UNFETTERED BYOD POLICY COULD ENDANGER TRADE SECRECY

A survey commissioned by Cisco has found that 95 percent of the 600 businesses it surveyed allowed employees to use their own smart phones, tablets and other devices in the workplace. 76 percent of the IT managers said that this led to workers being more satisfied with their jobs, which in turn led them to be more productive. This BYOD, Bring Your Own Device trend, according to the study, brought in between $300 and $1,300 each year, in productivity gains. On the reverse side, the survey reported that 20% of all IT spending in 2014 will, for mobility initiatives, be up from 10% in 2010. Joseph Bradley, general manager of Cisco's Internet business solutions group, which commissioned the survey said, “No doubt, BYOD's difficult, and if there were a way to get out of it, IT would. It's a serious challenge. But what the survey shows is that IT understands that consumerization's actually happening and they wonder how they can create value. It's a painful process, not just to support a consumer device, but provide security. There are so many things to consider." IDC analyst Rohit Mehra said that the number of consumer devices accessing business applications inside of an enterprise is still relatively small, estimating that only around 41 percent were used for this purpose. "It's one thing to just let an employee-owned device on the [corporate Wi-Fi] network [for browsing or social networking] and not allow access to enterprise applications, and that penetration is pretty high. But the real proof in the pudding is how many users have true enterprise application access with their devices, and those numbers are still relatively low." Companies with a liberal BYOD policy would do well to adopt mobile device management software that will help monitor, manage and secure mobile network environments. With the thousands of applications available and the far-reaching range of the devices, security threats are considerable. MDM Solutions ensure that the company’s mobile network is protected and safeguarded from such malicious applications. Wichita Falls, Texas, has found a way to circumvent the ad hoc use of consumer devices by executing rollouts of Smartphone’s and tablets to reduce costs. The company has rolled out 7 iPad 2 tablets to municipal court workers, including Municipal Court Judge Larry Gillen, to reduce paperwork and backlogs for traffic ticket and other non-criminal legal proceedings. Patrick Gray, database applications analyst for Wichita Falls said, “The judge can even easily work on cases remotely when defendants aren't in the same location. He can work on the move, and a two months' wait for a record under the old system might be a two-minute wait." Gray said although he could not put a specific figure on the amount saved, "It's cost effective and paying for itself. There's savings in paper and to the community looking up documents." Companies that adopt a Bring Your Own Device Program would do well to take the following precautions. Specify clearly to your workers, which phones and tablets are permitted and which are not. Establish an inflexible security policy for the use of the devices. Insist that workers must accept a company password for their devices. There is too much sensitive information that could be misused if unregulated use of the device is allowed at the workplace. Define a clear policy regarding the BYOD criteria to the employees. What sort of support will be provided for the devices? What initial connections will be provided? What will be done in case of broken devices? It should be abundantly clear to the employee, that they own the device but the data belongs to the company and that the company reserves the right to erase data, in case of lost or misplaced devices, even if it means that personal pictures, personal data and personal music may also get erased in the process. A serious question to address is whether the users will be allowed to download, install and use an application that presents security or legal risks. Or whether, he is exposing the company to copyright infringement by downloading unauthorized movies or music? Last but not the least, it is important to set up an employee exit policy. This is to ensure that when the employee leaves the company, all data, information, email access and proprietary applications are removed. Want to see which IT manager jobs are available near you? Click here to see.