BY JOE STODDARD

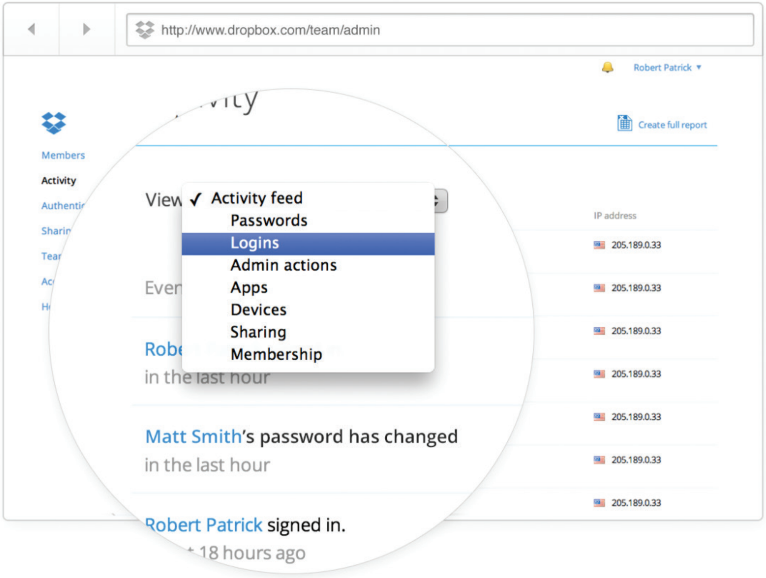
Bring Your Own Device

Bring Your Own Device (**BYOD**) is a trend among employees and subcontractors who resist using employer-supplied mobile hardware in favor of using their own personal smartphone, tablet, or laptop for work. BYOD is nothing new, but the potential effects on businesses are changing fast. Ten years ago, the occasional BYOD request came from an "early adopter" asking to use a personal laptop for work, possibly before the company itself had been computerized. Today, practically every company is using technology, but then so is practically every employee, tradesman, and homeowner. And this year's smartphones are next year's "wearable computers" with the Internet built in. BYOD is here to stay, so you might as well start thinking about how to integrate employee-owned technology with company systems.

When it comes to office technology, adoption is everything. If people are unwilling or unable to use the systems you set up, the whole initiative will never get off the ground. BYOD is not a cure-all, but people are much more likely to use a device that they're already familiar with—and that is already set up just the way they like it—than they are to use a company-issued device.

The problem is that a device which is set up "just the way they like it" is often at odds with what is best for your business. In general, people are terrible at securing and maintaining their digital devices. Consequently, one of the first things I do for my builder and remodeler clients is to survey every device that could potentially access their network, cloud-based applications, or data, whether online or off. Then we create a policy that will allow employees and subcontractors to bring their own devices to work while reducing the potential risk to the business.

Here is a list of some of the potential BYOD issues you'll face, with suggestions for how to deal with each of them.



Even

Robe
in the last hour

Matt Smith's password has changed
in the last hour

Robert Patrick signed in.
18 hours ago

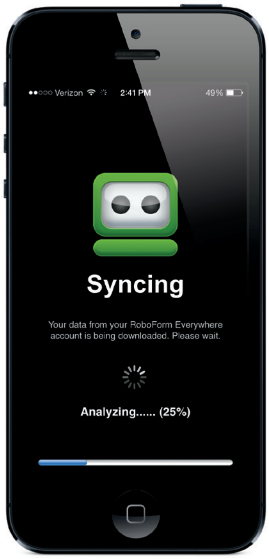
Image: courtesy Dropbox.com

Dropbox for Business provides a central administrative console where you can manage members. Members can add and edit, but they can't permanently delete files in the company's Dropbox. The administrator always has tools to recover damaged or deleted files.

Mismatched devices. If the mobile apps your company is using are designed to work best on Android smartphones, but your employee shows up with an iPhone, the mismatch—even if there is a way to make it work—could create endless technical support issues, as well as generate lots of excuses like, "I couldn't get on the project website."

Solution: Require employees (and trade contractors) to sign off on a list of approved devices that will work correctly with the apps and services your company uses. This should also include specifications for the operating system, minimum processor speed, amount of memory and storage necessary, and so forth. Update the standard annually and make it part of your employee handbook and your trade contractor agreements.

Password problems. Using weak—or no—passwords is the digital equivalent of leaving all of your doors and windows wide open, then complaining when someone breaks into your office. In my experience, most people avoid anything that slows them down when they use their technology, and having to enter passwords of any kind tops the list of obstacles. And strong passwords that are difficult to remember or enter? Fuggetaboudit.



Syncing

Your data from your RoboForm Everywhere account is being downloaded. Please wait.

Analyzing...... (25%)

Password managers such as LastPass and RoboForm (shown here on an iPhone) can keep hundreds of passwords, account numbers, credit cards, and other sensitive information secure and synchronized across multiple devices. Using these password helpers makes it less of a hassle to always use unique, strong passwords to access cloud service accounts.

Solution: You can't do much about a user's lack of common sense, but you can ensure that the cloud-based services your company uses require strong passwords—that is, eight characters or more; no "dictionary" or other easily guessed words; a mix of numbers and letters, lowercase and caps; and at least one special character. Password-management software, such as LastPass (lastpass.com) or RoboForm (roboform.com) can be a big help.

Malware. Roughly 75% of all personal devices I've surveyed have had a virus or some form of malicious software installed on them. That includes iPhones, iPads, and Android devices, which, contrary to popular belief, are not immune to malware. Sources of this junk include celebrity websites, ad pop-ups, social media, and other free software installations. It's easier to evict a deadbeat tenant from a rental property than it is to completely get rid of malware from a mobile device.

Solution: If employees are using their own devices for work, you can't control which sites they surf or what software they download, but you can insist that they install and use good anti-malware software and that they allow you to spot-check their devices to make sure they're keeping them up to date. This is easier than it sounds because most people don't want the malware hassle either. Sometimes all it takes is a bit of education about which websites and games to avoid.

No security updates. As is the case with malware protection, it's rare to find someone who regularly updates his or her operating system and software. Even when the device is set up to automatically do the updates, often the process is interrupted and never restarted and completed.

Solution: One builder I worked with allowed BYOD, but only after checking out the devices to make sure they were malware-free and fully updated. This builder scheduled the checks for times when a group of employees was together—at a weekly sales or production meeting, for example. Even though this required some hands-on attention from him, it was no more effort than it would have been had the company supplied the devices.

Personal versions of business services. Employers used to worry about employees storing sensitive company documents or other data on thumb drives or SD cards, then losing those devices or being careless about who could access them. Lost thumb drives still represent a threat, but an even more serious threat today is employees or subs using their personal cloud-based file-storage accounts for work. I'm talking about personal consumer versions of such services as

Evernote (evernote.com) and Dropbox (dropbox.com). Once your data disappears into one of these personal accounts, you've lost control of it.

Solution: Spend a little more money to purchase cloud-based services that have "business" or "professional" versions. These typically give you better control over the data created and stored, including access to it. Employees and subcontractors should be able to add and view information—and possibly edit some information—but they should never be able to delete it. If storage space is an issue, employees can make room for new files by archiving rather than deleting existing information.

The business versions of these services add an administrative interface that allows you to stay in control of who can access the service and what they can do once there (see screen image, page 27). Some services even have an option to store every version of every file forever—cheap insurance against someone accidentally deleting something important.

Unfortunately, none of these controls will stop people from making personal copies of things they shouldn't, but at least they won't be able to accidentally delete or corrupt mission-critical business data.

Other inappropriate uses. Last of the BYOD issues are those related to employees spending hours on the phone for personal calls, wasting work time surfing the Internet for fun, and publishing compromising photos—which can be something as simple as a picture of a client's address that winds up on Facebook. In my experience, these things will happen whether it's your device or the employee's, but it's arguably much easier for you to discover and control these behaviors if you supplied the hardware.

Solution: Good hiring practices along with a solid, written company policy and procedures manual go a long way here. Even if you don't allow BYOD and you supply everything yourself, you still need a good mobile-device management policy on which everybody signs off. Of course, policy alone probably isn't going to stop every employee or subcontractor from doing something they shouldn't do with the technology in their pocket, but it's part of the education process, and at least it gives you some recourse to handle a repeat offender.

Joe Stoddard consults with contractors about technology. jstoddard@mountainconsulting.com; twitter.com/moucon