



Navigating Business Interruption Risks in the Age of Cyber Disruptions

In an age where incidents like the CrowdStrike outage, and CDK and Change Healthcare cyber-attacks are more commonplace, it is becoming readily apparent how critical contingent (dependent) business interruption (BI) and standard BI coverages are for safeguarding against the cascading effects of cyber outages.

Organizations that rely on these types of vendors have been dealt significant operational challenges and most are still coming to terms with the repercussions. While the CDK attack resulted in **\$1 billion** of losses and CrowdStrike outage led to over **\$5 billion in losses**, a BI policy in place and the implementation of risk mitigation strategies could substantially offset these numbers for future organizations.

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.



Risk mitigation strategies

Today's operational standards often require businesses be intricately connected to a broad network of vendors and service providers. This interconnectedness means that a cyber event affecting one vendor can reverberate throughout the supply chain, causing substantial setbacks. To proactively address these challenges, companies should adopt robust risk mitigation strategies designed specifically for cyber-related disruptions.



Cloud backups

Implementing regular cloud backups is a fundamental step in ensuring business continuity when facing a system failure. These backups should be updated frequently and tested at least once a year to confirm reliability. Organizations can utilize varied methods for backing up data, including manual backups stored on Network-Attached Storage (NAS) devices, which offer an additional layer of protection.



Robust IT teams

Having a skilled IT team can be the difference between resolving system issues quickly and having to wait days for operations to resume. Many organizations benefit from partnering with Managed Service Providers (MSPs) that can offer expertise and support in real time. This capability ensures that technical issues are addressed promptly, allowing businesses to maintain operations during disruptions.



Incident response plans

Developing an Incident Response Plan (IRP) is becoming standard practice, with some cyber markets offering resources to assist in their creation. Many insurance carriers are even providing tabletop exercises at discounted rates. These exercises simulate a full attack scenario and yield actionable insights for improvement. Additionally, organizations should assess the impact of potential disruptions on third-party vendors and devise contingency plans accordingly.



Manual workarounds

Developing manual processes as contingency plans can be invaluable. When digital systems become compromised, manual workarounds can help prevent total shutdowns. By training staff on these processes, companies can ensure a smoother transition during crises.



Coverage options for BI

When it comes to safeguarding against financial losses due to business interruptions, companies have several coverage options and strategies to consider:

- **Business Interruption Insurance:** This type of coverage compensates businesses for lost income and additional expenses incurred due to system outages. It's a fundamental protection for any organization reliant on digital operations.
- **Contingent/Dependent Business Interruption Insurance:** This coverage helps to protect against losses stemming from disruptions to a company's suppliers or service providers. Companies should seek coverage that encompasses both IT and non-IT vendors, as some policies only address technology-related disruptions.
- **Cyber Event vs. System Failure Coverage:** It is crucial for policies to differentiate between business interruptions triggered by cyber events (like malware or hacks) and those caused by system failures unrelated to cyber issues. CrowdStrike's recent outage and subsequent issues serves as a reminder that organizations must ensure that their policies adequately cover both scenarios.
- **Layered Coverage Approach:** Implementing a layered insurance strategy helps spread risk across various types of coverage including cyber liability, contingent business interruption insurance, and E&O, providing more comprehensive protection against different kinds of disruptions such as supply chain disruptions, equipment failures, and transportation disruptions.
- **Waiting Periods and Time Retentions:** Understanding the waiting periods associated with coverage is vital. Insurers may require that a business be down for a certain amount of time—typically eight hours or more—before coverage kicks in. Policies that offer Ground Up coverage, paying from hour zero once the threshold is crossed, are ideal.
- **Extra Expense Coverage:** Extra expense coverage is crucial as it allows insurers to pay for reasonable and necessary costs incurred during the restoration period, helping businesses mitigate income loss.

We Help You Win

Ultimately, adopting a proactive mindset and thorough planning can help organizations navigate the evolving landscape of cyber risks effectively. It's a combined effort that, when implemented, can decrease the effects of disruptions tremendously.

Amwins is a leading professional lines wholesale broker, equipped with the expertise, proprietary products, and data needed to place coverage for your client's evolving cyber risks. Amwins also offers our clients **discounts with industry-leading cyber security service providers** who can help insureds improve their risk profile.

Empower your clients to operate with confidence by partnering with Amwins. Reach out to a broker today.

Insight provided by:

- Anthony Howley, AVP, Amwins Brokerage in Seattle, WA