Endorsement – IMIA Advanced Cyber Exclusion 2018

Notwithstanding any provision to the contrary within this Policy or any endorsement thereto, it is understood and agreed as follows:

1. Any loss, damage, liability, costs or expenses directly or indirectly caused by or contributed to or resulting from the cyber incidents as set forth in the following provisions a) to g) are not covered by this Policy, regardless of any other cause or event contributing concurrently or in any other sequence to the loss, damage, liability, costs or expenses:

   a) **Damage to or Loss of Data** occurring on the **Insured's Computer Systems**, or

   b) a **Computer Malicious Act** on the **Insured's Computer Systems**, or

   c) **Computer Malware** on the **Insured's Computer Systems**, or

   d) a **Human Error** affecting the **Insured's Computer Systems**, or

   e) a **System Failure** occurring on the **Insured's Computer Systems**, or

   f) a **Defect** of the **Insured's Computer Systems**, or

   g) a **Cyber Extortion**.

2. Where this Cyber Exclusion is endorsed on policies covering risks of war or terrorism this Cyber Exclusion shall also exclude **Cyber Terrorism** or **Cyber War** according to **Clause 1** above.

3. The Insurer's obligation to indemnify the Insured in accordance with this Policy is subject to the Insured's fully compliance with all of the following conditions:

3.1 In case of any loss event that might give rise to a claim under the Policy, the Insurer or an **Expert**, agent or a representative of the Insurer may, at any reasonable time, inspect and examine the Insured's premises, the Insured Property, the **Insured's Computer Systems**, and the Insured's **Computer Networks** in order to conduct claims handling. The Insured shall - at the Insurer's expenses - in a timely manner provide the Insurer or an **Expert**, agent or a representative of the **Insurer** with all relevant details and information that may be required by the **Insurer** for its claims handling. Additionally, the **Insured** shall - as far as possible - ensure that the **Insurer** or an **Expert**, agent or a representative of the **Insurer** is allowed to inspect the **Computer Systems** operated for the Insured of any **Outsourcing Provider** of the Insured if such an inspection is required to conduct claims handling.

3.2 Upon the occurrence of any loss event that might give rise to a claim under this Policy, the Insured shall

3.2.1 cooperate at all times with the Insurer or an **Expert**, agent or a representative of the Insurer with regard to the loss event that might give rise to a claim under this Policy;

3.2.2 do and permit to be done anything that is reasonably necessary to support the Insurer or an **Expert**, agent or a representative of the Insurer in order to establish the cause and extent of the loss or damage resulting from the loss event that might give rise to a claim under this Policy;

3.2.3 preserve any hardware, software and **Data** which may be affected by the loss event that might give rise to a claim under this Policy and make them available for inspection by the Insurer or an **Expert**, agent or a representative of the Insurer as long as required by them;

3.2.4 furnish any information, reports, materials, **Data** and documentation that the **Insurer** or an **Expert**, agent or a representative of the Insurer may require to deal with the claim; and

3.2.5 support the Insurer or an **Expert**, agent or a representative of the Insurer in any forensic investigation of the cause of the loss event that gives rise to the claim under this Policy and in any preparation of the documentation of the results.

3.3 The Insurer shall ensure that all information obtained by the Insurer, the **Expert**, agent or a representative of the Insurer according to **Clause 3.1** and **Clause 3.2** will be kept confidential and shall only be used by the Insurer as any other information provided by the Insured for its claims handling and claims management.

4. The boldfaced, capitalized terms used in this Cyber Exclusion Endorsement shall have the following meanings and the singular shall include the plural and vice versa:

Computer Malicious Act
Means any wrongful act carried out through the use of **Data**, **Computer Systems** or **Computer Networks**. The term **Computer Malicious Act** shall also encompass a **Denial of Service Attack.**

Computer Malware
Means any hostile or intrusive software, including computer viruses, spyware, computer worms, trojan horses, rootkits, ransomware, keyloggers, dialers, spyware, adware, malicious browser helper objects and rogue security software**,** designed to infiltrate and disrupt computer operations, gather sensitive information, or gain access to **Computer Systems** without consent.

Computer Network
Means a group of **Computer Systems** and other computing hardware devices or network facilities connected via a form of communications technology, including the internet, intranet and virtual private networks (VPN), allowing the networked computing devices to exchange **Data**.

Computer Systems
Means the Information Technology (IT), industrial process control or communications systems, as well as any other item or element of hardware including and IT infrastructure, software or equipment that is designed to be used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting **Data**. The term **Computer Systems** shall also include IT devices such as laptops, external drives, CD-ROMs, DVD-ROMs, magnetic tapes, magnetic disks or USB sticks that are used in **Data** processing to record and store **Data**.

Cyber Extortion
Means any unlawful and intentional use of a threat or series of threats by an extortionist against the **Data** on an **Insured's Computer Systems** or against the **Insured's Computer Systems** (e.g. **Denial of Service Attack**) in order to extract a **Cyber Extortion Ransom** from the Insured by use of coercion.

Cyber Extortion Ransom
Means anything of value, including money, or other property or services that the Insured is forced to pay or to provide to the extortionist or any other party.

Cyber Terrorism
Means any disruptive act or series of disruptive acts or threat thereof of any person or group of persons, whether acting alone or on behalf of or in connection with any organization through the use of **Computer Systems**, to destruct, disrupt, subvert or make use of any **Computer System**, **Computer Network**, IT infrastructure, the internet, the intranet, telecommunications and/or its content, committed for religious, ideological or political purposes including but not limited to the influencing of any government and/or to put the public or a section of the public in fear.

Cyber War
Means any state of hostile conflict (whether declared or not) to resolve a matter of dispute between two or more states, nations, or political entities or organisations by using - wholly or partially - **Computer Systems** or the internet, to render non-functional, disrupt, subvert or make disruptive use of any **Computer System**, **Computer Network**, IT infrastructure, the internet, the intranet, telecommunications and/or its content.

Damage to or Loss of Data
Means any introduction, corruption, creation, modification, redirection, alteration or deletion of **Data** which, when stored or processed by a **Computer System**, may lead to an impaired, corrupted or abnormal functioning of the **Computer Systems** and/or the interruption or disruption of processing operations.

Data
Means any information, irrespective of the way it is used or rendered including text, figures, voice, images or any machine readable data and including software or programs, that are being transmitted or are stored in a digital format outside the random access memory.

For the avoidance of doubts the term **Data** shall not be considered as tangible property and shall not be covered under this Policy.

Denial of Service Attack
Means any malicious attack leading to a total or partial deprivation, disruption and/or unavailability of **Computer Systems** or **Computer Networks** being altered or rendered temporarily or permanently non-functional or otherwise unavailable to anticipated users of such **Computer Systems** or **Computer Networks** through the deluging and overloading of **Computer Systems** with an incoming stream of requests or **Data**. The term **Denial of Service Attack** includes a distributed denial of service attack in which a multitude of compromised systems are used to coordinate a simultaneous attack as well as both volumetric and application specific attacks.

Defects
Means any fault, defect, malfunction, error or omission in design, plan, specification, material or programming on or of the **Insured's Computer Systems**.

Employee
Means any natural person that performs services or provides labour in the service and on the premises of the **Insured** under an express or implied employment contract, under which the Insured has the right to control the details of work performance. The term **"Employee**" shall also include external staff hired by the Insured in order to provide IT services working within the operational structure and under the functional authority of the Insured.

Expert
Means any person with a high degree of skill in or knowledge of a certain subject, including but not limited to IT specialists, lawyers, consultants or auditors.

Human Error
Means any negligent or inadvertent IT or OT (Operational Technology) operating error, including an error in the choice of software to be used, a set-up error or any improper IT or OT operation carried out by an **Employee** of the Insured.

Insured's Computer Systems
Means (i) any **Computer Systems** under the control and management of the Insured that are owned, licensed or hired by the Insured or (ii) any **Computer Systems** under the control and management of the **Outsourcing Provider** that are owned, licensed or hired by the **Outsourcing Provider** or the Insured or (iii) any **Computer Systems** under the control and management of a customer or supplier of the Insured that are owned, licensed or hired by the customer or supplier of the Insured. The aforementioned term "supplier" shall also include any electricity, cable, satellite, GPS signal generation, propagation or reception, telecommunication or internet provider.

Outsourcing Provider
Means any IT service provider that is assigned by the Insured by written contractor by written contracts ultimately authorized by the Insured to offer IT services including **Data** or **Computer System** management, **Data** storage and **Data** processing, software maintenance and/or development for the benefit of or at the request of the Insured on a **Computer System** that is controlled and managed by the IT service provider.

System Failure
Means an unintentional or unplanned - wholly or partially – outage, reduction in functionality, availability or operation of a **Computer System** not directly caused by a physical damage.

Information for underwriters:

The IMIA Advanced Cyber Exclusion shall be deemed as a “tool box” for underwriters to deal with the various cyber perils as listed in Clause 1.

The idea of the IMIA Advanced Cyber Exclusion is:

- to provide underwriters an overview of the wide range of cyber perils which has to deal with,
- to provide provisions for the involvement of cyber experts in case of a claim because the burden of proof that the IMIA Advanced Cyber Exclusion applies is on the underwriters,
- to have a clear understanding of the cyber-related terms by the use of the definition section, and
- to use the IMIA Advanced Cyber Exclusion as an instrument to write-back some cyber risks according to the respective risk appetite and cyber expertise if required.

Underwriters should be careful in using buy-backs because this can increase the exposure of cyber-related claims significantly. On the other hand, the purpose of the IMIA Advanced Cyber Exclusion is to provide a strict cyber-related exclusion which could lead to a narrower scope of coverage as agreed upon between the insurer and the insured in some cases wherefore a specific write-back is needed. This should also be kept in mind.

Underwriters should also consider that with some write-backs specific exclusions might be required such as the outage of external networks exclusion.