

Silent Cyber – Buyer Beware When Renewing Property Policies: The Growing Risk of Uninsured Loss

As commercial properties become increasingly reliant on digital systems, a hidden threat has emerged in traditional property insurances: **Silent Cyber risk**. Silent cyber refers to cyber-related losses that are not explicitly covered but rather excluded in conventional insurance policies, creating ambiguity and potential uninsured exposures. In recent years, insurers have sought to clarify and close this gap, most notably through exclusionary endorsements such as **LMA5400, CP1095**. Seemingly, each carrier now has their own version of these exclusionary endorsements which look innocuous but could have far-reaching effects on the coverage the insured expects.

This “silent” risk received heightened awareness with the January 2019 letter from the UK Prudential Regulation Authority¹ and Lloyds that insurers must have an action plan to reduce the unintended exposure that can be caused by non-affirmative Cyber coverage.

The Rise of Cyber Exclusions in Property Coverage

Historically, property policies were silent on cyber exposures. This meant that losses triggered by a cyber event—such as a hack causing physical damage—could fall into a grey area. To eliminate this uncertainty, carriers have increasingly added endorsements which states in part:

“We will not pay for any loss, damage, liability, cost or expense... directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any cyber act or cyber incident...”

The Insurance Services Office, Inc. (ISO), in 2020, introduced two (mandatory) endorsements to address this exposure in property policies – CYBER INCIDENT EXCLUSION (CP 10 75 12 20) and CYBER INCIDENT EXCLUSION WITH ENSUING CAUSE OF LOSS EXCEPTIONS (CP 10 76 12 20).

The Cyber Incident Exclusion (CP 10 75 12 20) endorsement adds an additional exclusion that affects both direct damage and business income/extra expense coverage. Due to the inclusion of anti-concurrent causation language, loss or damage is excluded regardless of any other cause or event that contributes concurrently or in any sequence to the loss. With this endorsement, there is no coverage for loss caused directly or indirectly by a cyber incident.

The other (CP 10 76) adds a specified amount of coverage for direct damage or business income if the cyber incident results in [covered] loss.

This sweeping language seeks to exclude virtually all losses tied to cyber activity, whether malicious (hacking, ransomware) or accidental (software malfunction). Many of these endorsements have some degree of carve-back language that allows for certain “perils” to be the exception to the exclusion – the LMA’s exception is “ensuing fire or explosion” – not a very broad “give-back”...

Real-World Implications: Uninsured Scenarios

For property owners and managers, the implications are profound. Consider the following examples:

- **Building Management Systems (BMS):** If a hacker infiltrates a BMS and disables heating or ventilation, leading to frozen pipes and subsequent water damage, a property policy with a broad Cyber exclusion attached may exclude coverage. Despite clear physical damage, the proximate cause would be deemed a “cyber incident.”

¹ Bank of England, Prudential Regulation Authority, *Cyber Underwriting Risk: Follow-Up Survey Results*, letter to chief executives of specialist general insurance firms from Anna Sweeney (Director, Insurance Supervision), 30 January 2019, <https://www.bankofengland.co.uk/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results>

- **Elevator Controls:** Modern elevators run on networked software. A cyberattack that disables the control system could trap occupants, trigger costly repairs, or cause bodily injury. Property policies with cyber exclusions would likely deny such claims.
- **Sprinkler Systems:** Imagine a cyber intrusion that disables sprinkler activation during a fire. The resulting fire damage might be uninsured because the exclusion links the loss back to the cyber act, even though the peril—fire—is traditionally covered.

The Implications of Liability Protection

Absolute Cyber Liability endorsements in a General Liability policy can seem more innocuous but imagine a malware attack that affects a company's key services systems causing a gap in protection (e.g. security systems) resulting in bodily injury or damage to third party property. The same example for Building Management Systems is conceivable for instance a virus causing elevators to crash injuring patrons.

While many liability insurers are being very conservative with this exposure, there are still insurers who can provide a "bodily injury" exception to an otherwise broad cyber exclusion.

Managing the Silent Cyber Gap

Finding coverage is a struggle...there are specialized products coming to market but one avenue is to secure a broad equipment breakdown form that will limit the restrictions from an electronic type loss including limitations or viruses in computer equipment.

For property owners, the takeaway is clear: standard property policies may no longer respond to cyber-triggered events, even when the result is tangible physical damage. Risk managers should:

- Review property policies for cyber exclusions (e.g., LMA5400).
- Assess critical building systems that rely on digital connectivity.
- Explore standalone cyber insurance or a new entry to the market "Cyber Property Insurance" to close the coverage gap.

In today's interconnected environment, Silent Cyber is no longer a theoretical concern—it is an evolving exposure that requires proactive risk transfer strategies.

If you have any questions on how to mitigate any of the risks described or would like to discuss any other risk and insurance related issues for your business, please contact Albert Sica at asica@thealsgroup.com or 732.395.4251.