BYOD? OMG!

Brian M. Gaff, McDermott Will & Emery, LLP

Bring Your Own Device—allowing employees to bring personally owned technology to their workplaces might improve productivity, but it also creates risks for employers.

BYOD isn’t just a new catchphrase, it’s a growing trend in which companies permit—and even encourage—their employees to use their personally owned devices, such as smartphones and tablets, on the job. Although this might seem attractive, it can make a company’s IT systems and data more vulnerable to malicious activity.

For an expanded discussion on this topic, listen to the podcast that accompanies this column at www.computer.org/computing-and-the-law.

WHAT IS BYOD?
It’s common for employees to bring their own devices to their workplaces so they can maintain contact with family and friends. In those instances, employees use their devices exclusively for personal reasons. Employers usually don’t take issue with that except, perhaps, if it becomes disruptive, hampers productivity, or creates a security risk (for example, if it’s used where classified materials are present).

BYOD refers to the use of these personal devices for business purposes and reflects a blurring of the line between personal and business use on the same device. For example, an employee might use his smartphone to access the company’s email system and read and respond to emails in connection with his job. He likewise might make telephone calls or send and receive text messages that are business related.

If a company allows the use of personally owned devices for business purposes, it needs to have a policy in place that, among other things, ensures the security of its systems, protects the confidentiality of its corporate materials, and respects the privacy of employees. The latter is particularly important, because employees undoubtedly have significant amounts of personal information on their devices.

REASONS FOR BYOD
Some argue that allowing employees to use their personally owned devices for work-related purposes will increase productivity. An underlying theory for this is that employees are more attuned to their personal devices and will therefore use them more efficiently and even in some cases use them for work during their off-hours as well. Personally owned devices are typically more advanced compared to those that are employer issued, and most people usually prefer having newer-generation technology.

An employer that allows BYOD might create the perception that it’s more accommodating to employees’ needs and, therefore, a preferred place to work. This can help with recruitment and potentially improve employee morale. Also, there’s the potential of reducing costs. Moving some or all of the device acquisition and usage costs from the employer to the employee could benefit the employer.

Another reason for allowing BYOD is that it’s likely a fait accompli: many employers probably can’t prevent employees from using their devices at work, so adapting to that reality might be the only reasonable option.

See www.computer.org/computer-multimedia for multimedia content related to this article.
POLICIES TO SUPPORT BYOD

Employers need to have a BYOD policy in place, and employees need to understand it, to protect the interests of both.

At a minimum, a policy should define the devices that are and aren’t acceptable for use in a BYOD context. Only certain brands, models, or configurations might be approved because of security or support requirements. If an employee isn’t able to use one of the approved devices, then BYOD won’t be an option.

The support issue is important. Unless the employer wants to make the investment to provide technical support for numerous and varied types of devices, setting limits on the types of devices is essential. The policy should set expectations as to the level of technical support available to employees using personally owned devices.

Even when an employee is using an approved device, the policy might need to restrict some of the device’s capabilities when it’s used for work-related purposes. For example, cameras could be prohibited in certain high-security environments. A policy might therefore require that the device’s camera be automatically disabled when connected to the employer’s network or when located in a certain area as determined by GPS.

To limit the likelihood of malware being introduced to the employer’s systems, the policy might prohibit the installation of certain apps, or only allow the installation of apps from trusted sources. Further, the policy could limit how acceptable apps are used, which could include mandatory Web filtering.

The policy should define what employer systems and apps the employee is allowed to access on a personally owned device. This can range from limited access to just email to full access to R&D and production management systems. The employer needs to delineate the boundaries, which can be based on the employee’s job responsibilities.

OWNERSHIP ISSUES

Having well-defined boundaries in place should help resolve the ownership issues. It’s generally clear that the employee owns the device itself and the personal information stored on it. However, the policy should spell out that information stored on the device that’s obtained from the employer’s systems, as well as any of the apps installed on the device for work-related purposes, remain the property of the employer.

Ownership becomes important when an employee loses his device. It’s important that the policy address this situation, as it can help limit the likelihood of a data breach. If the device can access the employer’s systems, or if the device has the employer’s information on it, the policy needs to allow the employer to remotely wipe the device to protect its systems and materials. As the term implies, “wipe” usually means deleting all information from the device, and that includes the employee’s personal information, such as contacts, email, and photographs. That’s potentially a significant loss for the employee, who will need to accept that consequence. Also, an employer might require a wipe in situations where the device isn’t lost; for example, when the employee leaves the company and takes his personally owned device with him. The employee needs to accept that as well.

The employer should consider requiring passwords for and encryption of employees’ devices. This doesn’t eliminate the need to wipe a lost device. However, it provides an additional layer of security for a device that’s lost but not yet wiped. Again, employees need to consent to this.

A BYOD policy might include terms that restrict how the device is used during personal time and off the employer’s premises. For example, the policy might mandate that the device not be used such that it creates a dangerous distraction—for example, prohibiting its use while driving. The scope and enforceability of limitations like these should be discussed with a lawyer.

For companies that have been involved in litigation, the depth and complexity of the discovery phase of the litigation can be daunting. During this phase, documents, email, memoranda, and the like that are relevant to the dispute at issue are typically retrieved and closely examined. To the extent that employees have relevant information on their personally owned devices, it’s possible that a litigation adversary will demand access to the devices. Whether the employee must consent to this should be part of the policy.

BYOD policy is essentially a contract between an employer and employee. In return for granting access to the employer’s systems and information, the employee agrees to abide by certain terms and conditions. For the policy to be enforceable, the terms and conditions should be reasonable and comply with the applicable laws and regulations, including those relating to employee privacy. That might include simultaneously complying with laws and regulations from multiple jurisdictions for employers that operate in different states and countries. Work closely with your lawyer to ensure that your BYOD policy is comprehensive and enforceable.

BRIAN M. GAFF is a senior member of IEEE and a partner at the McDermott Will & Emery, LLP law firm. Contact him at bgaff@mwe.com.