The “Bring Your Own Device” Boon Comes at the Expense of Security. How Can You Protect Your Business?

By Cody Cooper

Bring your own device policies in the workplace aren’t novel. Companies have experimented and implemented policies requiring employees to use their own personal phones, computers and tablets in the scope of their employment rather than the employer providing these devices. There are certainly benefits to companies that offer the flexibility of “bringing your own device.” Companies can reduce or avoid large hardware costs. Employees enjoy the freedom to choose and use the technologies they already love compared to juggling a Blackberry for work and an iPhone for friends and family. Additionally, by using a personal device, employees tend to be “connected” and available more than with an employer-provided device.

Now, while you may think, “you mean I can require to employees to bring their own electronic devices and never have to worry about the costs and resources for maintaining or upgrading those devices? SIGN ME UP!” Not so fast. While there are certainly benefits to BYOD policies, there are also potential pitfalls.

Who owns the information on the phone?

Particularly where a company’s value is primarily driven from the information it creates and maintains, BYOD policies can prove dangerous. Oklahoma law protects information that is considered to be “trade secret,” being information that derives independent value and where there are reasonable efforts to keep it secret. Examples are customer lists or

business research (think geological surveys showing potential oil reserves). Although Oklahoma law protects this sort of information from theft, enforcing an employer's rights can prove time-consuming and costly and sometimes even unsuccessful. While an employer could confiscate and completely erase a company-owned phone in the event an employee is fired, the same may present potential legal issues if it is the employee's personal phone and contains their personal information.

You can't fire me, I quit!

By allowing employees to bring their own device and then use that device for work, employers are now placing potentially incredibly sensitive information in the hands of its employees. As any employer knows, employees are sometimes prone to change their mind and seek employment elsewhere or need to be let go for whatever reason. This presents an incredible risk depending on the employer's line of business and the employee's role. Particularly where sensitive email information is frequently shared or contacts are vital (i.e. sales centric businesses) the potential for data misappropriation is high.

There are now a number of programs for cellphones, tablets and personal computers (laptops or desktops) that create what is essentially a biodome of employer information residing within a secure environment on the user's computer, while restricting the user from copying information or other potential acts of abuse. This could be the saving grace for companies that are particularly sensitive to data loss.

Increasing the e-discovery pie

E-discovery is growing at an exponential rate and as employers rely more and more on computers and computer systems, it will continue to do so. In a lawsuit, parties are generally entitled to discovery any information that is relevant to the suit. Having employees use personal devices will require

employers to collect, preserve and review the information on the devices for relevant information in the event of a lawsuit. This further broadens the scope of discoverable information and increases the costs of these efforts for the employer.

The effects of BYOD are still being realized

These are just two of the major concerns of BYOD policies, but there are more. Privacy rights of an employee can obviously come into play with the use of personal devices at work as well as acceptable use and non-use of the devices both at work and away. Even with the potential downsides, BYOD policies can be an excellent tool for business looking to shed the cost and burden of maintaining personal devices for their employees. It is important to consult with an attorney in drafting an effective BYOD policy to ensure that the individual needs of your business are taken into consideration along with the ever-changing laws. First look introspectively to determine how much you value your information and ask what the cost of releasing some of the control of that information is worth to you. Then, if you think the potential risks are outweighed by the benefits, say goodbye to all those BlackBerrys you'll never buy again!