RT ProExec
INSIGHTS
VOLUME XXVII ISSUE 3
FALL 2024

CYBER LIABILITY SUPPLY CHAIN & BUSINESS INTERRUPTION COVERAGE CONSIDERATIONS

Recent events serve as a warning: Businesses do not need to be targeted directly to experience data loss, business interruption, and reputational damage. Cyber incidents involving any vendor within a company's supply chain can have devastating impacts. Brokers need to discuss these exposures with their clients, and structure coverage to protect against the threat of supply chain and related business interruption arising from cyber incidents.

Recent Supply Chain Cyber Events

Until more recently, business interruption coverage has been associated with property insurance, responding to disruption caused by fires, storms, and other physical events. However, as companies have grown more dependent on digital solutions, cyber incidents have also become a cause of business disruption.

Large cyber incidents involving vendors have made headlines in recent months. The following are just a few examples:

- Change Healthcare, a subsidiary of UnitedHealth, was hit by a cyberattack in February 2024. According to the Energy & Commerce Committee, Change Healthcare is one of the largest health payment processing companies in the world, clearing 15 billion medical claims each year. The cyberattack knocked Change Healthcare offline and may have leaked the sensitive health information of millions of Americans onto the dark web. *Becker's Hospital Review* says Massachusetts hospitals were losing at least $24 million a day due to system disruption, possible impacting their credit ratings, and it will take weeks to months, before hospitals and other providers recover fully. AP News reports that the lack of multifactor authentication at Change Healthcare allowed the cyberattack to occur.
- On June 19, 2024, a ransomware attack resulted in a system shutdown at CDK Global, a car dealership software company. According to *USA Today*, more than 15,000 auto dealerships rely on CDK for management of key operations, including financing, repairs, maintenance, sales and vehicle acquisitions. CDK hoped to restore services to all dealers by July 4, meaning at least some dealers may have been without services for two weeks. According to *CBS News*, experts say vehicle sales could be down by about 100,000, or 7%, due to the outage.
- In July 2024, CrowdStrike, a global cybersecurity company, experienced a widespread outage that impacted devices running Microsoft Windows. According to CISA, the outage was due to a faulty software update initiated by CrowdStrike, and it impacted more than 8.5 million Windows devices. While the consequences for large national companies like Delta made the news, thousands of small-to-medium sized enterprises also suffered severe interruptions in their business operations and income.

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

RT ProExec

The Challenge Controlling Supply Chain Cyber Risks

According to the 2024 Data Security Incident Response Report from BakerHostetler, 25% of the more than 1,150 data security incidents studied involved a vendor. With supply chain failures continuing to cause widescale disruption, it's become evident that these risks are complicated to control. When incidents do occur, they can lead to a myriad of problems, from business disruption to data privacy concerns.

Businesses are in control of their own cybersecurity and employ measures like multifactor authentication to reduce the risk of a cyberattack. However, it is harder to determine whether their service providers are equally secure. Likewise, it is easy for insurers to ask policyholders about the insured's own cybersecurity policies and practices; but quantifying the exposure posed by various vendors, suppliers, and partners is another matter.

Analyzing the likely impact of an outage at, or an attack upon, a vendor is a crucial aspect of risk assessment. Well prepared insureds should explore the following:

> New Data Privacy Laws Add to the Regulatory and Legal Costs of a Cyber Incident
>
> By the end of 2024, nearly 40% of U.S. consumers will be protected under a comprehensive state-level privacy law, up from 20% in 2023.
>
> Out of 1,150 data security incidents in 2023, at least 58 resulted in data privacy lawsuits.
>
> Source: BakerHostetler's 2024 Data Security Incident Response Report

- **Upon which vendor(s) does the company depend?** When assessing supply chain cyber liability risks, it is easy to focus on technology vendors. However, recent events show that other partners also deserve attention. Any vendor that provides web-based services utilized by a business – whether human resources, call center, payroll, suppliers, or other non-technology providers – has the potential to cause disruption.
- **How long could the company survive without the vendor?** According to Sophos, 35% of companies across all industries take longer than a month to recover from ransomware. In some cases, daily operations may continue, but the impacted parties experience other losses. For example, while doctors could still provide care when Change Healthcare was offline, the Energy & Commerce Committee says the incident caused a backlog of claims and created cashflow problems for the medical providers. In other cases, disruptions force operations to grind to a halt. By way of example, Delta's operational issues during the CrowdStrike outage.
- **What contracts do you have in place to mitigate exposures?** When a cyber incident occurs on the vendor's side, who is responsible for the loss? Having these liability issues worked out in written contracts may prevent lengthy legal battles. For example, the Delta Air Lines CEO told *CNBC* that the CrowdStrike outage cost the airline $500 million and that CrowdStrike had offered no compensation other than free consulting advice. The incident could also lead to reputational damage – according to *USA Today*, customers were still struggling to receive refunds for cancelled flights weeks later. The situation is especially complex when it involves multiple parties (e.g., Delta, CrowdStrike, and Microsoft).

Coverage Considerations for Supply Chain Cyber Incidents

Policy language is not standardized thus careful attention must be given to the nuances involved in coverage for supply chain cyber incidents. To ensure that there is adequate coverage in place, brokers and their clients should secure policies with clearly defined coverage terms that addresses the following:

- **Direct and contingent business interruption coverage.** A cyber incident on any part of a business's supply chain may have disastrous effects. Therefore, it's important to know how a policy covers (or does not cover) contingent business interruption, such as the disruption Delta experienced.

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

RT ProExec

- **Coverage for non-technology providers.** Is contingent business interruption coverage limited to technology vendors? If so, the Insured will be exposed to disruption caused by non-technology vendors.

- **Scheduled or automatic coverage.** In some cases, vendors may need to be scheduled for coverage to apply. If so, it's important to run a thorough assessment of vendors and think through outage scenarios that could pose a risk – it can be easy to overlook dependencies. In other cases, coverage may apply to vendors (or at least to technology vendors) without the need for scheduling.

Average Costs for Business Interruption Claims for Small to Medium Enterprises

- Business Interruption: $487,000
- Crisis Services: $297,000
- Legal and Regulatory: $455,000
- Incident: $995,000

Source: NetDiligence Cyber Claims Study 2024 Report

- **Security incidents and system failures.** Ransomware and other cyberattacks are the cause of many cyber incidents. However, as the CrowdStrike outage shows, bad actors are not always the culprit. A well negotiated policy will include contingent business interruption caused by a vendor's system failures as well as by its security incidents.

- **Data restoration.** Data restoration is another crucial element of coverage. In addition to business disruption, a system failure or security incident may lead to loss of data. Regaining access to or recreating data involves expense.

- **Extra expense coverage.** The coverage responds to additional expenses relative to normal operating expenses to avoid and/or minimize business interruption loss. For example, companies may have to utilize alternative sources to meet contractual obligations of customers, employ contract staff, incur overtime costs for employees, and engage with specialist consultants including IT forensic consultants.

- **Reputational Harm.** When operations are down due to a cyber incident, the frustration may also be experienced by the impacted party's customers. For example, CBS News shows how one family couldn't take possession of their new vehicle due to the CDK outage. This type of disruption can lead to negative reviews and lost customers, resulting in financial loss that continues long after systems have been restored.

In closing...

Cyber liability supply chain outages present complex business interruption risks. As coverage continues to evolve, there is considerable variation in the breadth of coverage provided by carriers. Insureds should not assume that all cyber policies provide equal terms.

By assessing both their contingent cyber business disruption risks and their Cyber liability policy terms, business leaders can help minimize their exposures. Having a broker that understands the various dynamics of structuring the insurance is imperative. We welcome the opportunity to discuss any of the above topics with you in further detail.

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

RT ProExec