CLM Narrative Document

Evaluating and Examining Business Interruption Claims in the Cyber Space

I. Understanding Cyber Business Interruption Claims

Probably one of the top issues facing businesses is the impact of cyber-related business interruption. Traditionally, first party business interruption claims ere straightforward and easy to quantify. With the new dependency on technology, business interruption claims are highly concerning to businesses and insurance companies alike given the number of factors that need to be considered in their calculation. With the evolution of cloud risk and dangers to the supply chain management, numerous factors must be reviewed and analyzed in connection with a cyber-related business interruption. The catastrophic potential of these claims cannot be overlooked with the likelihood of extreme accumulated losses.

II. Handling BI Cyber Loss – Insured's Perspective

A BI cyber loss claim for a business is likely to be more severe from a loss perspective than claims for reimbursement of expenses incurred for a breach response. The ever growing threats of malware and ransomware make it even more important to be prepared to address the specific financial losses associated with the cyber incident.

Projecting losses after a cyber event often depends on a company's cyber preparedness for breach response. Once a breach is contained and remedied, a proactive strategy can enable a company to calculate any ensuing loss related to the cyber event. Risk managers must have the ability and tools to effectively evaluate risk and understand the possible levels of recovery. Timeframes for cyber events are immediate so calculation and response are dependent on an organization's ability to react. The need for concrete documentation focusing on the effects on revenue, mitigation costs and continuing expenses is critical for claim presentation and the use of a forensic accountant is an absolute necessity.

III. Coverage and the Cyber BI Loss

Business interruption coverage is more nuanced in the cyber context. There are multiple conditions that must be examined and considered to determine whether a BI claim is compensable.

From a carrier perspective, Business Interruption and Contingent Business Interruption liability are two of the more nuanced coverage extensions and complex exposures to underwrite. This results in inconsistent terms (coverage triggers) and strategies across the market. When underwriting an insured, we are evaluating risk factors in 2 main areas – company metrics and mitigating factors. In general terms, given limited loss history, we begin by assessing an Insured's class of business, Geographic footprint, and

current/past/projected revenue streams. Not all BI exposures are created equal – certain industries present clearer risks and more quantifiable potential losses. As we refine our underwriting, we look at an individual risk's mitigating actions – Incident Response Plans, Disaster Recovery, Business Continuity Plans, etc. As mentioned, this is a tough exposure to directly UW (see Merck) so preparedness and preventive action on the Insured side presents favorably in all underwriting analysis.

There is no common place approach to BI/DI coverage extensions, as not all risks or industries are comparable. Certain businesses can more accurately quantify exposure (i.e. retail), while others, such as companies with variable revenue flow (FIs), present more complex methods of calculating loss. When evaluating the individual risk, we must determine the appropriate application of our coverage - notably the retention (time and/or money), capital deployment (capacity and attachment), and scope (full limits v. sub-limits and blanket v. scheduled). An insurer can manage attachment point, capacity and retention to ensure the coverages are within their appetite and appropriate for the insured. As the industry continues to collect and refine data, I believe we will move toward more consistent application of coverage – this will present organizations with a broader range of coverage provided in a more tailored fashion to meet their needs.

IV. BI Calculation Following a Cyber Event

BI coverage aims to indemnify loss of profit or revenue, as well as increased cost of working and the cost of mitigating losses. Consideration is then given to fluctuations in market conditions which then make cyber BI losses more complex and less tangible. As such, several factors come into play.

A. Establishing Cause

Unlike traditional property policies, cyber incidents often do not result in physical damage. In the digital space, one must establish the nature of the loss that triggers the cyber policy coverage. Obviously, this is established by the examination of a digital forensics expert.

B. Waiting Period and Deductibles

BI coverage comes paired with a time-based deductible referred to as a "waiting period or a financial deductible." The waiting period can range between 4-12 hours. In other words, a business must wait out the prescribed policy timeframe before a loss is considered a cyber business interruption "event" under a policy. The purpose of the waiting period is to make sure insurers are not covering frequent short outages. It should also be noted that insurers will also limit the period of indemnity for interruption for which the policy will pay for losses. Analysis is then required to establish when a return to normal operations has occurred.

C. Aggregation

One of the more important concerns from a cyber insurance standpoint is the potential for aggregation of events. Attacks on digital infrastructures create unknown risks for industry and the possibility of a catastrophic accumulation of cyber exposures. Coupled with the potential risks of supply chain management, these risks can be difficult to assess. Accordingly, there is a wide variety of coverage offerings for contingent business interruption, but some policies restrict coverage for contingent business interruption. The risk of a catastrophic loss and determine how to ensure it will continue to evolve as risks are assessed and tools are developed to model cyber exposures.

D. Insuring Reputation

Another topic that is often addressed as an item of damage after a cyber attack is whether reputational damage covered under a cyber policy. Extended disruptions of business operations could lead to lack of confidence or trust in one's customer base which companies then argue equates to a business loss. Reputational impact is a striking feature of cyber losses and can be a significant driver for business interruption losses. However, reputational injury is tough to prove in light of market trends and fluctuation. Given the difficulty to quantify such losses, coverage is either difficult to find or excluded.

E. Best Tools for Quantifying BI Loss

[Simon: Thoughts?]