Reliance on third-party vendors increases exposure to cyber risk

Businesses face an increasing exposure to disruptions and lost income as they become more interconnected and dependent on third-party vendors for data storage and management, including web hosting and cloud support. In the spring of 2017, Amazon Web Service S3 cloud servers unexpectedly went offline for four hours on a Tuesday afternoon, disabling hundreds of thousands of websites and disrupting businesses dependent on any sort of cloud support to operate. While some businesses may have experienced a minor blip in productivity due to the inaccessibility of certain sites or online tools, many businesses experienced significant delays or were inoperable for hours, costing millions of dollars in lost revenue.

Third-party disruptions estimated to cost U.S. companies billions of dollars

According to *Cloud Down—Impacts on the US Economy*, a 2018 emerging risk report co-produced by Lloyd's and AIR Worldwide, the disruption of a top three cloud service provider for 3-6 days would cost the U.S. economy between $6.9 and $14.7 billion dollars. While larger companies may invest in their own web hosting or cloud storage technology and solutions, smaller businesses outside of the Fortune 1000 are more likely to rely on support from third-party or cloud data services. Smaller businesses are also less likely to have cyber insurance to cover lost income from a disruption and would suffer an estimated 63% of the losses.

Surprisingly, the industries that would be hit the hardest are not the ones that you would think. The manufacturing and wholesale and retail trade industries stand to lose an estimated $1.4 to $8.6 billion in the event of a massive cloud service outage. Businesses like these may not think they are vulnerable to a cyber event, but you don't have to suffer a direct breach to be negatively impacted. If a third-party data hosting or storage vendor goes down as the result of a security or system failure, other businesses could also be impacted resulting in the loss of irrevocable income. Employers run into trouble when they are unaware of or underestimate their exposure.

Protect your business from costly disruptions

Business interruption coverage as part of a commercial property policy covers lost income from disruptions caused by physical perils like fire and wind. Business interruption as part of a cyber policy provides the same coverage, but is triggered by a security failure in a company's network and systems, such as a cyber attack or data breach. Business interruption can even be extended to cover disruptions caused by a security failure at a third-party data hosting or storage vendor. Some insurance carriers will even extend this coverage to include system failure in the event of human error or an automated system fails.

Continued >>

Businesses can take additional steps to protect themselves from a damaging disruption caused by a third-party vendor:

- Consider requiring vendors to carry first and third-party cyber liability insurance with adequate limits to provide added protection.
- Regularly review vendors' policies and procedures for handling and protecting data. This may even be required by the first party insurance company's underwriter.
- Review insurance policies to make sure there is coverage in the event of a breach or third-party disruption. It can be challenging to predict how much coverage is needed, so employers should be sure to review their policies with a trusted insurance professional. Review policies periodically as the needs and exposures of the business will change over time.

It's no longer a matter of if, but when a disruption will occur. Employers need to make sure their businesses are prepared.

For more information, contact us.

Associated
Benefits and Risk Consulting

Phone: **800-258-3190** | Email: **Info@AssociatedBRC.com**