

# A summary of the key changes to Your Cyber Complete Policy



Changes to your policy you need to know about before you renew.

This notice tells you about the changes to your policy which will take effect from your renewal date as shown on your schedule. Please ensure you read the changes carefully (together with your policy wording), as they will form part of your contract of insurance, and keep them together with your other policy documents.

## Product Name Change:

- **Cyber Complete**

We've recently expanded the number of cyber products we are able to offer our commercial customers. In order to provide clarity on the product you have chosen, we've renamed our existing 'Cyber' product to 'Cyber Complete'. There are no changes to the level of cover provided within your policy and you do not need to take any action.

## Statement of Fact

- **General Details - Sanctions**

Please note that We have updated the General Details section of the Statement of Fact document to include statements relating to sanctions. Please read and check the Statement of Fact to ensure The Business complies with these statements. Should there be any concerns or queries with the ability of The Business to comply with the updated Statement of Fact, please contact Your insurance adviser in the first instance.

- **Cyber Security - Virus or Similar Mechanism**

This statement has been changed to align with Your Policy Condition, Protection - Virus or Similar Mechanism. This is to provide consistency across Your documentation. The amended statement now reads:

Your Computer equipment and any personal devices used for accessing your computer systems must have effective and up to date anti-virus software that's updated at least once a month.

- **Cyber Security - Firewall**

This statement has been changed to align with Your Policy Condition, Protection - Firewall. This is to provide consistency across Your documentation. The amended statement now reads:

Your Computer Equipment is protected from unauthorised access by an active firewall.

- **Cyber Security - Software Updates**

You may not have seen this in last years Statement of Fact, in order to align with Your Policy Condition, Protection - Software Updates, this will now display. The statement reads:

Updates to firewalls, firmware, operating systems and software are completed within 14 days from release where they are addressing vulnerabilities:

- with a severity that the provider has described as critical, important or high, or
- with a Common Vulnerability Scoring System (CVSS) v3 score of 7 or above.

- **Cyber Security - External Cyber Crime**

You may have seen this in last years Statement of Fact, in order to align with Your Policy Conditions, this has now been amended to only display when 'External Cyber Crime' is selected. The statement reads:

You have a documented policy, which states that details of any new payee requests or amended payment instructions are always checked verbally by using details held on file or a published website and do not solely rely on the new instruction. You stipulate that this policy must be accepted by all Partners, directors and Employees, and such acceptance is recorded.

# Definitions

## • **Cyber Operation**

This is a new definition:

The use of any Computer Equipment by, on behalf of, or in support of a sovereign state to disrupt, deny, degrade, exfiltrate, manipulate or destroy any data or Computer Equipment in or of another sovereign state.

## • **Cyber Terrorism**

This definition no longer includes infrastructure, the Internet, the intranet and telecommunications. The definition now reads as follows:

Any act or series of acts or threat thereof of any person or group of persons, whether acting alone or on behalf of or in connection with any organisation through the use of computer systems, to destruct, disrupt or subvert any computer system, computer network and/or its content, with the intention to cause harm or committed for religious, ideological or political purposes (including, but not limited to, the influencing of any government and/or to put the public in fear).

## • **Designated Official**

This is a new definition:

Any person holding one of the following positions, or equivalent, within a sovereign state

- (a) Head of government
- (b) Interior minister
- (c) Foreign minister
- (d) Defence minister
- (e) Official representative of a national intelligence or security service

## • **Essential Service**

This is a new definition:

A service which is essential for the maintenance of critical societal or economic activities of a sovereign state including but not limited to financial institutions and associated financial market infrastructure, transport network, health services or utility services.

## • **Relevant State**

This is a new definition:

Any sovereign state

- (a) in which the Data or Computer Equipment affected by a Cyber Operation is physically located or stored
- (b) which is a permanent member of the United Nations Security Council
- (c) which is a member of the Five Eyes intelligence alliance
- (d) which is a member of the North Atlantic Treaty Organisation.

## • **The Defined Territories**

The following definition has been updated to remove reference to 'or offshore installations within the Continental Shelf around such territories' and is restated as follows;

Great Britain, Northern Ireland, the Channel Islands or the Isle of Man.

## Policy Conditions

### • Data Backup

This Condition has been extended to give clarity on data backups. The amended Condition now reads:

You must maintain adequate backup copies by backing up all data no less frequently than every 7 days. The integrity of any data backup must be validated using operating system routines or checks.

Backups must be stored securely and separately from the original data or programs by

- (a) holding a copy offline, such as backup tape or disconnected service such as a USB device or external hard drive; or
- (b) using a specific cloud service that is separate from your main network; or
- (c) replicating to another of your networks that is separated and disconnected from your main network.

### • Data Disposal (formerly Data Storage)

This Condition has been extended to give clarity on the disposal of Data. The amended Condition now reads:

All Personal Data and other sensitive business Data must only be disposed of in a secure manner by

- (a) shredding any paper copies
- (b) ensuring any Computer Equipment has all Data erased before disposal.

### • External Cyber Crime

This Condition has been changed to give additional clarification on the processes You should have in place in Your business for all payments and the steps that need to be taken to make sure everybody knows such processes.

The amended Condition now reads:

You must

- (a) ensure that Partners, directors and Employees are trained in the dangers of Social Engineering Fraud, and keep a record of such training
- (b) have a documented policy, which states that details of any new payee requests or amended payment instructions are always checked verbally by using details held on file or a published website and do not solely rely on the new instruction. This policy must be accepted by all Partners, directors and Employees, with such acceptance recorded.

### • Protection - Firewall

This Condition has been changed to remove the need for monthly updates under this condition. However, you must continue to carry out software updates as described in the Protection- Software Updates Condition. The amended Condition now reads:

‘You must ensure that Computer Equipment that is connected to the internet or any other external network is protected against unauthorised access by an active firewall.’

### • Protection - Software Updates

This Condition has been changed to give clarity on addressing software vulnerabilities. The amended Condition now reads:

You must install any updates for firmware, operating systems, software and programs within 14 days of an update being released by the manufacturer or provider where:

- (a) the update fixes or vulnerabilities described by the vendor as ‘critical’ or ‘high risk’, or
- (b) the update addresses vulnerabilities with a Common Vulnerability Scoring System (CVSS) v3 score of 7 or above.

## Exceptions

### • Terrorism

We have added additional language, bullets (iv) and (v), to it make clear that Cyber Terrorism does not include war or a Cyber Operation. Please refer to the Cyber Terrorism Definition for additional information.

- (3) any Damage, or the threat thereof, or any consequence resulting directly or indirectly from or in connection with any of the following regardless of any other cause or event contributing concurrently or in any other sequence to the loss
  - (a) Terrorism
  - (b) civil commotion in Northern Ireland
  - (c) any action taken in controlling, preventing, suppressing, or in any way relating to (a) and/or (b) above

In any action, suit or other proceedings where We allege that any Damage, or the threat thereof, or any consequence whatsoever results from 3(a) and/or (3)(b) and/or (3)(c) and is therefore not covered by this Section, the burden of proving that any such Damage, or the threat thereof, or any consequence whatsoever is covered under this Section will be upon You.

However We will provide cover for Cyber Terrorism as insured by this Section other than in respect of Damage which results directly from

- (i) fire, explosion, flood, escape of water from any tank, apparatus or pipe (including any sprinkler system),
- (ii) impact of any aircraft or any aerial devices or articles dropped from them,
- (iii) impact of any sea-going or water-going vessel or of any vehicle whatsoever or of any goods or cargo carried in or on such vessel or vehicle
- (iv) war, invasion, act of a foreign enemy, hostilities or a warlike operation or operations (whether war be declared or not), civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power
- (v) a Cyber Operation

#### • **Infrastructure**

Exception (16) has been restated as:

- (16) any loss or liability arising directly or indirectly out of any failure, interruption, disturbance, degradation, corruption, impairment or outage of any utility provider, internet service provider, telecommunications provider, domain name service, certificate authority or content delivery network. However, We will cover Your direct losses if such services are under Your direct operational control.

#### • **Cyber Operation**

A new Exception(23) has been added to Your policy:

- (23) any loss or liability arising directly or indirectly out of a Cyber Operation that has a major detrimental impact on
  - (a) the functioning of a sovereign state due to disruption to the availability, integrity or delivery of an Essential Service in that sovereign state; or
  - (b) the security or defence of a sovereign state

If a Designated Official of a Relevant State attributes a Cyber Operation to another sovereign state, or asserts that a Cyber Operation has been carried out on behalf of or in support of a sovereign state, then for the purposes of this exception, a Cyber Operation shall be deemed to have taken place, and this exception will apply. A Cyber Operation shall still be deemed to have taken place and this exception will still apply if any other sovereign state, including (without limitation) a Relevant State, contradicts or denies the attribution or assertion.

In the absence of attribution or assertion by a Designated Official of a Relevant State We will be entitled to apply this exception in reliance on any reasonable inference as to the attribution of the Cyber Operation to another sovereign state or to anyone acting in support of or on behalf of a sovereign state.