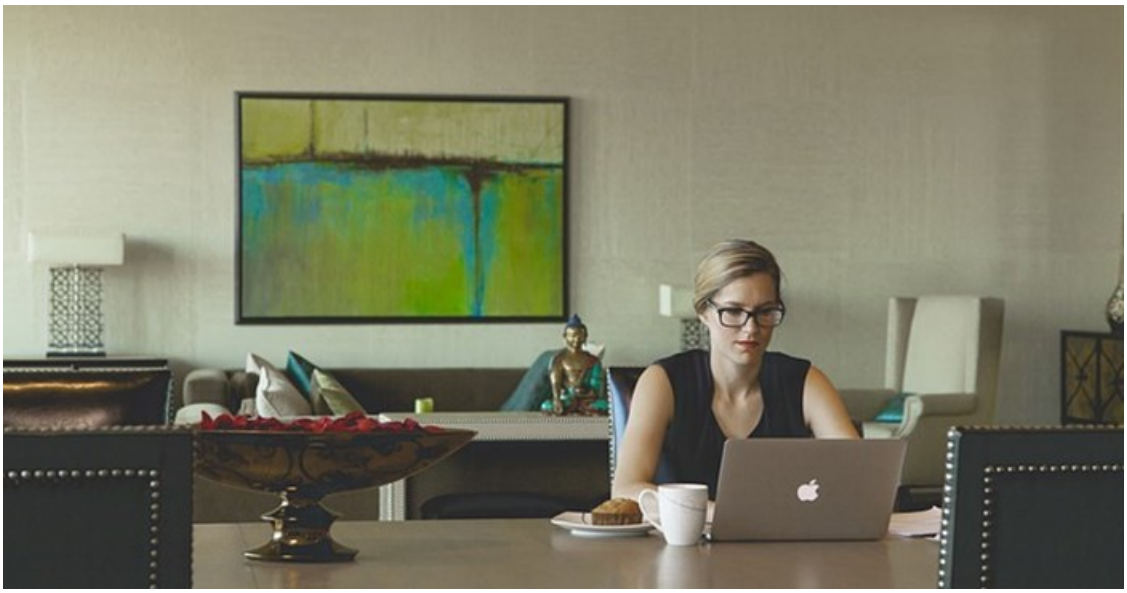
BIZCOMMUNITY

Five tips for securing the home office successfully

By Peter Davidson

9 Oct 2015

The ability to attract and keep good employees means that companies must be competitive. Sure, you can offer a 401k and health insurance, or even profit-sharing, and those these benefits are desirable, what a lot of companies are finding is that increasingly, employees value work-life balance. Included in their idea of the perfect company is the ability to work from home.



moleshko via pixabay

The ability to work from home eases day care issues and expenses and gives them a more relaxing atmosphere in which to work. It can also cut down on the long hours they would otherwise have to stay at the office when a project is due or the CEO is demanding statistics now. Many companies are also finding that allowing employees to work from home can actually cut down on their own costs. But with this perk comes security issues that should be dealt with long before your work at home strategy begins.

Policy

Before anyone is allowed to work from home, you should set up a policy that dictates the minimal requirements needed before any employee is allowed to take company data and access it from outside the workplace. As you have seen over and over again in the news, removable media is a problem with work at home employees. Your policy should state the do's and don'ts of data access and storage and you must define the penalties for violating those rules.

Another important aspect of accessing your network from outside of the company is on you. What security mechanisms are you going to put in place to minimise the potential for viruses or malware to infect your network through your employee's home office system? There are numerous ways you can mitigate the potential problems if you look at it carefully before you give the green light to your work-life balance perk.

Secure sign in

The best solution for allowing employees to work from home is to have them sign on through a Virtual Private Network (VPN). A VPN is a tunnel that the employee sign on to that is set up by the company. It is secure, is controlled by the same network protocols you have at the office and it decreases the vulnerability of the data traveling from the office to the employee's home. It offers log-on protection and password protection and is the single most important move you should

make when you allow employees' entry into your system from home.

Antivirus protection

At the office, you have antivirus protection that is constantly updated to keep abreast of potential threats that seem to be developed daily by outside forces beyond your control. Any good business owner knows that a virus or malware attack can bring a company to its knees and will likely result in loss of data that can cost a bundle. The problem with work-at-home employees is that unless you are giving them the hardware to use, you don't know what they are using to log into your network.

This is where your policy comes in. You need to include in your policy an antivirus software that updates automatically so you don't have to rely on the employee to ensure that regular updates are completed. Remember, this is your company, your data, and your network. If they want to work from home, they have to follow your policy and your policy should include the antivirus software they must install.

Storage

The ideal work-from-home environment gives your employee business-grade tools to store the data they are working on. If you provide the equipment they use to work from home, you have far more control over their ability to use removable media, download programs and install whatever else they want. You can block their ability to all of these things with permissions on the hardware's software platform. If you don't provide the equipment, your control is limited. If you offer easy to use tools to store their reports and data on your network, and allow file sharing with these tools as well, they will be less likely to give in to the temptation of just saving it to a USB drive and bringing it back to the office.

One other temptation that must be prohibited is the use of cloud storage. Cloud storage tools like Drop box and Google Drive are increasingly popular, but as a business, do you really want your company's sensitive data stored on a public, unsecured platform? Probably not. That again is where your policy comes in. Your job is to ensure that your employees' data and your customers' data are secure. Though the employee may be the one that violated policy and caused everyone's social security numbers to be stolen, ultimately you are responsible. It is your company that will bear the burden of the mistake and the tarnish on your brand name. The employee can find a new job, but the ramifications for your company doesn't disappear so easily.

ABOUT PETER DAVIDSON

Peter Davidson is a senior business associate and strives to help different brands and startups to make business decisions and strategies efficiently. He loves to share his views on the latest technologies and applications through his well-researched content pieces.

- Five tips for securing the home office successfully - 9 Oct 2015
- Predix Cloud could be the next game changer - 10 Sep 2015

View my profile and articles...