b. the net increased costs incurred to avoid a reduction in **revenue** directly as a result of the interruption to **your business** provided
the amount of increased cost paid is less than **we** would have paid for a reduction in standard **revenue** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries or overhead expenses.

The amount is calculated by reference to the **records of your business** and any other documents that **we** request. **Impact on business costs** do not include **cyber event response costs**. **We** will not pay any **impact on business costs** incurred under this Optional Cover – Contingent Business Interruption Cover during the waiting period of three days (72 hours) after the first interruption to **your business**.

indemnity period is amended and means the continuous period starting from the first interruption to **your business** until:

a. supply from **your** direct external supplier resumes, or until **you** have a substitute supply (in the case of **supplier outage**), or
b. the outage is sufficiently restored to support **your** usual **business** operations (in the case of **system failure**)

plus reasonable additional time to allow **your business** and **revenue** to normalise. The **indemnity period** shall not exceed a total length of 35 days.

supplier outage means an interruption to **your business** directly arising from an outage at **your** direct external suppliers' business, where, in **our** opinion, the outage has been caused by a **cyber event** at **your** direct external supplier's business.

system failure means an interruption to **your business** directly arising from an unintentional, unexpected and unplanned outage of **your IT infrastructure** or **IT infrastructure** under the direct control of **your IT contractor**, but does not include outage:

a. caused by a **cyber event**;
b. caused by using untested, disapproved or illegal software, or software that is past its end-of-life and no longer supported;
c. caused by use of a non-operational part of **your IT infrastructure**;
d. falling within parameters of a service level agreement;

e. arising out of commercial dispute, failure to pay for services or refusal to deliver services paid for; or

f. arising out of physical cause or natural peril, such as fire, wind, water, flood, lightning, explosion, collision, subsidence, earthquake, or any other act of God.

Policy Reference	Description
"Optional Cover – Criminal Financial Loss Cover"	*Item c. identity-based theft has been added to the Criminal Financial Loss cover.* **We** will pay a **direct financial loss** to **you** or a **direct financial loss** to others directly arising out of: a. **cyber theft**; b. **socially engineered theft**; c. **identity-based theft**; d. **telephone phreaking**; or e. **cryptojacking** that is first discovered by **you** and notified to **us** in the **policy period**.
Optional Cover – Tangible Property Cover	*Clarification that cover extends to IT hardware if it becomes "no longer suitable for use".* **We** will pay the cost of the replacement or repair of **your** IT hardware that is physically damaged or no longer suitable for use solely and directly because of a **cyber event** covered under this **policy** or the incurring of related **cyber event response costs**.

Section E – What Certain Words Mean

Policy Reference	Description
"aggregate" definition	*New definition added to wording. No change in intention, more clearly expressed.* **aggregate** means the most **we** will pay, including **defence costs**, in any one **policy period** for all **cyber events**, **losses**, **claims**, **preventative shutdown allowance**, **investigation costs** or **direct financial loss** for all insureds, under Sections A - Losses To Your Business,

	Section B – Loss To Others and Section C – Cyber Event Response Costs and any Optional Covers taken out by **you**. The **aggregate** is stated in **your schedule**.
cyber event – definition of "cyber extortion"	*Definition now includes cover for extortion based on data.* **cyber extortion** which is a crime involving an attack or threat of attack against **your IT infrastructure**, or data in **your IT infrastructure**, coupled with a demand for money or other valuable consideration (including digital currency) to avert or stop the attack.

Policy Reference	Description
Cyber event – new cover and definition for "privacy error"	*New cover and definition added.* **privacy error** where acts or omissions by **your** employees lead to unauthorised access to, unauthorised disclosure of or loss of data (including non-electronic data) which necessitates incurring **notification costs** or **identity theft response costs**.
Cyber event response costs – new definition for "identity theft response costs"	*New cover provided as follows.* **identity theft response costs** incurred in supporting an individual with reporting of the **identity theft** and re-establishing identity and essential records.
New definition – "Identity-based theft"	*New definition added.* **Identity-based theft** means an **identity theft** that happens without the individual's knowledge and results in **direct financial loss** to the individual. **Identity-based theft** does not include **cyber theft** or **socially engineered theft**.
New definition – "Identity theft"	*New definition added.* **identity theft** means the unauthorised use of the identity of an individual whose data or information has been accessed because of a **cyber event** that happens to **your IT infrastructure**. **Identity theft** does not include **identity-based theft**.
Amended Definition of "impact on business cost"	*Definition has been updated.* **impact on business costs** means: a the amount that the **revenue you** earn during the **indemnity period** falls short of the **revenue you** ordinarily earn directly as a result of a **cyber event**,

less any consequent savings, and

b. the net increased costs incurred to avoid a reduction in **revenue** directly as a result of a **cyber event** provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **revenue** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries or overhead expenses.

impact on business costs do not include **cyber event response costs**.

The amount is calculated by reference to the **records of your business** and any other documents that **we** request. **We** will not pay **impact on business costs** incurred during the waiting period of the first 12 hours after **you** discover a **cyber event** unless a different waiting period has been specified on **your schedule** or unless the first discovery of the **cyber event** occurred during a **preventative shutdown**.

Policy Reference	Description
New Definition for "preventative shutdown"	*New definition added for preventative shutdown.* **Preventative shutdown** means the reasonable, necessary and intentional shut down of **your IT infrastructure** in response to a **cyber event** in **your business**, or a credible threat to **your IT infrastructure** following: a. a **cyber event** at **your** direct customer, supplier or business partner, b. specific instruction from your financial institution, law enforcement or the Australian Signals Directorate or similar agency of the government, or c. communication by a third party threatening to carry out **cyber extortion**, a **denial of service** attack or other **cyber event** against **your business** and where such shutdown will mitigate the threat or avoid otherwise larger claims under this **policy**. **Preventative shutdown** does not include shutdown due to routine maintenance, patching or updating of software, use of software that is past its end-of-life and no longer supported or for any reason other than mitigation of threat to **your IT infrastructure**.
New Definition for "preventative shutdown allowance"	*New definition added for preventative shutdown allowance.* **Preventative shutdown allowance** means a. the amount that the **revenue you** earn during the **preventative shutdown** falls short of the **revenue you** ordinarily earn directly as a result of the **preventative shutdown**, less any consequent savings, and

Policy Reference	b. the net increased costs incurred to avoid a reduction in **revenue** directly as a result of a **preventative shutdown** provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **revenue** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries or overhead expenses. c. Reasonable and necessary costs **we** agree to for an independent security audit to assess the threat to **your IT infrastructure**. **Preventative shutdown allowance** does not include **cyber event response costs** or **impact to business costs**. **Preventative shutdown allowance** does not include the cost for **you** to implement critical security audit recommendations or other measures as required to mitigate the threat. The amount is calculated by reference to the **records of your business** and any other documents that **we** request. **We** will not pay **preventative shutdown allowance** during the waiting period of the first 12 hours after **you** initiate a **preventative shutdown** unless a different waiting period has been specified on **your schedule**. The **excess** does not apply to the **preventative shutdown allowance**. **We** will pay a **preventative shutdown allowance** for up to a maximum of 48 consecutive hours after the waiting period and ending at the earlier of: a. first discovery of the **cyber event** affecting **your IT infrastructure**; or
Description	b. the safe resumption of operations of **your IT infrastructure**. The **preventative shutdown allowance** is set out in **your schedule** and is the maximum **we** will pay for all **preventative shutdowns** in any one **policy period**. It is included in and forms part of the **limit** for Section A – Losses To Your Business.
New Definition for "records of your business"	*New definition added for records of your business.* **records of your business** means all documents that evidence **your revenue**, including **your** bank records, GST records, tax records and usual business records including records that evidence **your** expenditure and outgoings.
Amended definition for "socially engineered theft"	*Definition amended to clarify that transfers must be business related ("in connection with your business").* **socially engineered theft** means an electronic transfer to an unintended third party that results in **direct**

	financial loss. The transfer must be made in connection with **your business** by **your** employee in good faith, in reliance upon intentionally misleading material facts communicated through **your IT infrastructure**, having believed such facts to be genuine and true. **Socially engineered theft** does not include **cyber theft**.
Amended definition for "you/your"	*The definition has been amended to accommodate cover for declared affiliates.* **you/your** means the **policyholder** referred to in **your schedule**. It includes **your subsidiaries**, any affiliates stated in **your schedule**, and any current, future or former employee for work performed in connection with **your business**, including directors and officers, or partners if **you** are a partnership. In the event of **your** death, incompetence or bankruptcy, if **you** are a natural person it also includes **your** estate, heirs, legal representatives or assigns for **your** legal liabilities.

Section F - Exclusions

Policy Reference	Description
Exclusion 19.	*Refinement of exclusion to accommodate expanded Criminal Financial Loss cover.* 19. arising from, attributable to, or as a consequence of **cyber theft, socially engineered theft, identity-based theft, telephone phreaking** or **cryptojacking**. This exclusion does not apply to **cyber event response costs** incurred solely and directly due to **cyber theft, identity-based theft, telephone phreaking** or **cryptojacking**.

Section G – Claims Conditions

Policy Reference	Description
Condition 4.	*Amended cover assessment condition* 4. **We** will assess whether cover applies under **your policy**. **We** may at our discretion appoint a forensic investigator to assist **us** determine if there is **cyber event** and assess whether cover applies under **your policy**. If **we** do not appoint a forensic investigator **you** can with **our** prior consent and approval appoint a forensic investigator. The costs of the forensic investigator are included in the **limit** that applies to the **cyber event**.
Condition 10.	*New condition introduced with respect to Payment Card Industry Liability* 10. **We** may at **our** own discretion appoint an auditor to review and audit any **Payment Card Industry Liability**.
Condition 16.	*New condition with respect to cyber theft, socially engineered theft or identity-based theft with respect to payments and recoveries* 16. If **you** suffer a **direct financial loss** as a result of **cyber theft**, **socially engineered theft** or **identity-based theft we** can at **our** discretion and if the funds remain unrecoverable pay the claim within 30 days of the claim being notified to **us**. If **we** do elect to pay the claim, **you** must cooperate with and assist **us** in **our** attempts to recover **your direct financial loss**. If the funds are recovered and paid into **your** own account, **you** must immediately advise **us** and repay to **us** the funds recovered.

Section H – General Conditions

Policy Reference	Description
Condition 14.	*Relocated from Section G – Claims Conditions to Section H – General Conditions* 14. If **you** report a **cyber event** or **claim** to **us** and either, or all, of **impact on business costs**, a **loss**,

	cyber event response costs, or **direct financial loss** are incurred then **we** will apply the **aggregate** and **excess** set out in **your schedule** as if one **cyber event** happened.
Condition 15.	*New* *15.* All reported incidents and claims which arise out of one **cyber event** or a series of **cyber events** involving **your IT infrastructure** or **business** will be deemed to be one **cyber event** and only one **aggregate** will apply.
Condition 16.	*New* 16. The notification to **us** of an incident or claim under one section of this **policy** will be deemed a **notification to us** under each section of the **policy** or any Optional Cover.

Emergence Insurance Pty Ltd (ABN 46 133 037 153, AFSL 329634) ('Emergence') acts under a binding authority given to it by certain Underwriters at Lloyd's.

More information on Emergence can be found on our website: **emergenceinsurance.com.au**