360 Cyber Policy Wording – Summary of Changes 31 January 2023

The 360 Cyber Policy is underwritten by certain Underwriters at Lloyds (Lloyd's). Lloyd's have amended the cover of the policy, by way of a contract endorsement to the Coverholder Agreement between 360 Financial Lines Pty Ltd (360 Cyber) and Lloyd's. 360 Cyber issue the policy on behalf of Lloyd's in its capacity as a Lloyd's coverholder, pursuant to that Coverholder Agreement.

As Lloyd's have changed the cover of the policy, 360 Cyber have updated the 360 Cyber Policy Wording to reflect this change. This document is designed to provide a summary of the significant differences between the previous 360 Cyber Policy Wording (version 360CYPWV722 with an Effective Date of 1 April 2022) and the new Wording (version 360CYPWV823 with an Effective Date of 31 January 2023).

The information contained in this document is general product information only. It does not constitute financial product advice (personal or otherwise) and should not be relied on as such. This document does not form part of the policy and is a summary of certain terms only. For the full terms, conditions, and exclusions of the policy, please refer to the current 360 Cyber Policy Wording. If your client enters unto a policy with us, their policy schedule will also form part of the terms and conditions of cover.

ITEM	PREVIOUS TERMINOLOGY	NEW TERMINOLOGY	WHERE DO I FIND IT
General Exclusions			
Item 5	"We shall not be liable to make any payment in respect of: .... 5. Or arising from any physical act of war, invasion, or warlike operations, civil war, riot, civil commotion, rebellion, revolution, insurrection or civil uprising"	"The insurer shall not be liable to make any payment or provide any benefit or service in respect of any claim, loss, damage, liability, cost or expense of any kind: …. 5. Arising directly or indirectly occasioned by, happening through or in consequence of **war**[1] or a **cyber operation**. The **insurer** shall have the burden of proving this exclusion applies. Attribution of a **cyber operation** to a **state** shall be determined as follows: a. The primary but not exclusive factor in determining attribution of a **cyber operation** shall be whether the government of the **state** (including its intelligence and security services) in which the **computer system** affected by the **cyber operation** is physically located attributes the **cyber operation** to another state or those acting on its behalf; b. Pending attribution by the government of the **state** (including its intelligence and security services) in which the **computer system** affected by the **cyber operation** is physically located, the **insurer** may rely upon an inference which is objectively reasonable as to attribution of the **cyber operation** to another **state** of those acting on its behalf. It is agreed that during this period no loss shall be paid; c. In the event that the government of the **state** (including its intelligence and security services) in which the **computer system** affected by the **cyber operation** is physically located either: + takes an unreasonable length of time to; or + does not; or + declares it is unable to. Attribute the **cyber operation** to another **state** or those acting on its behalf, it shall be for the **insurer** to prove attribution by reference to such other evidence as is available.	Page 11 **General Exclusions**

1 Please note that all word/phrases in bold are defined in the current 360 Cyber Policy Wording. Please refer to the definitions in the current 360 Cyber Policy Wording to fully understand the quoted term of the policy.