access one

Cyber Security for a Hybrid Workforce: Are You Prepared?

Businesses are preparing for the long haul of hybrid work models – which often means taking a look at current cyber security strategies to ensure continued coverage for workers at home. This checklist will help you determine if your cyber security is adequate to keep your network and data safe in the era of hybrid work.

1

When was the last time you updated your BYOD policy?

For a hybrid workforce, BYOD can encompass a whole slew of devices that may not be properly secured. Updating your BYOD policy to specifically account for hybrid and remote workers provides employees with guidelines for acceptable use of personal devices.

2

Do you have an employee security training program in place?

Having a BYOD policy is necessary, but not sufficient to ensure remote workers understand how to implement your cyber security policies. Training and education are essential for the hybrid workforce.

3

Do you use multi-factor authentication?

Remote workers utilizing personal devices create additional risk – especially if those devices aren't properly secured. Multi-factor authentication ensures that only the people who should have access to your network will be able to get in.

4

Have you added (or upgraded) endpoint protection?

Endpoint security is a challenge for businesses with any number of remote workers. Every device that connects to your network – from anywhere – adds a point of vulnerability. Up-to-date endpoint protection is essential for hybrid workforces.

5

Are your remote workers connecting via a VPN?

Virtual private networks (VPNs) allow your remote workers to connect to your network virtually – so there's no sensitive data being accessed or saved directly onto unsecured devices.

6

Do your workers have access to a cloud-based file repository?

The hybrid work era is also the era of the cloud. If you're still allowing remote workers to save company data and files on their devices, you're enabling easy access for cyber criminals. Cloud storage is managed and protected by a third party who has a vested interest in keeping your data safe.

7

Do you have effective collaboration tools available to your remote workers?

Hybrid teams require different collaboration tools than those based exclusively in the office. Cloud-based collaboration solutions give your remote workers the same capabilities they would have if they were all sharing physical office space – so they can work together effectively even from afar.

8

Are you checking in regularly with your remote workers?

Remote shouldn't mean unsupported. Scheduling regular check-ins with your remote workers not only helps ensure they stay productive, but it also allows them to communicate proactively if there are technologies they need to effectively do their jobs.

9

Have you revised your escalation guidelines?

Escalation is relatively easy if your entire team is working in the same office. Remote workers need clear guidelines for escalation so that if customer issues arise while they're away from the office, risk is minimized and problems are addressed in a timely manner.