Crisis Solution (Corporate) 2.0 Endorsement

CYBER EXTORTION INCIDENT RESPONSE

It is agreed that:

1. The policy is amended by adding the following schedule:

Cyber Extortion incident Response Schedule

Cyber Extortion Limits of Liability
(all amounts specified are for each single **Cyber Extortion**):

1.	Cyber Extortion Overall Limit of Liability:	USD [ ]
2.	**Ransom**:	USD [ ]
3.	**Crisis Consultants** fees and expenses:	USD [ ]
4.	**Cyber Extortion IT Expenses**:	USD [ ]
5.	**Cyber Extortion Legal Expenses**:	USD [ ]
6.	**Reputation Protection Expenses**:	USD [ ]

2. Insurance Cover 1, Ransom, is amended by adding the following:

   The **Insurer** shall also reimburse the **Policyholder** for **Ransom** surrendered by an **Insured** as a result of a **Cyber Extortion** which commences during the **Policy Period** and within the **Territory**.

3. Section 1, Insurance Covers, is amended by adding the following:

   Cyber Extortion Expenses Insurance Cover

   The **Insurer** shall pay on an **Insured's** behalf, or reimburse the **Policyholder** for, **Cyber Extortion Expenses** incurred by an **Insured** in connection with a **Cyber Extortion** which commences during the **Policy Period** and within the **Territory**.

4. In Section 2, Definitions, the definition of **Insured Even**t is amended by adding the following:

   For the purposes of Insurance Cover 1.1 (Ransom), Insurance Cover 1.3 (Crisis Consultant Response) and the Cyber Extortion Expenses Insurance Cover only, **Insured Event** also means a **Cyber Extortion**. For the purposes of all the other Insurance Covers, **Insured Event** does not include a **Cyber Extortion**.

   A result of this is that, as well as cover with regard to **Cyber Extortions** being afforded under Insurance Cover 1.1 (Ransom) and the Cyber Extortion Expenses Insurance Cover, cover with regard to **Cyber Extortions** is afforded under Insurance Cover 1.3 (Crisis Consultant Response).

5. In Section 2, Definitions, the definition of **Loss or Expense** is amended by adding the following:

   Loss or Expense also means **Cyber Extortion Expenses**.

6. In Section 2, Definitions, the definition of **Ransom** is amended by adding the following:

Ransom also means cash, funds, monetary instruments, cryptocurrency, securities, **Property** or services surrendered or to be surrendered by or on behalf of an **Insured** to meet a **Cyber Extortion** demand.

7. Section 2, Definitions, is amended by adding the following:

Breach of Corporate Information means unauthorised disclosure or transmission of **Corporate Information** in a **Company's** or **Information Holder's** care, custody or control or for which a **Company** or **Information Holder** is legally responsible.

Breach of Personal Information means unauthorised disclosure or transmission of **Personal Information** in a **Company's** or **Information Holder's** care, custody or control or for which a **Company** or **Information Holder** is legally responsible.

Communications Consultant means the crisis communications specialists, FleishmanHillard, or any other crisis communications specialists used with the **Insurer's** prior written consent.

Confidential Information means **Corporate Information** and **Personal Information** in a **Company's** or **Information Holder's** care, custody or control or for which a **Company** or **Information Holder** is legally responsible.

Corporate Information means any third party's items of information that are not available to the public and/or trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports, documents subject to contractual or legal protection.

Cyber Extortion means the making of illegal threats, other than in the conduct of **War or Terrorism**, directly or indirectly to an **Insured**:

(i) to release, divulge, disseminate, destroy or use **Data** acquired through the unauthorised access or use of a **Company Computer System**;

(ii) to introduce a malicious code into a **Company Computer System** or use of a **Company Computer System** as a vehicle to transmit malicious code;

(iii) to corrupt, damage or destroy a **Company Computer System** and:

  (a) electronically communicate with the **Company's** customers, falsely claiming to be the **Company**, or to be acting under the direction of the **Company**, in order to falsely obtain personal information of the **Company's** customers (also known as "pharming", "phishing", or other types of false communications);

  (b) restrict or hinder access to a **Company Computer System**; or

  (c) disclose electronic or non–electronic **Confidential Information**; or

(iv) to execute a denial of service attack on a **Company Computer System**,

that involve an actual or threatened unauthorised access to a **Company Computer System**, give rise to actual or potential financial and reputational harm to the **Company** and are made by a person or group who demands a **Ransom** specifically from an **Insured's** assets as a condition of not carrying out such threats.

Cyber Extortion does not include the making of any threats:

- by or on behalf of a state or any government, authority or institution of a state; or
- involving any collusion, collaboration, procurement, incitement, encouragement, active non-prevention or similar participation or conduct by a state or any government, authority or institution of a state.

Cyber Extortion Expenses means **Cyber Extortion IT Expenses**, **Cyber Extortion Legal Expenses** and **Reputation Protection Expenses**, but not including any fees or expenses of the **IT Specialist**, **Legal Adviser** or **Communications Consultant** in:

(i) recreating **Data** which is not machine readable or is corrupted;

(ii) reloading or re-customising such licensed software operated by a **Company** at the time of the **Cyber Extortion** as is not machine readable;

(i) updating, upgrading, enhancing or replacing a **Company Computer System** to a level beyond that which existed prior to the occurrence of the **Cyber Extortion**;

(ii) removing software program errors or vulnerabilities;

(iii) repairing or replacing tangible property;

(iv) preparing for notification of an actual or suspected **Breach of Personal Information** or **Breach of Corporate Information** to **Data Subjects** or to a **Regulator**, whether by investigating, or collating information about, that actual or suspected **Breach of Personal Information** or **Breach of Corporate Information**, setting up call centres or otherwise;

(v) providing credit or identity theft monitoring services to identify possible misuse of any **Personal Information** as a result of an actual or suspected **Breach of Personal Information**; or

(vi) obtaining insurance.

Cyber Extortion IT Expenses means the necessary fees and expenses, incurred with the **Insurer's** prior written consent, of the **IT Specialist** in:

(i) investigating a **Cyber Extortion**, including:

  (a) assessing whether the threat is credible and how it occurred; and

  (b) identifying whether the **Cyber Extortion** has resulted in a **Breach of Personal Information** or a **Breach of Corporate Information** and establishing the extent of the **Personal Information** or **Corporate Information** that may have been compromised;

(ii) containing the **Cyber Extortion**, including containing a denial of service attack;

(iii) resolving a denial of service attack, removing malicious software, computer code or virus from a **Company Computer System** and identifying any comprised **Data**; and

(iv) examining a **Company Computer System** to determine the remediation actions that are required in order to comply with an **Enforcement Notice**.

Cyber Extortion Legal Expenses means the necessary fees and expenses, incurred with the **Insurer's** prior written consent, of the **Legal Adviser** in:

(i) taking instructions regarding the factual background of the **Cyber Extortion** and coordinating the **IT Specialist** and the **Crisis Consultants**;

(ii) advising on requirements to notify **Regulators**, and assisting with notification to, and correspondence with, such **Regulators**;

(iii) advising on notifications to **Data Subject**s;

(iv) monitoring complaints by **Data Subjects** and advising on questions from **Data Subjects**;

(v) providing legal advice relating to media strategy and public relations; and

(vi) advising on response to the **Cyber Extortion**.

Cyber Terrorism means the premeditated use of disruptive activities against a **Company Computer System** or network, or the explicit threat to use such activities, with the intention to cause harm and further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. **Cyber Terrorism** does not include any such activities which are part of or in support of any military action, war or warlike operation.

Data Protection Legislation means the General Data Protection Regulation (Regulation (EU) 2016/679), the Data Protection Act 2018 and any other law or regulation of any jurisdiction relating to the regulation or enforcement of personal data protection or personal data privacy.

Data Subject means any natural person whose personal information is collected, stored or processed by or on behalf of a **Company**.

Enforcement Notice means a notice from a **Regulator** requiring a **Company** to:

(i) confirm compliance with applicable **Data Protection Legislation**;

(ii) take specific measures to comply with applicable **Data Protection Legislation**; or

(iii) refrain, within a specified time period of less than 5 years, from processing any specified **Personal Information** or **Data** held on behalf of a person other than an **Insured**.

Information Holder means a third party to which a **Company** has provided **Confidential Information** or which has received **Confidential Information** on behalf of a **Company**.

IT Specialist means the consultants, KPMG, or any other IT specialists used with the **Insurer's** prior written consent.

Legal Adviser means the law firm, Norton Rose Fulbright, or any other law firm used with the **Insurer's** prior written consent.

Newsworthy Event means the actual or threatened public communication or reporting in any media which arises directly out of an actual or potential or suspected **Cyber Extortion**, which is likely to bring any **Insured** into disrepute or tarnish their reputation or to damage public confidence in a **Company**.

Personal Information means any information that relates to a natural person and that is non–public information capable of individually identifying such natural person. **Personal Information** includes a natural persons' name, email address, telephone number, credit card or debit card number, account and other banking information, medical information, or any other data protected under any data privacy law or regulations.

Regulator means the United Kingdom's Information Commissioner, any other supervisory authority (as defined in Article 4 of General Data Protection Regulation (Regulation (EU) 2016/679) or any other regulatory body with power to investigate or regulate an **Insured's** conduct relating to data protection or data privacy.

Reputation Protection Expenses means the necessary fees and expenses, incurred with the **Insurer's** prior written consent, of the **Communications Consultant** in providing advice and support to mitigate or prevent the potential adverse effect or reputational damage from a **Newsworthy Event**, including by designing and managing a communications strategy

War or Terrorism means any war, terrorism (except **Cyber Terrorism**) invasion, military action (whether war is declared or not), civil war, mutiny, popular or military rising, insurrection, rebellion or revolution, military or usurped power or any action taken to hinder or defence against any of these events.

8. Section 3, Limits of Liability, is amended by adding the following section:

Limits of Liability for Cyber Extortions

Section 3.1, Limits of Liability Other Than for Death or Disability Benefit, does not apply to **Cyber Extortions**.

For each single **Cyber Extortion**, the maximum amount the **Insurer** shall pay or reimburse for **Loss or Expense** is the amount specified in Item 1 of the Cyber Extortion Incident Response Schedule ("the Cyber Extortion Overall Limit of Liability"). Then, for each single **Cyber Extortion**, the maximum amount the **Insurer** shall pay or reimburse:

(i) for **Ransom** under Insurance Cover 1.1 is the amount specified in Item 2 of the Cyber Extortion Incident Response Schedule;

(ii) for fees and expenses of the **Crisis Consultants** under Insurance Cover 1.3 is the amount specified in Item 3 of the Cyber Extortion Incident Response Schedule;

(iii) for **Cyber Extortion IT Expenses** under the Cyber Extortion Expenses Insurance Cover is the amount specified in Item 4 of the Cyber Extortion Incident Response Schedule;

(iv) for **Cyber Extortion Legal Expenses** under the Cyber Extortion Expenses Insurance Cover is the amount specified in Item 5 of the Cyber Extortion Incident Response Schedule;

(v) for **Reputation Protection Expenses** under the Cyber Extortion Expenses Insurance Cover is the amount specified in Item 6 of the Cyber Extortion Incident Response Schedule.

Each amount referred to in (i) to (v) immediately above is a part of and not in addition to the Cyber Extortion Overall Limit of Liability).

9. In Section 4.1, Notifications, the words "in the case of **Kidnapping**, **Hijacking** or **Extortion**" are amended by adding the following:

or **Cyber Extortion**