CARLTON FIELDS

Allowing employees to connect own devices has risks, benefits

January 29, 2014

Smartphones and tablets are everywhere. People are spending more and more money to have the latest smart devices, and employers are struggling to keep up with employees' demands for the latest technology. Not surprisingly. companies have realized there is a less expensive way to deploy the latest technology: increasingly they are allowing employees to connect to corporate networks from the devices they own. This phenomenon has become known as bring your own device, or BYOD. The benefits of BYOD are obvious: companies spend less on equipment, employees can use their preferred devices, and they need only have one of each (I remember carrying two phones for awhile – one for work and one personal-it was a nightmare). Surveys have shown BYOD helps employees work faster and smarter, making them more efficient and raising their overall effectiveness. BYOD is also believed to raise workplace satisfaction because employees get to work on the devices they are most comfortable with, eliminating the need for training on multiple operating systems or programs. But with these benefits come some major risks. Data loss is the most significant risk to companies that implement BYOD programs. By relinquishing some control and allowing devices from "the wild" to access internal networks, companies place their information systems and sensitive data at greater risk. Implementing a BYOD program means the company's network will be accessed by a wide array of devices from open Internet connections (think Starbucks). These devices will have different software, different apps and, most scary of all, different owners accessing different files from different places. Human error remains the single-biggest threat to information security. **Security Policies**

To protect their networks from all these new dangers, companies will have to implement comprehensive BYOD security programs that include strong policies and governance rules. These rules and procedures will have to be clear and concise, easy to follow and transparent so that employees will not resist them. Companies also will have to invest in technology to monitor and secure their networks and all the new devices accessing their information. Many companies are turning to mobile device management, or MDM, solutions to help safeguard their information. MDM software works by enforcing security rules and protocols on all the devices that access the company's network. For MDM to work effectively, the software must be installed on every single

device that accesses the network. This presents the second major risk of BYOD: company management of privately owned devices. MDM software gives companies a lot of power over their employees' privately owned devices. This raises many privacy questions that must be addressed. For example, how much access and control is too much? How can companies balance increasing security with employee privacy? The answers to these questions are not yet clear, but companies cannot wait to see what happens or they will risk losing talent and efficiency. So, what can a company do to avoid the privacy pitfalls of BYOD? Let's revisit the BYOD policy and governance program mentioned above. Before implementing a BYOD program and before installing any software on employees' devices, companies must inform and train employees about their BYOD program. Transparency will be a key component to successfully implementing a BYOD program. Additionally, employers should request and receive consent from employees before installing software on their devices. Companies should explain the capabilities of the software to their employees and disclose what data is being collected about them and how it is being used. Everything should be memorialized in policies and procedures written by lawyers, not information technology managers. Finally, companies should take care to follow their own policies and keep employees updated on any changes to the BYOD program. Failing to be transparent, not following your own policies and not disclosing all the elements of the program can be catastrophic. This will be perceived as deception, create conflict and possibly lead to litigation. BYOD is here to stay and employers are scrambling to put the technical safeguards in place to take advantage of it. The benefits of embracing new technologies come with responsibilities that companies increase their networks' security and respect their employees' privacy, By investing in now technology and implementing comprehensive and commonsense policies that are understandable and transparent, companies can try to manage the risks they must take to remain competitive. *Originally published by the Daily Business Review, Vol. 88, No. 159 (January 2014).*

Related Practices

Technology
Business Transactions
Cybersecurity and Privacy

Related Industries

Technology