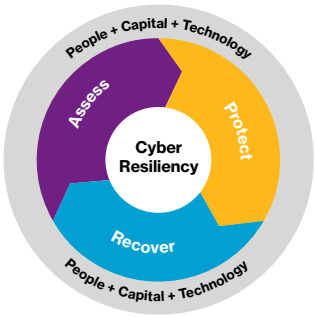

Decode prepared.

Estimating business interruption loss due to a cyberattack: Best practices

by **Mark Gallagher**

The staggering business interruption losses sustained by various organizations as a result of recent WannaCry and NotPetya attacks have served as a catalyst for many first-time cyberinsurance buyers. While business interruption claims resulting from a cyber breach are less frequent than claims for reimbursement of expenses incurred for a breach response, they are generally more severe in loss exposure. Given the current environment, attacks leading to a prolonged network business interruption are almost certain to increase.

Although only 5% of the claims that make up the Willis Towers Watson 2017 Reported Claims Index are for business interruption, the losses associated with these claims were significantly greater than those for other types of claims. We expect this percentage to rise in the coming years as malware and ransomware become more sophisticated. A cyberattack or operational failure of an organization's network systems can have dire financial consequences, such as loss of productivity and sales, and lack of or impaired access to websites, which is especially harmful for online retailers and financial institutions. Companies subject to cyberattacks face the potential for significant financial and reputational damage as well.

Type	Percentage
Business Interruption	5%
Security-Privacy Liability	19%
Incident Response Expense	76%
Extortion	4%
Regulatory	10%
Other	11%

Given the expected trend and the potential losses resulting, a strategy for minimizing, estimating and calculating damage from a business interruption should be part of every organization's cyber incident response plan – well before the organization is faced with a cyber event.

The need for pre-planning: projecting losses

When faced with a catastrophic cyber event, an organization's successful recovery often depends on its preparedness. A proactive strategy helps reduce the impact of the business interruption and enables a smooth process when seeking recovery for lost income and incident-related mitigation expenses. Most incident response plans, however, focus on event management costs, such as forensics, public relations, breach notification, and credit/identity monitoring services. Many organizations tend to overlook losses due to business interruption and do not have a plan in place for calculating the ensuing loss.

Willis Towers Watson

One approach for addressing this blind spot is to test various possible business interruption scenarios to determine the likely amount of loss in the event of an incident, as well as how those losses will be calculated. For example, an online retailer may want to consider daily, monthly and seasonal impacts on sales and staffing levels to ensure an accurate projection of lost sales as a result of a business interruption.

Risk managers are encouraged to work in tandem with their IT and finance departments to understand the potential operational costs and financial exposure resulting from the failure or outage of a particular system. Relationships with vendors that may need to be retained to respond to the cyber event should be considered and set in place ahead of time with pre-negotiated rates and pre-approval from insurers, where possible.

From planning to action: calculating losses

An organization's incident response plan will not be truly tested until faced with the fallout from a cyber event. While an organization's technical team is focused on restoring the network and getting the business up and running after such an event, others will likely be focused on monitoring sales and costs to determine variations from expected results. All components of income statements and balance sheets must be scrutinized, as the impact from a cyber-related interruption may not be immediately obvious.

When calculating business interruption loss stemming from a cyberattack, there are different factors to consider depending on the type of organization affected. Some examples follow:

- If the reservation system of an airline were impacted, it would be important to determine when the decline in revenue would be reflected on the company's books, as there is often variability in when customers rebook their flights following a network outage. As such, future revenues should also be analyzed to quantify the true impact to the airline.
- If a cyberattack impacts a manufacturing company's production processes, the organization may need to show that it was unable to continue generating revenue using its finished goods inventory on hand.
- If a financial institution is impacted and the settlement of a trade is delayed, that institution may need to determine when the income would have been reflected on the company's books.

Effective communication between departments is an important part of the loss calculation process to ensure accuracy. Without effective communication, the forensic accounting team could be left unaware of a certain expense incurred by one department that would be necessary to know in order to mitigate the loss and/or make a customer whole. As an example, if the customer service department of an online retailer elects to grant a 5% discount or service credit to customers that experienced difficulties in completing orders after an event, the finance department may consider preparing documentation to support the discounts as a response to the cyber event, rather than merely a show of goodwill.

Insurance and recovery process: best practices

While coverage for business interruption loss under cyberinsurance policies is becoming more prescriptive, the language in most insurance policies is still somewhat open-ended and subject to competing interpretations. Therefore, it's important to fully understand what the policy covers before making a business interruption claim. Most business interruption coverage includes a waiting period of a certain number of hours and a requirement that net profit or loss, charges and expenses be calculated on an hourly basis. It's important to recognize that cyberinsurance policies provide for the recovery of lost net profits and mitigation costs, as well as continuing expenses, such as employee salaries.

In presenting the claim to the insurer, the claim/incident narrative is key. We recommend including specific explanations for costs incurred, along with supporting financial documents and spreadsheets.

For example: *"We implemented [Solution A] because of [Situation X], which was cheaper than [Solution B]. This course of action helped prevent the possibility of [Situation Y] from occurring."*

This approach demonstrates the applicability of the expense to the business interruption and highlights reasonable and necessary steps taken to mitigate the loss. Note: while we encourage companies to cooperate with insurers' reasonable request for information/documents pertaining to business interruption, it is equally important that insureds be succinct in their responses — too much information or voluminous documents, particularly irrelevant ones, can delay payment of the claim.

Insurers are increasingly turning to forensic accountants to analyze claims. As such, retaining your own forensic accountant may be prudent for the following reasons:

- The process of calculating loss can be difficult and the assistance of a trained forensic accountant will allow for more accurate allocation of time and resources put against the interruption.
- Insurers may view the analysis of an independent forensic accountant as more objective and credible.
- If the claim is denied or disputed, the organization will be better prepared with an expert of its own, especially if the expert is already familiar with the case.

Because there are no hard and fast rules on the type of information that insurers or their claim adjusters may request or the length of time it might take to process the claim, we recommend that companies work with their brokers (and outside counsel, where applicable) to ensure a succinct, relevant and timely response to an insurer's request for information. Note: business interruption claims are under an incredible amount of scrutiny and are likely to undergo several layers of management review before being approved and paid.

Finally, it is more important than ever for the decision makers within organizations across all industries to be proactive in their approach to managing cyber exposures and risks. Three prongs of any holistic approach to combating cyber risk should be to:

1. Prepare for the inevitable business interruption as a result of a cyber event.
2. Understand how to calculate any resulting loss given the unique elements and characteristics of the organization's business and network structure.
3. Effectively present the loss to the insurer(s) for payment or reimbursement.

The more that can be done upfront to prepare against a possible business interruption, the less financial damage is likely to be caused.

Contact

Mark Gallagher
Willis Towers Watson
404 224 5027
mark.gallagher@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson