When growing up on a farm in southwestern Kansas, my family constructed a 125-foot CB (Citizens’ Band) antenna outside of our house and installed CB antennas on and radios in various vehicles and farm machinery. Our intent: rather than driving to and from the field to deliver communications, we hoped to communicate in real time with other family members and employees, thereby enabling improved operational efficiencies. Unfortunately, the innovation never quite lived up to expectations—CB radio simply doesn’t transmit long distances, especially over the hills, and reception quality was marginal, even on its best days.

In the approximately 35 years since, mobile devices have transformed how consumers, small businesses, and global enterprises communicate. A perfect example of the rapid adoption of new mobile technologies is the tablet. When it was initially released, most saw it as largely a consumer-based play with passing business applicability. With the ink on this initial prognostication still wet, I vividly remember visiting two customer locations within a few weeks of the Apple iPad launch and finding business owners who had adopted it as their primary computing device; they had relegated their laptops to the scrap pile of “ghosts of technologies past.”

Mobility: opportunities—and challenges
Over the past year, the pace of mobile device adoption—across virtually all business segments—has rapidly accelerated. For many businesses, mobile devices are essential business tools, providing employees with much more than basic email and calendaring services. In Symantec’s recently released “2012 State of Mobility Survey,” 59 percent of respondents disclosed that they are making line-of-business applications accessible, while 71 percent plan to implement corporate stores for mobile applications. The consumerization of IT and the desire to increase efficiencies are two of the primary reasons why mobility has emerged as one of the most transformative innovations since the mass-marketing of the PC.

While the opportunities are immense, the challenges are just as substantial. In particular, IT risk is greatly increased if an organization doesn’t have the right technologies and policies in place. Indeed, the lack of security measures is a serious problem; the aforementioned report found that less than half of organizations have implemented antivirus software and remote disabling of devices as part of their mobility efforts.

As a result, it is not surprising that the cost of a mobile incident for an enterprise—including data loss, brand damage, productivity drains, and loss of customer trust—averaged a whopping $429,000 last year! Further, management of mobile computing is consuming precious IT staff time: survey respondents indicated that 31 percent of IT staff, on average, is involved in some way with mobile management. So, as they would say on the CB radio, “Breaker, breaker, what’s your mobility 20?” Where is your organization in its adoption of mobile devices and apps? And more importantly, what security technologies and policies are in place? The following are some of the issues that you need to consider when planning your mobility strategy.

1. Managing the devices
Management of devices is critical—for both security and operational efficiency. This becomes even more important with the consumerization of IT and the Bring-Your-Own-Device (BYOD) models many organizations have embraced. IT organizations should work with their business owners to develop the right device, content, and application policies and then implement them into their mobile management toolset.

The right mobile management platform should enable the provisioning of new users and devices, secure those devices with passwords, encryption, and other rules, and then manage them through a unified end-
point management interface. The latter involves policy settings based on user identity, whereby apps are provisioned to devices based on the identities of their users. This results in the management of business applications and data without affecting the employee’s personal data and applications.

2. Protecting information
The value of the actual mobile device pales in comparison to the value of the enterprise information accessible on and through the device. Deploying the right identity management and data loss prevention systems and processes is crucial. And understanding who owns the data, where it is stored, and who can access it is a fundamental starting point. For data accessed or sent from the mobile device, it is important to monitor and protect it. Activities you need to manage include email and network communications, use of apps, and interactions with social media sites.

3. Securing and managing mobile apps
Mobile devices are being used for much more than email, calendaring, and other basic services. Users often have hundreds of public apps installed on their devices. Many of these are for personal use; others are for business purposes. In the event of the latter, they should be managed separately from personal apps; using a virtual container to segregate corporate apps from personal apps is an approach many organizations are taking. And for company-owned devices, the ability to block certain apps from being downloaded—from those that are time-wasting to those with inappropriate content—is something to consider.

But as the Symantec survey shows, organizations are not simply satisfied using public apps but are looking to develop their own corporate apps—for employees, partners, and customers. Controlling and managing access to those apps is important, and using two-factor authentication to access them is the best way to do so. Once identity policies are in place, corporate apps can then be provisioned only to devices that are pre-approved based on the identity of the user.

Protocols and standards around mobile app development are still in flux, though HTML5 seems to be gaining significant traction. Regardless of the programming platform, IT organizations need a proactive security approach for app development; questions around security tools and policies should be asked and answered during the design phase and not during the final rollout. In addition, a representative of the information security team needs to be a member of every mobile app development project.

4. Looking to the cloud
Additional advantages abound when mobility and the cloud are coupled together. As an example, two-factor authentication, which was only available as a hard-token-based solution a few years ago, is now readily available from the cloud. It can be seamlessly deployed across traditional laptop devices and various mobile devices and apps. The same is true of corporate apps. Instead of developing these from scratch and then hosting and managing them on the network, IT organizations can turn to cloud providers for out-of-the-box and customizable solutions.

Mobility “20”
We live in a very exciting time, when the technology innovations of the past—such as the CB radio—become historic relics in a matter of a few years. Mobility is a great example of a disruptive technology that has transformed—and it’s just getting started—how consumers and businesses communicate, interact, and work. And with the right security measures and policies (or your “mobility 20” in CB parlance), organizations can venture into this new land of opportunity with confidence that the devices and their confidential information will be protected. You can give that a big 10-4.

Patrick E. Spencer (Ph.D.) is editor in chief and publisher for CIO Digest.