Cyber Claims: A Guide to Calculating Business Interruption

1st Edition

JS|HELD UNIVERSITY

516.621.2900 • university@jsheld.com • jsheld.com

While cyber was incorporated in some general liability policies (GL) of the 1980s, the first cyber standalone policy was written in 1997 through AIG. Though groundbreaking, as it was the first to address cybersecurity, it was a third-party liability policy only.[1] According to Statista, standalone worldwide cyber policy premiums have grown from $2.5B in 2014 to over $7.5B in 2020.[2]

Business Interruption (BI) coverage is now being offered in a high percentage of standalone cyber insurance policies (cyber policies). One of the significant events in cyber insurance in recent years has been the addition of more meaningful business interruption insurance for cyber-related events. It is common to see standalone cyber coverage that either combines first-party business interruption coverage with data breach liability or includes only first-party business interruption. It generally covers partial or complete business interruption following a cyber-attack or technical failure.

This paper addresses the most common and material BI measurement issues and the importance of a technical evaluation of the incident.

Technical Evaluation of Cyber Claims

Just like with fire, water, and other physical damage losses, it is necessary to perform a technical evaluation of the incident and any compromised equipment to understand the scope of damages, impact, period of recovery, and identify any upgrades or betterments that are wrapped into claim submissions.

Why is a technical evaluation of a cyber claim important to the BI evaluation?

- To confirm the cause of the event or loss and so carriers can determine if a covered event occurred.
- To identify specific affected systems and impact to the business.
- To identify the proper corrective action and most efficient recovery timeline.
- To identify any upgrades of technical changes that may have been completed concurrently with the event recovery that may impact the period of recovery.

It is imperative for this information to be gathered at the onset of a loss evaluation so that insurance carriers can understand how the loss applies to their policies and also understand the total exposure. The technical evaluation and the BI can be analyzed concurrently with respective experts.

[1]100 AIG Stories. The First to Tackle Cyber Risk. (2019) https://www.100.aig/stories/first-tackle-cyber-risk/
[2]Statisca.com 2020 Estimated Value of Cyber Insurance Premiums Written Worldwide from 2014 to 2020. https://www.statista.com/statistics/533314/estimated-cyber-insurance-premiums/

BI Measurement and Computation Issues

In this paper, business interruption is considered to equal the loss of net income plus continuing cost not earned. Cyber coverage, related to cyber risk, available in the marketplace is far from standard. There is a vast array of cyber products, each with its own terms and conditions, which may vary dramatically from insurer to insurer, even from policy to policy, underwritten by the same insurer.

There are many types of incidents and scenarios that are classified as a cyber claim. They can include:

- Ransomware
- Viruses / Malware
- Network Breaches
- Denial of Service
- Data Theft / Exfiltration
- Data Loss

With cyber claims, it's imperative to understand the important BI measurement and computational issues. Based on our research of a sampling of over 2,500 business interruption losses, the top three BI measurement issues between as claimed and as calculated, by issues in order of frequency, are:

1. Sales projections
2. Period of indemnity
3. Saved or avoided costs

Sales Projections

The first step for a forensic accountant in a BI computation is to determine the "But For" sales. "But For" the event, the sales would have been "X" amount. The policy wording is similar in many cyber policies when compared to property policies, but not identical. The common wording in cyber policies includes:

> *"Due consideration shall be given to the prior experience of the business and the insured business before the beginning of the security failure and to the probable business an insured could have performed had no security failure occurred."*

The policy goes on to state the insured shall not profit from favorable business conditions caused by the event (paraphrased).

With sales projections related to cyber, forensic accountants will be looking at the entire company, as opposed to just one particular location or region, which is usually the case with a fire or hurricane. An example of why this is important can be understood by comparing the different margins of an e-commerce company and brick and mortar store. In order to be most accurate, sales and margins need to be analyzed individually by business group.

Period of Indemnity

The focal point of determining the period of indemnity (POI) is usually the cyber technical experts working with the insured and claims adjuster that determine the POI. Accountants may have an ancillary role but are not the project lead.

The POI denotes the time period for which indemnity or compensation is payable under a business interruption policy. The POI is one of the most critical components of quantifying the business interruption loss.

A technical evaluation by a cyber technical expert is key to understanding how the incident will have an impact on the POI. All situations are unique and require technical expertise to evaluate. Some questions that must be answered are:

- What systems were confirmed to be affected?
- What were the specific functions of those systems?
- How do those functions impact the business?
- What was done to mitigate downtime or impact to the business during remediation?
- Whether there are technical alternatives to expedite recovery?
- What issues may have transpired during the recovery?
- What date was the remediation complete?

After a cyber event, it is common that upgrades or changes are made to systems and infrastructure to prevent a future incident. Identification of these costs and scopes are important because they may increase the claim value and period of recovery. Therefore, they may need to be adjusted. This can include:

- Purchase of additional hardware
- Changing software or security services
- Implementing redundancy or backup systems
- Moving systems to other locations / offsite
- Migrating systems to new software

In first-party BI losses, it is common to measure the POI based on a theoretical period of restoration. This is necessary when an insured decides to make improvements and betterments and not to rebuild. Cyber losses realize a similar scenario. Frequently the insured will choose to enhance their security network after a breach. The "beefing up" of the network may take additional time, which is not generally recoverable under the BI time period. This is an opportunity for a potential difference in opinion upon various experts/professionals as to how long it would have taken to "rebuild" as was.

Saved Costs

Saved (avoided) costs are required to be computed to determine the lost net income. Frequently, the most significant decision made by a business owner is whether they continue to pay non-productive employees during the outage period or have a layoff. The cyber BI coverage may or may not cover the cost of these employees. In traditional coverage, ordinary payroll is identified as non-essential payroll. This has largely been adopted by the insurance market to mean hourly payroll.

Conclusion

Completing both a technical and BI analysis related to a cyber loss is a combination of science and art.

This process includes:

- Confirming the cause of the event and extent of impact
- Identifying any upgrades
- Identifying the POI
- Computing lost sales
- Deducting saved costs

As simple as it may sound, each cyber claim will likely have a unique twist that is not comparable with prior events. Therefore, it is important to remember these three key points:

1. The cyber technical experts, the insured, and the claim personnel need to confirm the incident while identifying the specific impacts and exposures, technical issues affecting recovery, upgrades, and period of indemnity covered by the policy.
2. The CPAs determine the lost sales within the period of indemnity. When dealing with the same deck (financials) there should not be a wide variance difference in projections, with the exception of a new company and/or a new product.
3. Calculating saved (avoided) costs is a mechanical exercise combined with experience.

Seeking the assistance of cyber technical experts and a reputable accountant with knowledge and experience with cyber claims is key. Together, these experts will make the mechanics of the BI computation easier for all involved.

- Understanding the insured's business, understanding technical issues and impacts to the business, understanding recovery and proper corrective action, and understanding the business impacts and how it makes money.
- Only requesting the documentation necessary to support a claim without making a burdensome request.
- Getting a handle on potential exposure early in the process and managing expectations of both the carrier (reserves) and the insured (expected reimbursement).

Cyber coverage represents a new insurance market. Much like boiler and machinery plus employee practices liability insurance, cyber policies are here to stay. While BI is not a new concept, BI coverage within a standalone cyber policy is.

Acknowledgements

We thank our colleagues Peter Hagen (forensic accountant) and Troy Bates (equipment consultant) who provided insight and expertise that greatly assisted this research.