OVERVIEW

You Don’t Own the System, but You Do Own the Risk

Vendor Business Interruptions occur when crucial vendors have unplanned outages or downtime, causing the businesses that rely on them to suffer the same. Some critical categories of vendor include: e-mail, instant messaging, customer relationship management (CRM), Infrastructure-as-a-service (IaaS), and payment processing.

In July 2016, e-commerce site Etsy.com began experiencing issues tied to its payment provider, WorldPay. Although WorldPay initially said the issue was with a single payment gateway, and impacted “1% of users,” when an e-commerce site as large as Etsy is in that 1%, this certainly has a multiplicative effect! Furthermore, the downtime wasn’t fixed within hours, it stretched on for multiple weeks.

Another outage which rippled throughout the internet was the Amazon Web Services (AWS) S3 outage in February 2017. AWS is cloud computing/IaaS provider, and S3 is a storage mechanism which backs websites, applications, and data pipelines for most companies who rely on “the cloud.” One of those companies was a messaging application called Slack, and at the time of the outage, many users began to notice that image uploads had started to fail. When they searched the internet to determine the reason for the issues, they found that many websites couldn’t load, and updates from AWS soon revealed the reason. Although the outage was resolved within hours for most websites hosting content there, companies hosting data pipelines relying on S3 could have incurred large backlogs that impacted their external Service Level Agreements, or internal Key Performance Indicators.

BEST PRACTICE

Vendor Business Interruption

Resilience’s Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. Resilience’s model for a vendor caused business interruption recommend that organizations do the following to prevent and mitigate these attacks:

- Employ industry-leading primary vendors with service level agreements that match your uptime requirements for business critical functions such as e-mail, instant messaging, CRM, and IaaS

- Where possible, have redundancy and/or backup vendors for these areas and the ability to quickly “fail over” between service providers
- Develop and practice a business interruption response plan by conducting tabletop exercises with organizational stakeholders

INSURANCE

Business Interruption

Modern businesses rely on third-parties to operate. Vendors power supply chains, manage data, and move money. Unfortunately security events and system failures at a vendor can cause substantial disruption for a company. Insurance should cover contingent business interruption for your income loss and extra expenses should your vendor disrupt your business. Ask you broker for more information.

Example Claim

A luxury consumer goods retailer's shopping website is operated by a hosting vendor. The vendor was hacked, suffering an outage, and as a result the retailer's website suffered downtime for a three-day period, greatly impacting sales.