JAVELIN

Rethinking Disaster Recovery

16 December 2020 By: Tracy Kitten

Disaster recovery plans must encompass strategies that outline the deployment of critical resources to maintain continual network and database availability. While financial services companies focus most of their disaster-recovery and business-continuity planning around responses to natural disasters, the losses associated with cyberattacks have the potential to cost institutions much more than a natural disaster. Businesses today face significant threats regarding ransomware, distributed-denial-of-service (DDoS) attacks, and employee negligence that places the stability of the enterprise in jeopardy when adequate provisions for recovery are not made.

This report reviews the challenges that financial services companies experience from a technological and organizational point of view, with an emphasis on recommendations to minimize the adverse impacts of restoring normal business continuity after a disaster.

Key questions discussed in this report:

- What unique cybersecurity risks do organizations face when they continue to rely solely on physical data centers for data backup?
- How are organizational structures weakened by siloed departments?
- What can cybersecurity professionals do to reduce their risks by revisiting and revising their business-continuity and disaster-recovery plans?

The data in this report was primarily collected from a survey of 506 cybersecurity leaders conducted in May 2020.

---

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100