WHAT IS MEANT BY 'SILENT CYBER'?

Prudential Regulation Authority – Supervisory Statement SS4/17 (*extracts 1.6 and 1.1*) July 2017:

The PRA expects firms to be able to identify, quantify and manage cyber insurance underwriting risk. This includes both of the following sources of cyber insurance underwriting risk:

(a) affirmative cyber risk, i.e. insurance policies that explicitly include coverage for cyber risk; and

(b) **non-affirmative** cyber risk, i.e. insurance policies that **do not explicitly include or exclude coverage** for cyber risk. This latter type of cyber risk is **sometimes referred to as 'silent' cyber risk** by insurance professionals.

Underwriting risk is defined as … underwriting insurance contracts that are exposed to cyber-related losses resulting from **malicious acts** (eg cyber attack, infection of an IT system with malicious code) **and non-malicious acts** (eg loss of data, accidental acts or omissions) involving **both tangible and intangible assets**.

WHAT IS MEANT BY ‘SILENT CYBER’?

- Reality: How many standard market material damage policies really don’t explicitly deal with electronic data risk in some way e.g. exclusions (NMA 2914/5, CL380, Pool Re buy-back, alternative insurer and broker versions) and/or basis of settlement for data?

- Current silent cyber debates in 1st Party property therefore focus on:

  - explicit write-backs from exclusions

  - potential losses within the scope of cover not caught by exclusions or otherwise dealt with

- Discussions usually distinguish between “Cyber-Physical” and “Pure Cyber” extensions to the main material damage cover

THE “CHAIN RULE” FOR STANDARD PROPERTY BI

In the event of “the incident”

Policy covers

An insured event

Causing loss, destruction or damage

To property used by the insured at the Premises for the purpose of the Business

Resulting in interruption of or interference with the Business

Loss of income and/or expenditure as defined “in consequence of” and “but for” the “incident”

For the defined indemnity period less any savings (and net of deductibles, other terms and limitations)

PURE CYBER LOSS TRIGGER CONSTRAINTS FROM THE 'INCIDENT' IN STANDARD PROPERTY BI COVER

An insured event

↓

Causing loss, destruction or damage

↓

To property used by the insured at the Premises for the purpose of the Business

↓

Resulting in interruption of or interference with the Business

- Can a Property policy insured event be anything other than physical loss or damage?
- Can data, software and firmware be established as "lower case p" 'property used at the premises'?
- What about the Material Damage Proviso?
- Can interruption/interference not caused by damage to property be claimed for?

Conclusion: multiple hurdles to overcome in the chain to claim a non-physical cyber loss trigger for BI on a standard property policy