Insights, News & Events

BLURRING THE LINE BETWEEN YOURS AND MINE: BEST PRACTICES FOR BRING YOUR OWN DEVICE POLICIES

Publication
Jun 1, 2014

Let's face it: bring-your-own-device (BYOD) situations are here to stay. With the ubiquity of employees having and using smartphones and tablets – devices that have more capacity and processing power than desktop computers from not so long ago – it was inevitable that employees would eventually start to use their own devices in a work capacity. This new reality presents benefits for employers, as their employees can now be productive away from the office and be responsive to work situations as they arise. Additionally, there are cost savings that can be achieved when an employer is no longer responsible for supplying devices to its employees.

The situation also benefits employees, as they often derive personal satisfaction from being able to link up their own preferred devices to the work system, creating a little node of personalization in an environment that they do not otherwise control. Surveys reflect that a significant percentage of job seekers will view a prospective employer more favorably if it has an IT system that supports the seekers' personal devices.

But if employers do not manage BYOD scenarios proactively, then they present risks in addition to rewards. To state the obvious, when your company's information is being sent, received, and stored over a device that you do not own, then the specter of data loss is present. This risk can come from an employee who intends to hurt the company by taking information and either using it on behalf of a competitor, or simply disclosing it to cause embarrassment. It can also

Related People

Michael P. Elkon
Partner
404.240.5849

come from an employee who inadvertently retains or loses it.

Either way, the employer that thinks through BYOD issues in advance and charts out rational, balanced policies before issues arise is going to place itself ahead of the game. Here are some best practices for BYOD situations:

HAVE TECHNOLOGY IN PLACE TO PROTECT YOUR INFORMATION

Take the typical employee's smartphone. Some employers require that the employee use an employer-issued email application like Good Technology. Other employers require that their employees download an application that allows the employer to shut down or access a device in certain circumstances. Some employers take the simple step of requiring that employees activate passcode protection on their devices, a policy that costs nothing because just about every device contains this option.

Regardless which of these options an employer chooses, it is the most basic step in dealing with BYOD situations. You need to acknowledge and deal with the fact that if your information is going to migrate to your employees' personal devices, then those devices need protection measures in place to ensure that the information is not lost or stolen.

THINK THROUGH YOUR KEY INFORMATION AND TAKE STEPS TO PROTECT IT

Some information is simply too important to permit it to migrate to an employee's personal device. Even with one of the data-security fixes in place, an employer might worry about information that remains on the device after the end of the individual's employment or that an employee will leave the device unattended for a moment and allow a third party to see sensitive information on the screen.

It's important to ask yourself three questions. First, what information would be most useful to its competitors if an employee left with it? Second, what information would be most embarrassing if it were leaked to the general public? Third, if asked on a witness stand "how many measures do you take to ensure that the company's most valuable, sensitive information remains private?" what would you or your Human Resources manager say in response? It's valuable to put yourself through this sort of self-critical

analysis in many scenarios; but it is specifically important in addressing BYOD situations.

MAKE CLEAR THAT EMPLOYEES CANNOT MISUSE THE COMPUTER SYSTEM

With the increased use of the federal Computer Fraud and Abuse Act and analogous state computer-protection statutes, employers are learning the importance of putting employees on written notice as to what they are not authorized to do on the company computer system. This includes both taking files from the system (such as by emailing files out as attachments or saving them to thumb drives) and deleting files prior to departure.

The key to unlocking the power of federal and state computer-protection laws is showing that the employees were on notice that they were not authorized to perform certain acts on the system. This general rule extends to BYOD policies. Put your employees on notice as to what they can and cannot do with respect to company information on their devices.

Just as it is helpful to think through confidential information issues in advance, it is also worthwhile to spend some time addressing common employee misconduct or negligence scenarios involving data security on personal devices and then covering them with written policies. A policy laying out general rules and then covering specific scenarios in an "including, but not limited to" string (a construction much beloved by lawyers) is ideal.

PAY FOR THE EMPLOYEE'S CELL PHONE

In the grand scheme of things, it is penny wise and pound foolish to have key employees pay for their own cell phone plans. If a company owns and maintains the account, then it can: a) terminate the account when an employee leaves so customers cannot reach out to him or her; b) determine whom the employee has been contacting in the final weeks with the company by reviewing call and text logs; and c) stop the employee from walking out with a de facto customer list on the phone. Thus, while employees might choose to use their own devices at work, you can still control the account and thus still be in command of the information on a device.

EMPLOY TIGHT EXIT PROCEDURES FOR DEPARTING EMPLOYEES

Perhaps the number one issue with the BYOD phenomenon is that when employees use their own devices, they end up with a large quantity of employer information on those devices. Whether intentionally or inadvertently, when those employees resign or are fired, they leave with a treasure trove of information. That information can be used to compete. It can be used to stir up issues with the employees who remain. It can be disclosed on social media or to reporters.

Therefore, it is critical to create and follow established exit procedures, so that when an employee leaves, you can show that you did everything in your power to get the company's information back. These procedures will never be foolproof against employees who choose to keep information on their devices, but at a minimum, it will help put you in a position to show that you took all reasonable steps to maintain the confidentiality of its key information.

The issue of protecting against data loss resulting from employees using their personal devices for work is a classic example of the maxim that an ounce of prevention is worth a pound of cure. Relatively small expenditures of time and money on the front end can deter an employee from exploiting key information on a personal device; can protect against that same employee accidentally losing information to a third party; and can position the company to recover the information if it is indeed lost. The critical first step is to acknowledge the reality of employees using their own devices and to plan accordingly.

For more information, contact the author at MElkon@fisherphillips.com or 404.231.1400.