ARTICLE COURTESY OF LEXICON SYSTEMS, LLC | +1 281.280.8106 | lexicon-systems.com

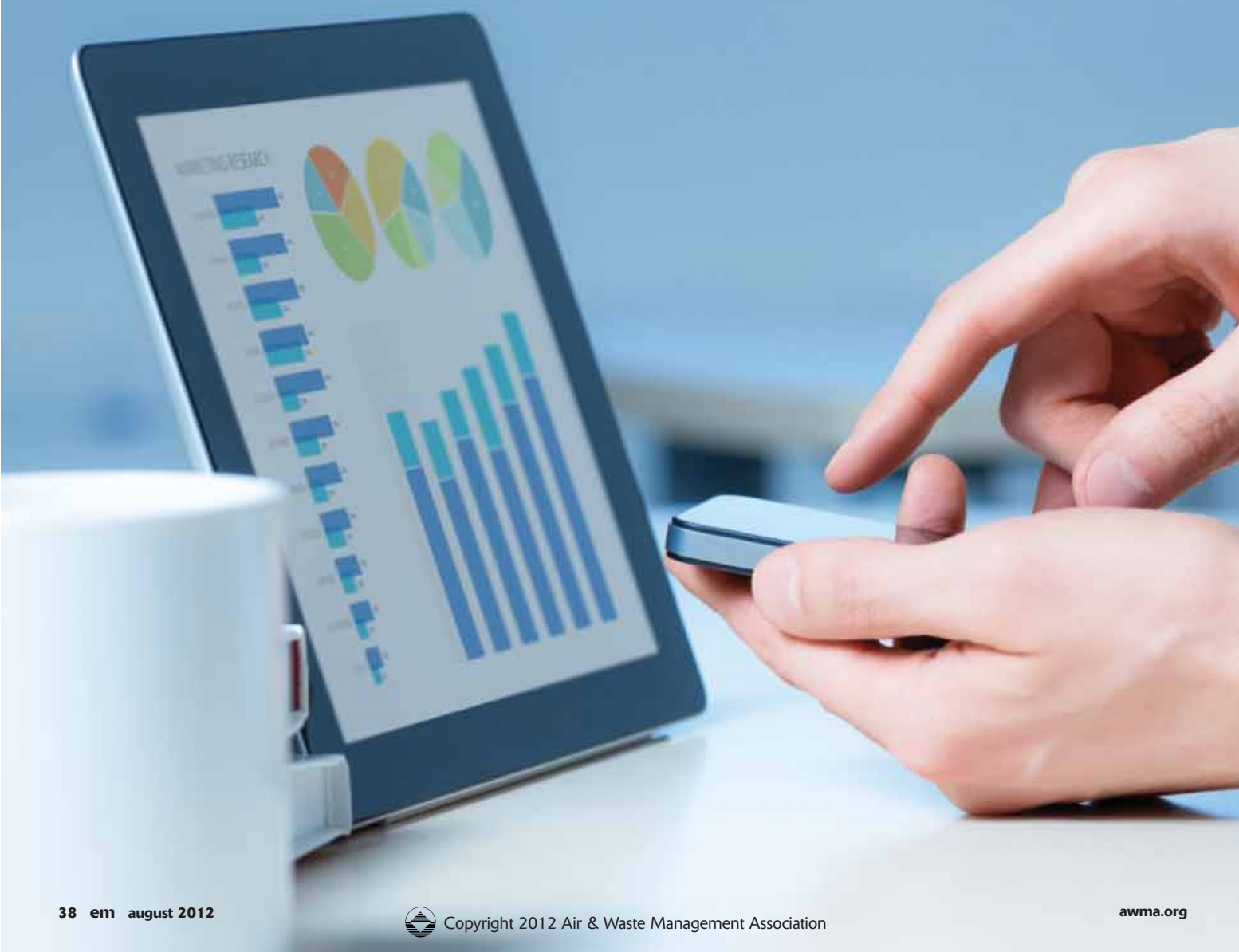
Tech Trends

Bring Your Own Device to Work

by Jill Gilbert

Jill Barson Gilbert, QEP, is president of Lexicon Systems, LLC. E-mail: jbgilbert@lexicon-systems.com.

At a recent software user group meeting, I noticed that several people had tablet computers or iPads. And at a series of software demos for clients, three vendors had iPad applications that worked with their enterprise environment, health, and safety (EH&S) software. Mobile applications are available to conduct audits and inspections, record visual smoke opacity readings, collect fugitive emissions monitoring data, and scan barcodes for chemical and waste storage inventory, to name a few.



Employees of organizations large and small continue to "consumerize" the enterprise by adopting mobile technology and bringing it to the workplace. Many organizations have allowed employees to use personal smartphones for quite some time. Today, as employees want to use more sophisticated personal devices to access company data, IT departments must address the opportunities and challenges associated with the Bring Your Own Device (BYOD) movement.

BYOD is making significant inroads in the business world with approximately 90% of employees already using their own technology (in at least a limited capacity) at work. Gartner Research studied the impact of the use of smartphones and tablet computers in the enterprise and found that "the growing smartphone base combined with huge sales of media tablets is forcing a reassessment of the client platform and IT best practices to support it."[1] In most cases, businesses simply can't stop the trend. Personal devices already access data within the organization. So, the issue is not whether to allow BYOD, but how to embrace it.

What Is BYOD?

Bring Your Own Device describes the recent trend of employees bringing personally-owned mobile devices to their place of work, and using those devices to access privileged company resources, such as e-mail, file servers, and databases.[2] A 2011 *CIO magazine* survey found that while employees most frequently bring smartphones to work, they also bring tablet PCs, laptops, and netbooks.[3]

IT departments adopt a range of policies, from allowing limited connectivity for e-mail access to full access to the IT network and corporate applications (see Figure 1). Open BYOD policies—where organizations allow employees to utilize whatever personal mobile device they wish to accomplish work tasks—can yield varying results.[4]

This trend presents both opportunities and challenges. According to information technology research firm Info-Tech, most companies do not have a formal mobile device strategy. The 24% of organizations that have such a strategy can track their telecommunications expenses and have fewer problems with mobile devices.[5]

Opportunities

BYOD presents several opportunities. Many organizations believe that BYOD provides anytime, anywhere mobility that helps to

- improve collaboration;
- retain and attract quality employees;
- reduce help desk requests;
- reduce overall IT spending;
- contribute to business success; and
- improve employee creativity, satisfaction, and productivity.

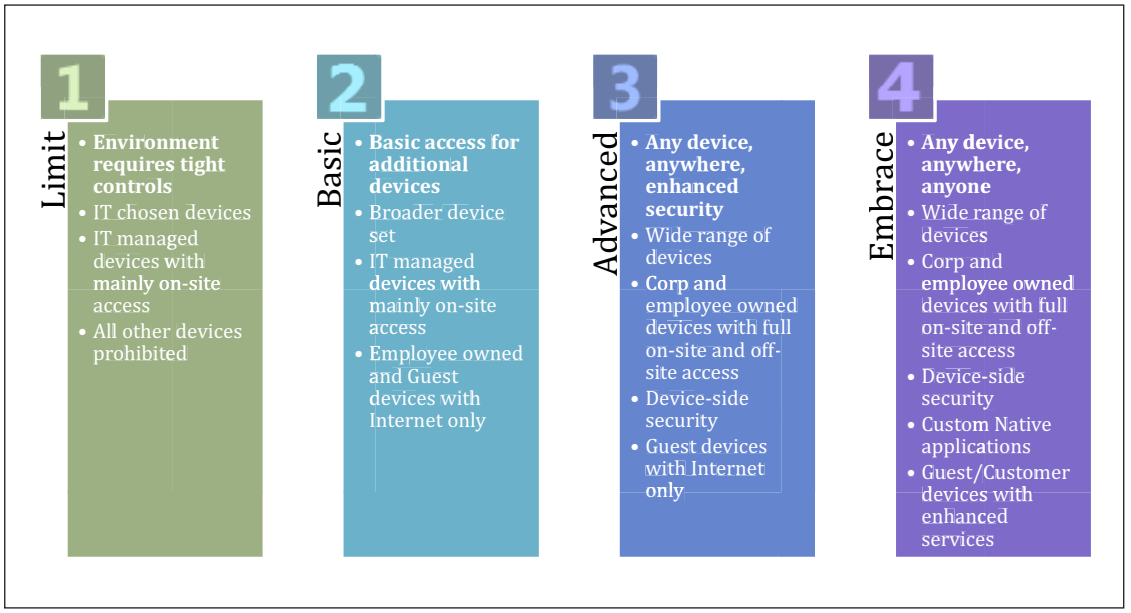


Figure 1. BYOD adoption scenarios.

Source: Adapted from Neil Anderson, Cisco Bring Your Own Device, Cisco Systems, April 18, 2012.

Challenges

Multiple needs and multiple devices. Employees bring a multitude of tablet computers, iPads, and smartphones to work, which use different operating systems and offer different features and functions. This variety of form factors, coupled with constantly evolving technology, makes it difficult to pre-approve a standardized set of devices, and impractical to support.

Data security and usage policy. Because employees may access sensitive data using their own devices, one of the greatest challenges is managing access to corporate and private networks. BYOD compels companies to use a secure wireless protocol to provide over-the-air encryption, user authentication, and network authentication. Corporate IT departments are concerned about data vulnerability. One energy company CIO told me that his organization allows BlackBerrys and iPhones, but not Android devices, because of security vulnerabilities associated with the operating system.

Device and data ownership. BYOD results in the use of both personal and business applications on the same mobile device. This commingling of personal and corporate data creates security and privacy issues. What happens to the data when the employee leaves work each day, and when the employee leaves the organization for good? Some enterprises are concerned with employees—particularly in sales—taking their phone numbers with them when they leave the company.

Help desk and support. The IT department must plan for onboarding (i.e., when an employee brings a new personal mobile device to work for the first time), as well as ongoing support.

Telecommunications costs. IT groups may like BYOD because it shifts part of the telecommunication costs to the employee—the employee purchases the device and pays monthly service and data subscription fees. Some organizations reimburse the employee for part or all of the monthly fees. Both parties can benefit from corporate discounts offered by the major telecommunications providers. However, the presence of a myriad of new devices may increase the overall telecommunications costs for an organization.

Mobile and WiFi system load. Personal mobile devices can stress the organization's wireless (WiFi) hardware, resulting in the need for more equipment and bandwidth to handle BYOD traffic. The transition to 4G (Fourth Generation) networks and the use of mobile high-definition video collaboration will stress the system more.

The issue is not whether to allow BYOD, but how to embrace it.

Mobile asset management. It may be important to know where mobile devices are at any given time, in case the device is lost. Some organizations use mobile asset management software; vendors range from focused firms like Mobiletron, Good Technology, and Zenprise to security software companies like McAfee, SmithMicro, and Symantec to enterprise companies like IBM and SAP.

The BYOD movement creates exciting opportunities, as well as challenges, for the enterprise. Shrewd organizations figure out how to manage BYOD, since personal tech is here to stay. **em**

References

1. *Media Tablets and Beyond: The Impact of Mobile Devices on Enterprise Management*; Gartner Research, January 30, 2012. See www.gartner.com.
2. Wikipedia.org.
3. Your BYOD Field Guide; *CIO magazine*, April/May 2012. See www.cio.com.
4. Burke, J. Bring Your Own Device: Risks and Rewards; *techrepublic.com*, December 14, 2011.
5. *Mobile Management Strategy Survey*; Info-Tech Research Group, April 2012. See www.infotech.com.