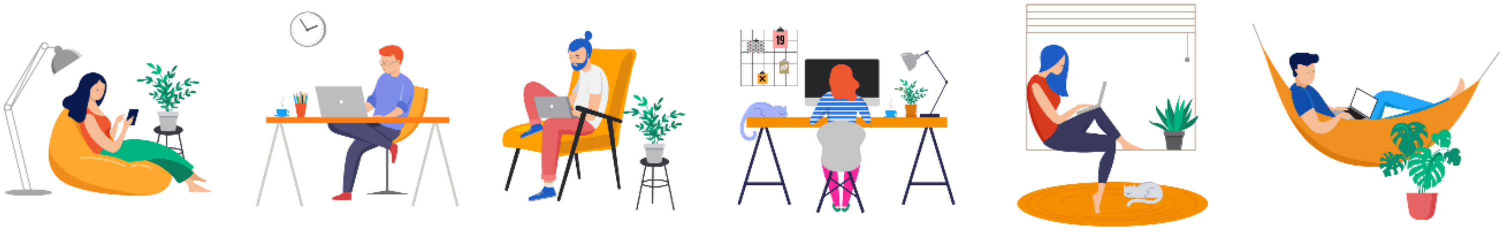
arcserve®

cristie data
an iomart company

Working from Home? Here are Four Top Tips for Keeping Data Safe and Secure.



The spread of coronavirus and social distancing mandates have put many IT pros in a precarious, but necessary, position of having to quickly transition to, and support, a largely remote workforce. While these precautions are absolutely critical and should be followed for the safety of employees and to slow the spread of the virus, you should not rush into this transition at the expense of data protection.

With more employees working from home, cybercriminals have more access points to exploit networks. The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency has even issued an alert about unpatched VPNs being targeted. Because of this, you need to ensure your infrastructure has the proper security measures in place and ensure workers are able to back up the data they're producing on their laptops to reduce the risk of data loss.

These are no doubt challenging times, and many IT teams are wading in uncharted waters as they try to figure out how to keep business moving forward amid the uncertainty. Partnering with Arcserve, here are our top four tips for keeping data safe and secure.

1. Don't panic and rush before security measures are in place

When trying to enable employees to work from home quickly, it can be easy to panic and rush the process. This can lead to implementing limited provisions on employee laptops. And, since you're essentially creating a multitude of "remote data centres," critical company data stored solely on individual devices will be unprotected without keeping cybersecurity, backup and DR at the forefront.

You should install centrally managed, cloud-driven cybersecurity solutions, including enhanced detection and response, ransomware protection, firewalls, and more to secure remote access. Missing this critical step leaves your organization at risk. When remote workers bring their devices into a home environment, there are suddenly an array of new devices operating within the same network, which significantly increases the attack surface that cybercriminals can take advantage of. So make sure you have your endpoints covered.

2. Get your Office 365 backup in place

Many users assume that cloud-based SaaS apps like O365 are automatically backed up. That's simply not the case. Making investments in third-party remote backup tools is essential to mitigating the risk of data loss when the company starts working from home (or even when it doesn't!). Cloud-to-cloud backup and DR solutions that are centrally-managed are ideal for remote work situations, which is especially important since most remote workers aren't likely to have proper security and data protection measures at home.

3. Test access, implement structure and provide training to maintain productivity

To coordinate work across multiple teams, you need to ensure that all shared apps are set up and tested ahead of time – the worst thing you can do is clear everyone to work from home, only to find out everyone is having trouble accessing the information they need.

Maintaining productivity is another challenge you're likely to face, but this can be eased by investing in tools that give employees the resources they need to work with one another effectively. Communication tools should have text, voice and video options, allowing staff to stay in touch with one another in a way that makes sense for them.

Once the toolset is established, employees will need to know how to use them properly, so making training available to everyone is a critical step in reducing hiccups during the transition. Some IT teams implement metrics to measure the progress and efficiency of tasks, which can also be helpful in making sure the company continues to stay on task.

4. Educate employees about cyber hygiene

In addition to training employees on how to properly use communication tools, you must offer cyber awareness training, too. Cybersecurity policies should be communicated widely throughout the entire organization, and employees should be educated about the warning signs of a phishing attack, including suspicious attachments, unknown links and doppelganger emails.

They should also be encouraged to report suspicious attempts, instead of sweeping them under the rug. Many employees often feel nervous about reporting a potential cyber incident, so open communication about these issues should be encouraged. Further, you should create a single source to report suspicious activity or potential phishing emails, whether that's via a dedicated IT support email, a dedicated messaging group, or even a Slack channel -- they need to know who to go to when working from home.

Remote workforces will be the standard for the foreseeable future, and it's hard to say what's next. We can hope and expect that things will be back to normal soon, but you should also be prepared to dig in for the long haul.