GLOBAL EDITION

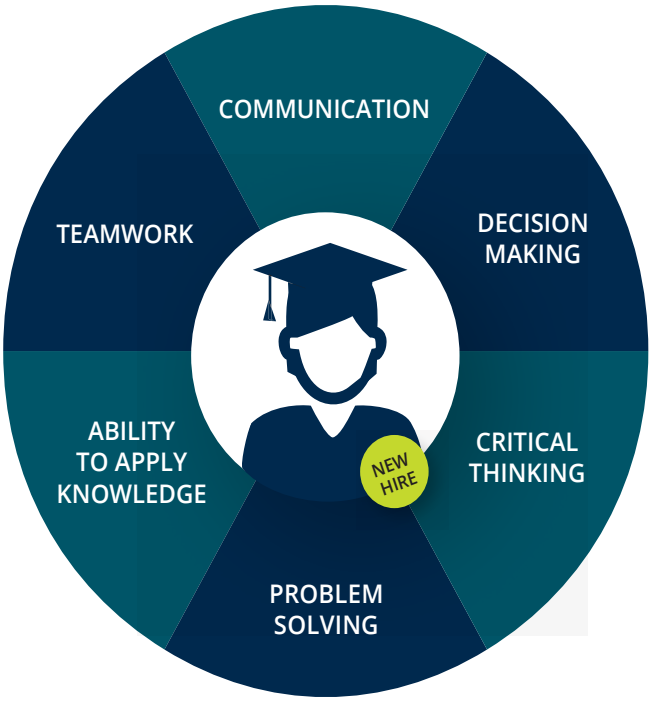
Using MIS

TENTH EDITION

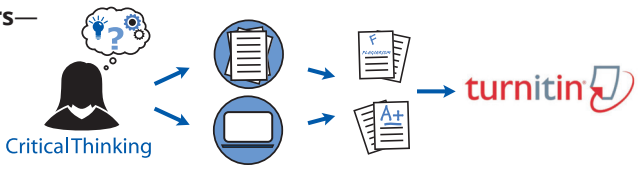
David M. Kroenke • Randall J. Boyle

Pearson

MIS: Engage, Apply, Empower



- **Writing Space**—Better writers make better **communicators**—who become better managers. Designed to help develop and assess concept mastery and **critical thinking**, the Writing Space offers assisted auto-graded writing assignments so students can receive meaningful, personalized feedback quickly and easily. And because of Intergration with Turnitin®, Writing Space can check students' work for improper citation or plagiarism.



Q4-7 What Are the Challenges of Personal Mobile Devices at Work?

So far, we've focused on mobile applications that organizations create for their customers and others to use. In this question we will address the use of mobile systems *within* organizations.

In truth, organizations today have a love/hate relationship with their employees' use of their own mobile devices at work. They love the cost-saving possibility of having employees buy their own hardware, but they hate the increased vulnerability and loss of control. The result, at least today, is a wide array of organizational attitudes.

Consider a recent report by Tech Pro Research that estimates 74 percent of companies have adopted BYOD or are planing to do so.[40] If you aren't already bringing your own device to work, you'll soon have to. Yet only 43 percent of all organizations have created an official mobile-use policy.[41]

Advantages and Disadvantages of Employee Use of Mobile Systems at Work

Figure 4-24 summarizes the advantages and disadvantages of employee use of mobile systems at work. Advantages include the cost savings just mentioned as well as greater employee satisfaction of using devices that they chose according to their own preferences rather than organization-supplied PCs. Because employees are already using these devices for their own purposes, they need less training and can be more productive. All of this means reduced support costs.

On the other hand, employee use of mobile devices has significant disadvantages. First, there is the real danger of lost or damaged data. When data is brought into employee-owned computing devices, the organization loses control over where it goes or what happens to it. IBM, for example, disallowed the use of Apple's voice searching application, Siri, on employees' mobile devices for just that reason.[42] Also, if an employee loses his or her device, the data goes with it, and when employees leave the organization, the data on their personal devices needs to be deleted somehow.

Organizations also lose control over the updating of software and the applications that users employ. This control loss leads to compatibility problems; users can process data, for example edit documents, with software that is incompatible with the organization's standard software. The result to the organization is a mess of inconsistent documents.

Possibly the greatest disadvantage of employee use of their own devices is the risk of infection. The organization cannot know where the users have been with their devices or what they've done when they've been there. The possibility of severe viruses infecting the organization's networks is real. Finally, all of these disadvantages can also lead, ironically, to greater support costs.

Given all that, organizations cannot avoid the issue. Whatever the costs and risks, employees are bringing their own devices to work. Ignoring the issue will simply make matters worse.

Advantages	Disadvantages
Cost savings	Data loss or damage
Greater employee satisfaction	Loss of control
Reduced need for training	Compatibility problems
Higher productivity	Risk of infection
Reduced support costs	Greater support costs

FIGURE 4-24
Advantages and Disadvantages of Employee Use of Mobile Systems at Work

Survey of Organizational BYOD Policy

A **bring your own device (BYOD) policy** is a statement concerning employees' permissions and responsibilities when they use their own device for organizational business. Figure 4-25 arranges BYOD policies according to functionality and control. Starting in the lower left-hand corner, the most primitive policy is to ignore mobile use. That posture, which provides neither functionality to the employee nor control to the organization, has no advantages and, as just stated, cannot last.

The next step up in functionality is for the organization to offer its wireless network to mobile devices, as if it were a coffee shop. The advantage to the organization of this policy is that the organization can sniff employees' mobile traffic, thus learning how employees are using their devices (and time) during work.

The next policy provides more functionality and somewhat more control. Here the organization creates secure application services using https (explained in Chapter 10) that require employee sign-on and can be accessed from any device, mobile or not. Such applications can be used when employees are at work or elsewhere. These services provide controlled access to some organizations' assets.

A fourth policy is more of a strategic maneuver than a policy. The organization tells employees that they can sign on to the organization's network with their mobile devices, but the employee is financially responsible for any damage he or she does. The hope is that few employees know what their exposure is and hence decide not to do so.

A more enlightened policy is to manage the users' devices as if they were owned by the organization. With this policy, employees turn over their mobile devices to the IS department, which cleanses and reloads software and installs programs that enable the IS department to manage the device remotely. Numerous vendors license products called **mobile device management (MDM) software** that assist this process. These products install and update software, back up and restore mobile devices, wipe employer software and data from devices in the event the device is lost or the employee leaves the company, report usage, and provide other mobile device management data.

This policy benefits the organization, but some employees resist turning over the management of their own hardware to the organization. This resistance can be softened if the organization pays at least a portion of the hardware expense.

The most controlling policy is for the organization to declare that it owns any mobile device that employees connect to its network. To be enforceable, this policy must be part of the employee's contract. It is taken by organizations that manage very secure operations and environments.

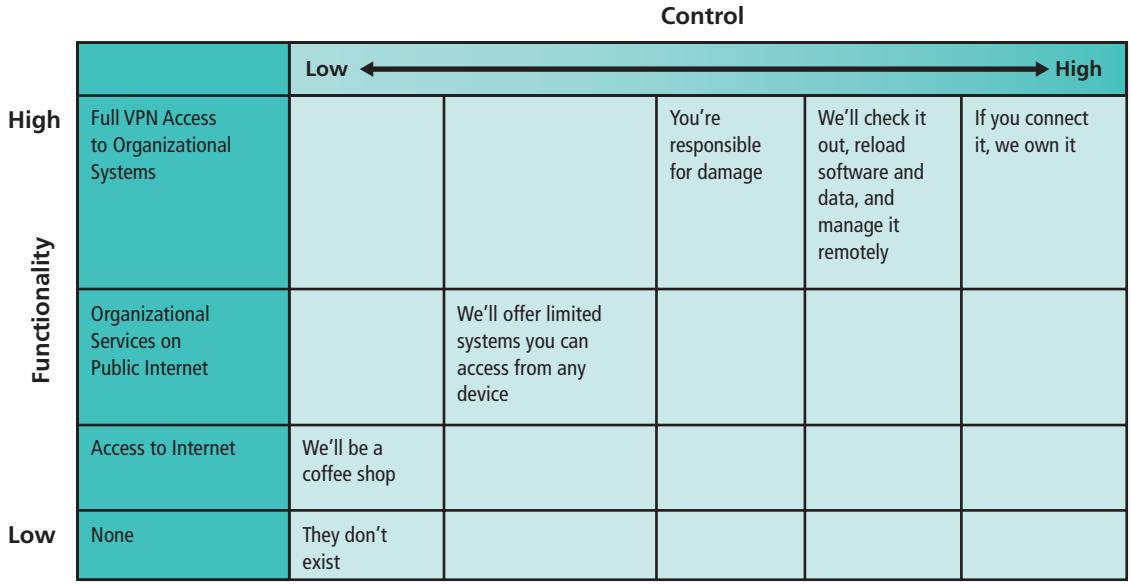


FIGURE 4-25
Six Common BYOD Policies

BYOD Policy	Description	Advantage to Organization
They don't exist	Organization looks the other way when employees bring mobile devices to work.	None
We'll be a coffee shop	You'll be able to sign in to our wireless network using your mobile device.	Packet sniffing of employee mobile device use at work.
We'll offer limited systems you can access from any device	Organization creates https applications with sign-in and offers access to noncritical business systems.	Employees gain public access from any device, not just mobile devices, without having to use VPN accounts.
You're responsible for damage	Threatening posture to discourage employee use of mobile devices at work.	Appear to be permissive without actually being so.
We'll check it out, reload software, then manage remotely	Employees can use their mobile devices just as if they were computers provided by the corporate IS department.	Employee buys the hardware (perhaps with an employer's contribution).
If you connect it, we own it	Employees are not to use mobile devices at work. If they do, they lose them. Part of employment agreement.	Ultimate in control for highly secure work situations (intelligence, military).

FIGURE 4-26
Advantages of Example BYOD Policies

In some military/intelligence organizations, the policy is that any smart device that ever enters the workplace may never leave it. The advantages of these six policies are summarized in Figure 4-26.

BYOD policies are rapidly evolving, and many organizations have not yet determined what is best for them. If your employer has a committee to develop such policies, join it if you can. Doing so will provide a great way to gain exposure to the leading technology thinkers at your organization.

Q4-8 2027?

There's a really old movie called *You've Got Mail* (1998) starring Tom Hanks and Meg Ryan. In it, the characters get really excited when they get "mail." The term *email* was so new at the time that it hadn't even caught on yet. You can see people in the movie reading newspapers and paper books. Oh, how times have changed.

Fast-forward to today. Email now comes in seconds after it's sent. You check your email during commercial breaks while you're watching TV, while you're driving in traffic, and while you're sitting on the toilet. Instead of checking your email with bated breath, you're dreading seeing more work pile up in your inbox. Or worse—bills, spam, and viruses.

New hardware and software have changed everyday life. People are always on, always connected, always communicating, always working and playing. This trend will continue. The Internet of Things will allow us to be continually connected to more and more devices. You'll be able to control your home, and everything in it, from your smartphone. Your home will be so smart that it will analyze you. It will see what, how, and when you do things and then anticipate your needs.

SECURITY GUIDE

POISONED APP-LES

Have you ever stopped to look up at the stars on a clear night and seen a faint white light tracking slowly across the sky? If so, you've seen a satellite orbiting the earth at speeds exceeding thousands of miles per hour. What may surprise you is that early spacecraft launched by NASA had less computing power than your smartphone. That's right—the small handheld device you use for checking social media and email and for playing games is more powerful than the first spacecraft. But why do you need all of that computing power? Phone calls and text messages don't seem to require massive processing power. Welcome to the era of the "app"!

Apps are the drivers of faster and more powerful smartphones. Apple and other smartphone manufacturers release new versions of their phones on an annual basis. Keeping up with the flashiest and most powerful apps drives the demand for faster processing chips and more memory. Advancements in both of these areas often happen without increasing the form factor of the phone or reducing battery life.

Smartphone users have a seemingly insatiable appetite for apps. In 2014, the Apple App Store contained more than 1.2 million apps, reported 75 billion app downloads, and listed 9 million registered app developers.[43] These apps allow you to do everything from making stock trades on the go to checking the latest weather conditions anywhere in the world. While most apps cost only a few dollars, many of them are free. You may be wondering, "How is this possible?" and "Are there any hidden costs?" You may be surprised to learn that free apps may not be such a great deal after all.

XcodeGhost Haunts iOS

The App Store is generally a well-regulated marketplace. Apps are screened for security vulnerabilities and vulgar content in order to create a safe experience for users. However, with more than a million applications available to consumers, it is inevitable that some malicious apps clear the screening process.

Apple recently reported that dozens of apps available on the App Store contained a malware application named XcodeGhost. Apps containing this malware reportedly accessed user credentials, hijacked URLs, were able to read and write data on devices, and compromised other iOS apps. WeChat, an app used extensively in China, was affected by XcodeGhost and contributed heavily to the tally of more than 500 million iOS users who could have been exposed to this dangerous malware.[44]

The malware was embedded in apps available on the App Store because developers chose to install a compromised version of the Xcode developers kit despite warnings that the software had been altered. Developers were downloading the compromised software because it had been posted on a server offering faster-than-standard download speeds.

Once this vulnerability had been identified, Apple notified users that the dangerous apps had been removed from the App Store and that they were collaborating with developers to ensure that this type of incident does not happen again. However, even with these apps identified and removed,

Source: © CarmenMurillo/iStock/Getty Images Plus

this security breach begs the question "What other vulnerabilities are lurking in the App Store, and have you already downloaded any of these potential threats?"

Installation App-rehension

Have you ever been using your phone and seen an alert message indicating that one of the apps on your phone was accessing your location information in the background? If so, were you worried? Did you allow the app to continue monitoring your location, or did you shut it off? A key point to consider is that an app does not have to be considered malware to be dangerous or invasive. In fact, many of the apps on your phone are likely accessing data that are unrelated to the app's specific purpose. For example, a survey of apps with built-in networking tools revealed that 13 out of 15 of these apps uploaded all user contacts on the phone to remote servers managed by the app developers.[45] Contact information can then be sold to advertisers and other third parties for a profit.

This type of indirect information gathering is why many of the apps downloaded from the App Store are free. End users end up paying for them with their privacy. But why do users tolerate an invasion of their privacy? Users often fail to review the usage agreement for each app.[46] Even more striking is that developers can change the terms of privacy agreements after a user has agreed to a prior version of the terms.

Despite the tremendous convenience, productivity, and entertainment afforded by our phones and apps, there are hidden costs. These hidden costs may include the risk of downloading dangerous software or inadvertently allowing apps access to private data. A little app-rehension may help users prevent a serious privacy invasion or data theft.

DISCUSSION QUESTIONS

1. Think about your use of various phone and computer apps and your interactions on social media. Have you ever experienced a breach of your privacy or personal data? What was the impact of this breach? Were you able to resolve it, or were you forced to live with the consequences?
2. Try to identify three different strategies that any smartphone user could follow in an attempt to minimize the risk of installing and using dangerous/risky apps.
3. Reflect on the trade-off between free apps and the potential privacy risks that these apps may introduce. Has this article changed your perception of free apps? If so, how?
4. Conduct an Internet search to identify if there have been any recent security vulnerabilities introduced through an app store (e.g., the App Store, Google Play, or Windows Phone Store). If so, conduct a brief investigation to see which apps are involved, how many people have been affected, and whether the vulnerability has been resolved.

Imagine your TV turning on every morning at just the right time so you can watch the markets open (see Figure 4-27). You smell fresh-baked bread, your shower turns on by itself, and your car knows exactly when to self-start so it's warm when you get in. Your self-driving car will let you work on your way to work. You'll see these anticipatory systems at your job too.

How will advances in hardware and software affect the types of jobs you'll go to? Ten years from now, the best-paying jobs will be ones that don't currently exist. The following are hot jobs today: IoT architect, marketing technologist, BigData architect, and DevOps manager. These job titles didn't exist 10 years ago. Ten years from now, there will be an entirely new set of jobs that you haven't heard of before.

How do you prepare for future jobs? What types of jobs will pay well? Regardless of your current college major, your future job will probably require a high level of tech skill. The best way to prepare for these types of jobs is to cultivate creativity, novel problem solving, and good judgment and have a sincere desire to learn new things.

CAREER GUIDE

Source: Alfredo Zorrilla

Name: Alfredo Zorrilla
Company: Microsoft Corp.
Job Title: Technical Account Manager
Education: University of Utah

1 How did you get this type of job?

When I interviewed for the role, I presented myself as a well-rounded candidate by highlighting a combination of soft and technical skills acquired as part of professional and academic experiences. The soft skills came as a result of several years serving in various customer service and relationship management roles at a major financial institution. Those skills include the ability to establish excellent interpersonal relationships, lead and work well with teams, and communicate in an effective and concise manner. The technical skills were acquired academically and include a broad understanding of a variety of IS topics like programming, networking, statistics, and system and database architecture and modeling.

2 What attracted you to this field?

Working as a technical account manager is a great way to combine relationship management with technical planning and troubleshooting. I realize that there's a certain romanticism around the stereotypical geek who can bang out 10,000 lines of code a day while chugging their favorite citrus-flavored soda and indulging in their preferred brand of crunchy cheesy-puffs, but I didn't want to just sit at a desk all day and "crush code." I also wanted to be involved in high-level strategy discussions with BDMs (business decision makers) and TDMs (technical decision makers). This field allows me to do a little of both.

3 What does a typical workday look like for you (duties, decisions, problems)?

There isn't a typical workday for me because there is always a different challenge or opportunity to tackle. I work directly with a very large Microsoft client, so some days I will be interacting with a VP of Infrastructure to learn more about the long-term IT goals of the organization and how they tie to its business priorities, while on others, I will be sitting side by side with a group of engineers trying to resolve a complex technical incident. I also have to work with several groups internally like Sales, Support, and the Product Group to ensure we are all achieving our mission of One Microsoft. The best way to describe what I do is this: work across every level of the client organization and leverage several different groups of my internal organization to ensure the customer is realizing maximum value from their software investments.

4 What do you like most about your job?

The best part about my job is the flexibility. Flexibility doesn't just mean that I can work whenever I want (which is true but does require a high level of self-motivation) but also that I can work toward my goals in whatever way I deem most efficient. We are encouraged to behave as "our own business," so even though there is an established set of best practices we can follow, how or if we implement them is ultimately up to us. Priority number one is for the clients to be happy with their Microsoft investment, and the best way to accomplish this is for their infrastructure to be stable.

5 What skills would someone need to do well at your job?

A successful technical account manager needs to wear many hats. One minute you may be discussing really technical problems with a systems engineer and the Microsoft Support team, and the next you may be presenting a solution to a VP or CIO alongside the Sales team. Therefore, the most important skill is to be able to interface successfully with anyone in the client and internal organizations. This requires the ability to communicate well, demonstrate a sense of empathy and ownership,