The Pleasures and Pitfalls of BYOD

CASE STUDY

Just about everyone who has a smartphone wants to be able to bring it to work and use it on the job. And why not? Employees using their own smartphones would allow companies to enjoy all of the same benefits of a mobile workforce without spending their own money to purchase these devices. Smaller companies are able to go mobile without making large investments in devices and mobile services. One IBM-sponsored study by Forrester Consulting found that a BYOD program using mobile enterprise services from IBM achieved a 108 percent return on investment and payback within one month. "Anywhere/anytime" access to computing tools increased workplace productivity and raised effective employee work time by 45–60 minutes per week. According to Gartner Inc., by 2017, 50 percent of employers will require employees to supply their own mobile devices for the workplace. BYOD is becoming the "new normal."

But…wait a minute. Nearly three out of five enterprises believe that BYOD represents a growing problem for their organizations, according to a survey of 162 enterprises conducted by Osterman Research on behalf of Dell Inc. Although BYOD can improve employee job satisfaction and productivity, it also can cause a number of problems if not managed properly: support for personally owned devices is more difficult than it is for company-supplied devices, the cost of managing mobile devices can increase, and protecting corporate data and networks becomes more difficult. Research conducted by the Aberdeen Group found that on average, an enterprise with 1,000 mobile devices spends an extra $170,000 per year when it allows BYOD. So it's not that simple.

BYOD requires a significant portion of corporate IT resources dedicated to managing and maintaining a large number of devices within the organization. In the past, companies tried to limit business smartphone use to a single platform. This made it easier to keep track of each mobile device and to roll out software upgrades or fixes, because all employees were using the same devices, or at the very least, the same operating system. The most popular employer-issued smartphone used to be Research in Motion's BlackBerry, because it was considered the "most secure" mobile platform available. (BlackBerry mobile devices access corporate e-mail and data using a proprietary software and networking platform that is company-controlled and protected from outsiders.)

Today, the mobile digital landscape is much more complicated, with a variety of devices and operating systems on the market that do not have well-developed tools for administration and security. Android has over 79 percent of the worldwide smartphone market, but it is more difficult to use for corporate work than Apple mobile devices using the iOS operating system. IOS is considered a closed system and runs only on a limited number of different Apple mobile devices. In contrast, Android's fragmentation makes it more difficult and costly for corporate IT to manage. As of July 2013, there were at least 11,868 different Android-based devices were available from more than 1,700 different brands, according to a report by OpenSignal, which researches wireless networks and devices. Android's huge consumer market share attracts many hackers. Android is also vulnerable because it has an open-source architectureand comes in multiple versions.

If employees are allowed to work with more than one type of mobile device and operating system, companies need an effective way to keep track of all the devices employees are using. To access company information, the company's networks must be configured to receive connections from that device. When employees make changes to their personal phone, such as switching cellular carriers, changing their phone number, or buying a new mobile device altogether, companies will need to quickly and flexibly ensure that their employees are still able to remain productive. Firms need an efficient inventory management system that keeps track of which devices employees are using, where the device is located, whether it is being used, and what software it is equipped with. For unprepared companies, keeping track of who gets access to what data could be a nightmare.

With the large variety of phones and operating systems available, providing adequate technical support for every employee could be difficult. When employees are not able to access critical data or encounter other problems with their mobile devices, they will need assistance from the information systems department. Companies that rely on desktop computers tend to have many of the same computers with the same specs and operating systems, making tech support that much easier. Mobility introduces a new layer of variety and complexity to tech support that companies need to be prepared to handle.

There are significant concerns with securing company information accessed with mobile devices. If a device is stolen or compromised, companies need ways to ensure that sensitive or confidential information isn't freely available to anyone. Mobility puts assets and data at greater risk than if they were only located within company walls and on company machines. Companies often use technologies that allow them to wipe data from devices remotely, or encrypt data so that if it is stolen, it cannot be used. You'll find a detailed discussion of mobile security issues in Chapter 8.

IBM's CIO Jeanette Horan believes that BYOD may cause as many problems as it solves. BYOD was not saving IBM any money and had actually created new challenges for the IT department because employees' devices are full of software that IBM doesn't control. IBM provides secure BlackBerrys for about 40,000 of its 400,000 workers while allowing 80,000 more employees to use their own smartphones or tablets to access IBM networks.

The IBM IT department found it had no grasp of which apps and services employees were using on their personal devices, and employees themselves were "blissfully unaware" of the security risks posed by popular apps. IBM decided to ban the use of such popular services as the Dropbox cloud-based cyberlocker, fearing that employees would put IBM-sensitive information in their personal Dropbox accounts, forward internal email to public Web mail services, or use their smartphones as mobile Wi-Fi hotspots. According to research by the International Data Company (IDC), 20 percent of corporate employees using personal cloud storage services admitted to using them to store enterprise data, so this is becoming a serious problem.

IBM will not allow an employee to access its corporate networks with his or her personal device unless it secures the device. The IT department configures the device so that its memory can be erased remotely if it is lost or stolen. The IT group also disables public file-transfer programs like Apple's iCloud; instead, employees use an IBM-hosted version called MyMobileHub. IBM even turns off Siri, the voice-activated personal assistant, on employees' iPhones because the spoken queries are uploaded to Apple servers.

Each employee's device is treated differently, depending on the model and the job responsibilities of the person using it. Some people are only allowed to receive IBM e-mail, calendars, and contacts on their portable devices, while others can access internal IBM applications and files (see Chapter 8). IBM equips the mobile devices of the latter category of employees with additional software, such as programs that encrypt information as it travels to and from corporate networks.

One company that has successfully implemented BYOD is Intel Corporation, the giant semiconductor company. About 70 percent of the 39,000 devices registered on its network are personal devices. Intel approached in BYOD in a positive manner, trying to find ways to make it work rather than to defeat it. Diane Bryant, then Intel's CIO, didn't want to be dependent on a single mobile vendor or device.

Intel hammered out a BYOD strategy and created an end-user service-level agreement that clarified that end users were voluntarily using BYOD rather than being mandated by Intel. The company developed different policies, rules, and access limits for each type of device-smartphone, tablet, or laptop—with multiple levels of controls in place. Intel maintains a list of approved devices. If a device does not meet its requirements, it is blocked from the network. Intel's BYOD program today offers 40 proprietary applications, including travel tools to help schedule a flight and conference room finders. The company has an internal "app store" and uses a variety of software and security tools, including mobile device management (MDM) software and mobile app management (MAM) software.

Intel's goal for BYOD is not to save money but to make employees happier and more productive. Employees like being able to use their own device and apps alongside specialized Intel apps. On average, Intel workers report that bringing their own devices saves them about 57 minutes per day, which amounts to 5 million hours annually company-wide.

Canadian Tire decided not to allow BYOD at all and issued new BlackBarry Q10 and Z10 smartphones to its 3,000 corporate employees. (Canadian Tire is one of Canada's largest companies, with an online e-commerce store and 1,200 retail outlets selling automotive, sports, leisure, home products, and apparel; petroleum outlets; and financial services.) The company felt that for its purposes, the bring-your-own-device model was not sufficiently secure. Canadian Tire's chief technology officer (CTO) Eugene Roman worries that an email could sent a virus into the company's core infrastructure. At present, Canadian Tire's management thinks BYOD is interesting but is not yet ready for the company's mainstream business applications.

In order to successfully deploy mobile devices, companies need to carefully examine their business processes and determine whether or not mobility makes sense for them. Not every firm will benefit from mobility to the same degree. Without a clear idea of how exactly mobile devices fit into the long term plans for the firm, companies will end up wasting their money on unnecessary devices and programs.

Sources: Dennis McCafferty, "Surprising Facts About Mobility and BYOD," Baseline, January 29, 2014; Beatrice Piquer-Durand, "BYOD and BYOA: Dangers and Complications," Techradar Pro, March 24, 2014; Tam Harbert, "Android Invades the Enterprise," Computerworld BYOD Consumerization of IT," November 2013; Forrester Consulting, "The Total Economic Impact of IBM Managed Mobility for BYOD," May 2013; Fred Donovan, "The Growing BYOD Problem," FierceMobileIT, February 13, 2013; Brian Bergstein, "IBM Faces the Perils of 'Bring Your Own Device'," MIT Technology Review, May 21, 2013; and Matt Hamblen, "Canadian Tire forgoes BYOD, Issues BlackBerries to Workers," Computerworld, May 20, 2013.

CASE STUDY QUESTIONS

5-14 What are the advantages and disadvantages of allowing employees to use their personal smartphones for work?

5-15 What management, organization, and technology factors should be addressed when deciding whether to allow employees to use their personal smartphones for work?

5-16 Compare the BYOD experiences of IBM and Intel. Why did BYOD at Intel work so well?

5-17 Allowing employees use their own smartphones for work will save the company money. Do you agree? Why or why not?

MyMISLab

Go to **mymislab.com** for the following Assisted-graded writing questions.

5-18 What are the distinguishing characteristics of cloud computing and what are the three types of cloud services?

5-19 What is the total cost of ownership of technology assets and what are its cost components?