JS|HELD

# PERSPECTIVES

## What Forensic Accountants Should Consider When Analyzing a Business Interruption Insurance Claim Following a Ransomware Attack

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

# INTRODUCTION

As businesses continue to rely on computers and digital storage of important data, cyberattacks are a growing potential threat. According to an August 2025 report from Statista, the number of monthly ransomware victims grew 381% between January 2023 and November 2024. Ransomware is malware specifically designed to disrupt, damage, or gain unauthorized access to a computer system. The threat actor employs encryption to hold a victim's information at ransom.

Ransomware attacks have affected organizations such as public school systems, insurance carriers, government agencies, computer companies, healthcare facilities, food manufacturers, and utility providers, just to name a few. Even companies that help recover from ransomware attacks, like cyber insurance carriers and data storage/backup vendors, are not safe.

Business interruption (BI) occurs when a company experiences a loss of income as the direct result of a system failure. Business Interruption claims are not new, but BI from a cyber liability standalone policy is an evolving concept. Historically, BI coverage has been provided through commercial property policies. An increasing number of business interruption claims are the result of cyber ransomware attacks. But cyber liability insurance policies differ from insurer to insurer, so it is important to understand the policy and ask crucial questions.

So, what makes cyber business interruption claims unique?

# WAITING PERIODS AND POLICY LIMITS

Most business interruption claims have a waiting period. Standalone cyber policies differ from typical property BI claims as cyber business interruption waiting periods are typically less than a day, falling between 6 and 24 hours versus the normal 24 to 72 hours for commercial BI losses. It is important to understand the waiting period as it is the amount of time an insured must wait before the business income calculation begins. It is also important to know whether the waiting period hours are based on clock hours or business hours as this can have a meaningful impact on the business interruption analysis.

In addition to understanding the waiting period, it is important to understand the policy limits as ransom payments may be included as part of the BI limit. This could affect how you analyze the BI claim (i.e., if you have a $1 million BI limit, a $3 million business interruption claim, and $700,000 ransom payment that was covered and paid under the BI policy, you may not need to analyze every aspect of the BI claim as the insured only has $300,000 of BI coverage remaining after the ransom payment).

# PERIOD OF RESTORATION/ PERIOD OF INDEMNITY

The restoration period refers to the period for which the income loss is covered. Cyber claims are typically a shorter period of measurement. Many insureds present a claim and they do not consider whether it falls within their coverage period. One of the primary difficulties in measuring a cyber business interruption loss involves the applicable indemnity period. For property claims, the period of indemnity is most often based on the repair period. With a cyber claim, the start and end time/date are more challenging to define. As accountants analyzing a business interruption claim, we need to understand not just the financial aspect of the business but the technical side of the event as well. We defer to the carrier for the proper period of indemnity.

An example would be a claimed lost contract due to a cyber event. It would be less challenging to quantify a lost contract measured on its face value; however, there are details to consider, including:

- The start date of the contract
- How long the contract would have lasted
- Did the contract fall within the defined period of indemnity
- Was the contract later replaced by another contract

- Could the contract be fulfilled at a later date
- What income was lost from the contract during the covered loss period

The period of indemnity could be further complicated if the business's systems are back online, but the insured continues to suffer business interruption losses. It is also not uncommon that certain system upgrades or changes may be made after the event. However, those upgrades may extend the time that it takes to resume normal operations. That extension of time may not be considered part of the period of indemnity under the policy provisions. Forensic accountants will rely on the technical evaluation of what was completed post-event and direction from the carrier as to how everything fits into the policy coverages.

## MAKE-UP/DELAYED

Consideration should be given for delayed revenues or revenues that could still be achieved after the repairs are complete. For example, if a manufacturer was not able produce its product for two days, had inventory on hand, production was made-up once their system was back online, and they were not at full capacity prior to the loss, there may not be a BI loss. However, if the insured increased production and paid overtime to employees to make up production during off hours, the insured might have incurred extra expenses instead of a business income loss.

## SAVED COSTS AND EXTRA EXPENSES

Saved (avoided) costs are required to be computed to determine the lost net income. Saved costs in a cyber claim may be different from a property claim. There are savings such as cost of goods sold, credit card fees, and other variable selling expenses that should be the same in either loss scenario. However, expenses related to the physical location, such as rent and utilities, may not be saved as the insured normally stays in their physical space as they restore their IT capabilities. In addition, the insured sometimes uses salaried IT staff to make the required IT repair/restorations. Frequently, the most significant decision a business owner must make is to decide whether they continue to pay non-productive employees during the outage period or temporarily lay off staff.

A common issue occurs when an insured uses their salaried personnel to rebuild/repair their systems and claims these costs as an extra expense. Salaried personnel are considered a fixed expense and are typically not allowed as an extra expense as the business did not incur additional salaries because of the cyber event. In addition, the insured may use internal hourly staff to work on the repairs. If the payroll stays at normal levels, there could be a duplication between the payroll allowed in the technical evaluation and the business interruption loss. Payroll should only be considered once. It is also common for an insured to claim lost billable hours for any employee who devoted time to the IT system restoration. However, only employees who were normally billable prior to the cyberattack would potentially lose revenue for the insured during the downtime.

It is important to communicate early in the claims process the potential saved costs or extra expenses and how they impact the BI analysis. In addition, consider whether these expenses fall within the period of indemnity.

## GEOGRAPHIC LOCATION

In a cyber event, a forensic accountant may need to look at an entire company as opposed to just one location or region. While some cyber losses may only affect one location, others may affect multiple locations, even globally. It is important to understand how the cyberattack affected sales, especially if the business generates sales through both e-commerce and brick-and-mortar stores. Sales and expenses would need to be analyzed for any potential make-up.

If there are multiple locations affected globally, it is imperative to work with the insured and carrier to determine the impact to only the covered locations as there may be multiple insurance policies involved and, potentially, no coverage for some locations.

## CONCLUSION

Cyber-attacks are inevitable and business interruption is a main driver in cyber losses. A forensic accountant should be engaged as early as possible to assist in communicating with the insured and adjustment team to understand the impacts from the cyber event. The accountant will also assist in managing the expectations of what will be needed to quantify a business interruption loss and to help identify ways the loss could be potentially mitigated.

## ABOUT THE AUTHOR

Jessica Eldridge is a Vice President and Director of Cyber in J.S. Held's Forensic Accounting – Insurance Practice. She has over 20+ years of investigative and forensic accounting experience in measuring financial damages involving business interruption, cyber, extra expense, stock, builder's risk, employee dishonesty/fidelity, personal injury, subrogation, and litigation support services. Jessica also has extensive experience with the administration of common fee funds and the oversight of property damage claims for large construction projects. Her industry experience includes, but is not limited to, automotive, life sciences, hospitality, manufacturing, retail, medical services, hospitals, college & universities, casinos, state and local municipalities, specialty human services, recycling plants, real estate, and construction projects.

Contact Jessica Eldridge at jeldridge@jsheld.com or
+1 857 219 5720