Marsh

CrowdStrike outage event coverage and recovery resource guide

August 2024

A business of Marsh McLennan

This brief resource guide is designed to help facilitate your organization's insurance recovery from the CrowdStrike outage event.

Our nearly 500 cyber colleagues around the world – including your client executive, placing broker, and our 65 cyber advocates and deeply experienced forensic accounting and claims professionals – are prepared to help you turn a potential cyber event crisis into an organized and manageable business process. This will allow you to return your focus to other significant business objectives with the confidence that recovery can be swift, streamlined, and effective.

For further guidance specific to this event and its impact on your business, please reach out to your Marsh representative, who will connect you with the appropriate Marsh resource.

Table of contents

What insurance coverage is available?[1]

From what we know to date about the incident, the three cyber coverages most likely implicated are cyber business interruption, cyber contingent business interruption (sometimes referred to as dependent business interruption), and errors and omissions (sometimes referred to as professional liability or professional indemnity). Consult with your Marsh representative to review any non-cyber and errors and omissions insurance policies you may have to determine if other coverage or any potential non-cyber avenues for your financial recovery may be available.

Table 1 – Comparison of cyber business interruption, cyber contingent business interruption, and errors and omissions coverage

	Description	Coverage trigger	Potential covered costs
Cyber business interruption	If computer systems owned, operated, or controlled by the insured organization were affected by the CrowdStrike outage event, and this resulted in an interruption to business operations, business interruption coverage may apply.	A security failure or system failure (an unintentional and unplanned outage) that directly affects the insured organization's own operations, leading to a temporary suspension or reduction in business activities.	Financial losses incurred by the insured organization due to the direct interruption of its own operations. These may include lost revenue, increased expenses, and other costs associated with the temporary suspension or reduction in business activities.
Cyber contingent business interruption	If an insured organization's systems were not directly affected by the CrowdStrike outage event, but the systems of its vendors or suppliers suffered outages that affected its business, contingent business interruption coverage may apply.	A security failure or system failure (an unintentional and unplanned outage) occurs to a specified third-party entity that has a direct impact on the insured organization's ability to continue its operations.	Financial losses incurred by the insured organization due to the disruption of a specified third-party entity. These may include additional expenses incurred to mitigate the impact of the third-party disruption.
Errors and omissions (E&O)	If an insured organization is a technology service provider, performs technology services, or provides technology products, there may be potential liability claims associated with its alleged failure to provide such services as a result of this event.	A written demand from a third party affected by the insured organization's performance of, or failure to perform, technology services.	Defense costs and damages. *Note:* No admissions of liability or offers of compensation should be made without your insurers' consent.

[1] These guidelines are provided for illustrative purposes only. Please consult the specific terms and conditions of any policy wording for specific coverage determinations.

Tips for insurance recovery

If you are pursuing financial recovery through applicable insurance coverage, please consider the following key steps.

Note: You should discuss the following with your Marsh representative and insurers before proceeding. Please keep in mind that notice to Marsh about a potential loss does not constitute notice to your insurer or under your policy.

1. **Notice:** Notify your insurer(s) that your systems or your vendors' systems may have been impacted by the CrowdStrike software update of July 19, 2024 04:07 UTC. Even if you are not aware of the extent of the potential loss or cannot quantify it at this time, you can still notify insurers of the circumstances surrounding the incident and/or notify your insurer(s) that you have received a written demand from a third party based on the technology services you provide them. Marsh can assist you with the notification process, but notice to Marsh does not constitute notice to your insurers.
2. **Assess your loss:** Keep detailed records around any loss you actually or potentially suffered. This includes how, when, and where it was identified, and any loss mitigation efforts.
3. **Retain vendors:** Hire outside vendors to assist with your own systems recovery and/or to minimize the impact of the event on your operations. Speak with your Marsh representative to determine if insurer consent is required before retaining vendors.
4. **Prepare your claim:** Assess the monetary impact and income loss calculation associated with the event. If employees assisted with the recovery of systems or operations, document any overtime incurred as a direct result of those activities. To the extent claim preparation coverage exists in relevant insurance coverages, such costs also may be a recoverable expense.
5. **Understand the impact:** Create a timeline of the outage and the recovery of systems and operations. Understand your cyber policy's waiting period before coverage is applicable.

Supporting documentation checklist

Examples of the types of documentation and data that should be maintained include, but are not limited to:

- **Invoices and receipts:** Keep copies of invoices and receipts for all expenses related to the recovery efforts. This includes invoices from temporary workers, outsourcing services, IT support, data recovery services, legal services, and any other vendors. These documents provide a clear record of the costs incurred and help validate expenses. Invoices from professional services firms (i.e., lawyers, accountants, consultants) who charge by the hour should show hourly rates, hours by day, and descriptions of tasks completed in detailed timesheets.
- **Timesheets and payroll records:** Maintain timesheets and payroll records for temporary workers, internal employees working overtime, and any additional labor costs incurred during the recovery period. These records support the basis for labor-related expenses.
- **Communication records:** Document all communications related to the cyber event and the recovery efforts.
- **Contracts and agreements/statements of work:** Keep copies of contracts and agreements with vendors, service providers, and consultants involved in the recovery process.
- **Detailed general ledger cost account:** Open a cost account in the general ledger that records all transactions related to the recovery efforts, ensuring accurate tracking of costs. Creating a handful of cost categories within the cost center would be helpful, i.e., IT Costs, BU Costs, Legal Costs, Other Vendor Costs.
- **Expense reports and reimbursement requests:** Require employees and stakeholders to submit detailed expense reports and reimbursement requests for any costs incurred during the recovery period. These reports should include itemized lists of expenses, supporting documentation, and explanations of the business purpose.
- **Incident reports and incident response documentation:** Maintain incident reports and any documentation related to the incident response efforts. These reports outline the details of the outage, the actions taken to address it, and the associated costs.
- **Operating account analytics:** Use these to demonstrate increased internal operating costs above normal. When response activities are performed internally there is no external invoice to point to. Inefficiencies caused by the outage event are likely to cause normal day-to-day operating costs to increase. Analytical review of normal operating costs will help identify these hidden increased operating costs. A review of the business continuity activities and efforts being undertaken by internal company personnel should help direct which operating accounts should be reviewed to capture these often-hidden increased costs (i.e., warehousing costs, shipping costs, communication costs, expedited postal costs, customer support costs, etc.).

The data management associated with the recovery exercise can be a unique challenge and needs to be thoughtfully constructed. It's recommended to set up an internal data share site where collected data can be categorized and posted. Note, some sensitive data may be collected (i.e., payroll data) and should be protected with limited access rights.

Marsh's Forensic Accounting and Claims Services (FACS) team can aid in: managing the initial response and flow of communications, documenting the timeline of events, properly categorizing costs, gathering and maintaining source documentation in data share sites, providing analysis of business interruption and financial impacts, and tracking any third-party liability claims that may arise.

Measuring business income losses

If your organization has suffered an income loss due to the CrowdStrike outage event, or perhaps only a temporary decline rather than a permanent loss, it's critical to follow a comprehensive process to measure the true economic impact of the event.

Known as an income loss calculation or analysis, below are nine key steps you can follow when setting out to accurately measure your outage-related economic loss, including the types of documentation required for the analysis.

1. **Gather initial key source documentation:** It's critical to collect all relevant documentation related to the event and its impact on your organization. This information may include, but is not limited to:

   - *Incident reports:* Detailed reports documenting the event, its causes, and the resulting impact on business operations.
   - *Financial records:* Granular monthly operating statements and other financial records for the affected period and comparable periods.
   - *Communication records:* Emails, memos, meeting minutes, and other correspondence discussing the event, its consequences, and any risk mitigation efforts.
   - *Contracts and agreements:* Any contracts or agreements with third-party providers, vendors, or service providers that may have been affected by the event.
   - *Insurance policies:* Reviews of the organization's insurance policies, specifically those related to business interruption or contingent business interruption coverage.

   Cumulatively, this information offers a holistic window into your organization's unique documentation process, initial reaction to the event, as well as greater insights into its impact across internal teams and third parties.

2. **Identify the precise period of loss:** Pinpoint the specific period during which the income loss occurred. This may include the duration of the event itself and any subsequent recovery period until business operations return to normal. This timeline may vary by business unit, but should document the following:

   - Which systems were affected
   - When systems came back online
   - When downstream operations returned to expected operating levels

   Equipped with this information, you can better understand the timeline of events pre-, mid-, and post-incident and, as a result, formulate more accurate analyses of lost income.

3. **Establish a baseline:** Compare the financial performance of the affected period with historical data from comparable periods. By analyzing business performance during similar time frames in the past, you can gain insights into expected financial outcomes

and identify any deviations from the norm. This establishes a baseline for assessing income loss.

In addition to historical data, it's also crucial to review and consider any pre-loss prepared management forecasts. These forecasts provide an estimate of the expected financial performance based on projected business conditions. If the actual performance during the affected period differs significantly from the forecasted expectations, it's important to understand the reasons behind the variance. It could be due to changes in business conditions, such as shifts in market dynamics, regulatory changes, or other external factors that impact your operations.

4. **Calculate insured gross profit loss:** Calculate the gross income loss by comparing the actual income during the affected period with the projected income based on the established baseline. This calculation should consider factors such as lost sales, reduced productivity, and any additional costs incurred due to the event.

   Keep in mind that the definition of insured gross profit is not synonymous with accounting gross profit, which is recorded on the profit and loss statement. Insured gross profit refers to the financial loss incurred by a business due to an insured event, calculated by comparing the actual income during the affected period with the projected income based on the established baseline. It does not deduct any continuing fixed overheads or continuing labor costs. Consultation with a forensic accountant who specializes in insured losses, like those in Marsh's FACS team, is recommended to ensure accuracy in this process.

5. **Consider risk mitigation efforts:** Evaluate any actions taken to mitigate the impact of the event on business operations. This may include implementing temporary workarounds, engaging alternative service providers, or other measures such as the use of inventory and overtime of personnel. Document these efforts and their associated costs.

6. **Deduct saved expenses:** Identify any expenses that were saved or reduced because of the event. For example, if certain operations were temporarily halted, there may be savings in areas such as labor costs or utility expenses. Deduct these saved expenses from the gross income loss to gain a more accurate picture of your actual loss.

7. **Consider extra and expediting expenses:** Identify and document any extra expenses incurred to continue or restore normal business operations after the event. This may include costs such as temporary workers, outsourcing services, communication expenses, data recovery costs, legal fees, and more. Additionally, consider any expenses incurred to expedite the repair, replacement, or restoration of systems and costs incurred to reduce the loss.

8. **Document supporting evidence:** Maintain detailed documentation to support the income loss calculation. This includes all previously mentioned documentation, as well as expense reports, invoices, receipts, timesheets, and any other relevant records. These documents provide evidence of the costs incurred and support the accuracy of the income loss calculation.

9. **Consult with experts:** Our FACS team is uniquely positioned to support companies with insights, expertise, and assistance in accurately assessing the monetary impact and preparing the income loss calculation associated with outage events. To the extent claim preparation coverage exists in relevant insurance coverages, such costs also may be a recoverable expense.

Marsh USA LLC
1166 Avenue of the Americas
New York, NY 10036-2774
www.marsh.com