InsideCounsel

Technology: It's a BYOD World and Companies Better Learn How to Deal with It

By David J. Walton

February 17, 2012

Not too long ago companies worried about making sure that they controlled their employees' use of company-owned computers and devices. Employers had greater financial resources to buy the newest technology so, naturally, employees wanted to use these devices for both work and their personal lives. The main concern was making sure that employees did not use the company's media to do something improper.

Now, the tables have turned. As the line between work and personal lives has blurred, so has the difference between work and personal media. More than ever before, employees have tremendous access to emerging, personal technologies and are using them for work instead of their company-issued computers or mobile devices.

The increased use of personal devices at work is sometimes called "bring your own device" to work, or BYOD. BYOD creates a whole new set of problems for employers. Personal cloud storage exacerbates the issue. Services like Dropbox, iCloud, SugarSync and Boxnet allow employees to easily lease space on large servers so they can access their data from anywhere in

the world (often for free). These services aren't going away and will keep growing. Indeed, BYOD on the whole is a paradigm shift that is permanently changing the way we work.

So what should companies do to manage BYOD?

Companies must think proactively by adopting policies that protect their data while giving employees the freedom of choice they crave. These policies should include several points:

As a basic issue, employees must promise not to use any company information on personal devices for anything other than personal use.

If employees are going to use personal devices for work, they must use passwords for the devices and tell the company what the passcode is. They also should describe the type of information they want to store and promise to update the company if they get new devices or access more information than initially identified.

Many employees use cloud-based services to store and access company information. Because these services are primarily free, they are easy to use and are the best way to manage data using an iPad or another tablet device. The BYOD policy must require employees who use these services with company information to tell the company what sites they are using, provide the account information to IT, give IT permission to access the site and promise to allow IT to check the site before the employee shuts it down.

When an employee leaves the company, IT must have the right to wipe, or at least inspect, any personal computers or devices that were used to store or access the company's confidential information.

While BYOD cannot be realistically eliminated from the workplace, companies should still prohibit specific, vital types of data from being copied to or stored on these devices. In conjunction, companies should also do an assessment of their actual trade secrets. If data is clearly a trade secret, the company should customize protections for that type of information to make sure that it does not fall into the wrong hands through an employee's use of a personal device.

BYOD is rapidly changing the face of our workplace. Companies must swim with the BYOD current or drown fighting against it. They can still protect their interests in the BYOD world, but they must be vigilant in doing so.

About the Author

Dave Walton

Dave Walton is a member in Cozen O'Connor's labor & employment practice group and co-chair of the firm's e-discovery task force. He has extensive experience in litigating matters involving

restrictive covenants, trade secrets, fiduciary duties and defending employers targeted by discrimination lawsuits. He can be reached at dwalton@cozen.com.