Security-less Technology in Your Pocket

(editorial)

K. Miller (U. of Illinois Springfield)

J. Voas (IEEE Fellow)

As gadgets shrink and wireless bandwidth expands, we are putting more of our electronic lives – both personal and professional – into our pockets. Many professionals today have at least 2 mobiles devices – one for their private life, and the other for their job. And for some unfortunate folks, that distinction gets subdivided further, meaning 3 or more devices, possibly of different brands, with different passwords, settings, data, etc.

Technically it is possible to "shrink" the functionality of all of these devices into one, that is, to use your own device at home, on the road, and at work. This integration is convenient, and has the potential for productivity gains. But there are also security dangers that should give pause, because the security needs for home, the road, and work, may not be easily "shrinkable" to a single device.

Today's handheld mobile devices are the just the beginning of a generation of tools that offer users on-demand communication to nearly anywhere, and are filled with numerous sensors that not only know everything a user does, says, or sees, but also the location of the user. Sensors can triangulate a device's location, record audio and video, and determine velocity. There are already aps available to record your heart rate using a mobile phone camera [http://www.smartplanet.com/blog/science-scope/how-to-check-your-stress-levels-and-heart-rate-on-your-mobile-phone/10044]; continuous monitoring of vital signs may become common, or even required by your health insurer.

Bring Your Own Device (BYOD), or the more recent Bring Your Own Technology (BYOT) is already common in many businesses. In a 2012 survey in the U.S. by CISCO, 95% of respondents said "their organizations permit employee-owned devices in some way, shape or form in the workplace." [http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD] That same survey led to an estimate that the average "knowledge worker" uses 2.8 connected devices at work,; that number is expected to rise in the next few years. Most who responded to the survey regard this as positive for their company, but there were some concerns about security and support. Another survey, this time in Europe by Aruba, showed smaller but still impressive numbers of companies allowing (if not fully embracing) BYOD. [http://www.computerworlduk.com/news/mobile-wireless/3359491/european-firms-allow-byod-despite-security-concerns/]

Both surveys describe some misgivings about security problems that can arise when employees connect personal devices to company resources. When an employee attaches a personal smart phone or tablet to an organizational network or machine (be it wired or wireless), it makes sense to worry about overall security. First, as soon as external (personal) devices are attached, malware could migrate from the personal device into the company's machines and over the company's networks. In the other direction, sensitive data is likely to make its way on to the personal devices. This data could include customer

information that should be kept private and company information that should be kept proprietary. When that kind of information walks out the door on a daily basis, bad things can happen. One especially bad thing is when a personal mobile device has sensitive data, and is subsequently lost or stolen.

The security concerns for BYOD are largely a replay of security issues that arose when laptops became common. (For example, see http://www.scambusters.org/laptop.html). But laptops are larger than smart phones, memory keys and tablets; laptops are less likely to be misplaced and more likely to be noticed when they "disappear." Furthermore, the number of personal devices has gone far beyond the number of laptops or netbooks that were brought into and out of the office.

There is another, less physical aspect that makes BYOD devices typically less secure than laptops. Especially when the laptops were owned by the company, the company security policies were often enforced for those machines. Passwords were required, and the most sensitive data might be encrypted. But BYOD is built on devices that the company explicitly does *not* own. Security policies are far less likely to be enforced on machines the company doesn't own. This is a key factor in understanding why BYOD opens up a multiplicity of potential security holes. As soon as information migrates to a device that the company does not control, the data is likewise no longer under control. Further, it would be cumbersome to tie differing categories of apps or data to different passwords. In this situation, going back to multiple devices might seem more practical.

If security concerns about BYOD are justified (and we think they are), why has BYOD apparently become so popular? First, we should acknowledge that some organizations do *not* allow employees to use personal devices for company data precisely because of these security and control issues. For example, close to a third of the respondents in the Aruba survey said their organizations have banned employees from connecting their personal devices to the company network. Perhaps other organizations that now allow such connections will rethink that policy if there is a well-publicized breach that is traced back to a BOYD connection. (A breach involving a laptop and a memory stick was recently reported in India. http://articles.timesofindia.indiatimes.com/2012-03-19/india/31209853_1_security-breach-pen-drive-usb-flash-drive)

Second, there is an acknowledgement that as employees become attached and bond to particular personal devices, they are often unwilling to learn a new device when they have already scanned the marketplace, selected the device and wireless plan they prefer, and invest their own time learning how to operate it. If management comes along and tells them they must use some other "approved" device that they already discounted in their search, the likelihood that such a bonding will be as successful is diminished.

Third, with BYOT and BYOD, management avoids the upfront cost of the device. The employee bears that cost. Further, management avoids the decision to push down onto all employees one specific device (with everything hard-wired in to enforce the wireless policies of the organization), a decision that many may not like. Employees are buying the hardware and software, and training themselves. No wonder many companies are encouraging the BYOD trend.

But while *security* seems to be the major concern when discussing BYOD and BYOT, the issue of *privacy* seems overlooked and potentially the more important. Mobile devices contain a wealth of data that a user may deem private, and if personal data is co-mingled with the employer data on the same device, how are the barriers implemented between personal and employer data? In cloud computing, the issue of data multi-tenancy is handled through elaborate partitioning schemes such that hopefully data cannot leak from one partition to another. What is analogous scheme for personal mobile devices that are regularly connected to corporate networks and machines? Currently, little attention has been paid to this issue, but that is a problem that will need to be addressed if BYOD and BYOT become adapted widely, particularly if companies begin to mine the data available on their employees personal devices.

Clearly, there are several important advantages for employees and employers when employees bring their own devices to work. But there are also significant concerns about security (where the employers have more to lose) and privacy (where the employees have more to lose). Companies and individuals involved, or thinking about getting involved with BYOD should think carefully about the risks as well as the rewards.