THE IMPORTANCE OF
BACKUP & DISASTER RECOVERY FOR REMOTE WORKERS

While the shift in work locations has left many employees and their employers adjusting to working from home, remote workers present security risks for their employers. Here's a closer look at the vulnerability of remote staff and the importance of a backup and disaster recovery (BDR) plan for your organization.

55% of businesses

offer some degree of remote work to employees

88% of businesses

encouraged or mandated employees to work from home because of COVID-19

54% of IT professionals

believe remote workers pose a larger security risk than on-site workers

review42.com/remote-work-statistics

45% **of employees** admit to using the same password more than once

More than 50% **of workers** admit they do not password-protect their home networks

90% **of employees** use employer-provided devices for personal activity

proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

TIPS FOR CREATING A BDR PLAN FOR REMOTE EMPLOYEES

Examine your current BDR plan. Are your recovery time objectives (RTO) and recovery point objectives (RPO) up to date? Can you meet them with your current backup and recovery technologies?

Express importance of robust passwords to remote employees and of changing them regularly.

Safeguard remote data by executing frequent backups from your remote employees' devices to their local external drive, the cloud or your corporate network.

Back up your data in multiple locations, such as on your company's servers and the cloud. Consider a BDR solution that does this automatically every few minutes.

Establish secondary Internet connections for remote employees, such as having them use their smartphones as hot spots to connect to your VPN.

Establish secondary power sources for remote employees. One option is to provide them with USB power blocks that are always kept plugged in and charged.

Ask employees to prepare a "bug-out bag" in case they have to evacuate in an emergency. This should include their work laptop, extra power supplies, a USB port, an HDMI cable and other relevant accessories.

40% to 60% of small businesses go out of business after a major disaster such as flooding, a hurricane or massive data loss.

20% of businesses have no disaster recovery plan.

fema.gov/media-library-data/1441212988001-1aa7fa978c5f999ed088dcaa815cb8cd/3a_BusinessInfographic-1.pdf

28% of businesses have experienced data loss within the last 12 months

19% of companies have had a security breach within the last year

invenioit.com/continuity/disaster-recovery-statistics

mxotech
Beyond IT. People.

mxotech.com

Sources:

blog.fentress.com/blog/remote-workforce-5-disaster-recovery-steps-to-take-now
blog.storagecraft.com/rethinking-your-data-backup-and-recovery-strategies-in-the-work-from-home-era
busycontinent.com/rethinking-your-work-from-home-data-backup-and-recovery-strategies
neuways.com/neuways-blog/remote-working-whats-your-data-backup-plan