Smart phones require smart security

It seems each time new technology comes along, there are arguments about whether, and to what extent, it should be allowed to change our work routines.

"Should we adopt desktop publishing, or is our typesetting process good enough? Do we really need computers on every desk, or just for the secretaries? Why do we need e-mail, when I can just walk down the hall and tell somebody what I want, or call them on the phone? We can save money by distributing publications online, but what about the members who can't or won't get them that way? If we let people telecommute, how will we know they are actually working? Why would we be on Facebook, when all you do is tell people what you ate for breakfast this morning?"

Which brings us to smart phones, the half-cell phone, half-computer that more and more of us are finding an indispensable part of our work lives. When 600,000 people overload AT&T's website to preorder a phone they've never actually touched and won't be able to get for at least a week, it says something about where the market for these devices is headed. A glance around any NABE, NCBF, or NCBP meeting reveals smart phones of all shapes and sizes in use by bar leaders.

What is the impact on bars, especially for the IT departments that have to make sure the phones can connect to bar computer networks?

The biggest concerns they face are security for the information on the devices, says Catherine Sanders Reach, director of the ABA Legal Technology Resource Center. If a bar staff member had confidential information on the phone, the IT department would want to be able to perform a "remote wipe," where the phone can have all its information deleted by IT staff if the phone is reported stolen or missing. Along those lines, the phone should also be able to be locked if an incorrect password is entered a certain number of times in a given period, indicating that an unauthorized person was trying to access the information.

At the ABA, as many as 25 percent of the approximately 1,000 employees have BlackBerries, the officially supported phone, Reach says. There are also other phones in use by other employees.

As someone who travels frequently on business, Reach finds her BlackBerry to be "a total lifesaver." She can have itinerary and confirmation numbers available immediately, read and respond to e-mail, keep up with tech industry news, access the ABA procurement system, and generally "keep business running."

The increasing reliance on remote computing devices is mirrored in other associations, says Reginald Henry, chief technology officer for the American Society of Association Executives & The Center for Association Leadership.

"Most association professionals have some smart phone, whether it's organization-provided or individual-provided," he believes. ASAE currently supports the Apple iPhone and Verizon phones based on the Android operating system, developed by Google.

Like the ABA, the biggest security concern ASAE has identified is confidential information on the phones. "These things are computers, not just phones," Henry explains. "It's not uncommon for them to contain members' names and phone numbers, or spreadsheets with the organization's financial information."

Another concern, Henry says, is that most smart phones have built-in cameras. A disgruntled employee might take a photo of sensitive documents or other unauthorized materials. “I know of one association that banned employees from bringing any cell phones with cameras into the building,” he notes.

Henry says he hasn’t heard yet of any associations that had security breaches traceable to smart phones. He believes taking a proactive approach is the best way to ensure that your association doesn’t have problems.

“The advances in technology are making things available that we never thought we’d see in such small scale,” he adds. “Just like with social media, we never had to worry about this stuff before.

“My philosophy is that we’ve got to educate each other about what’s going on, develop good guidelines about what’s appropriate in our organization, and then you have to trust that you’ve hired professionals. But keep your eyes open at the same time.”

—By Dan Kittay