

July, 2011

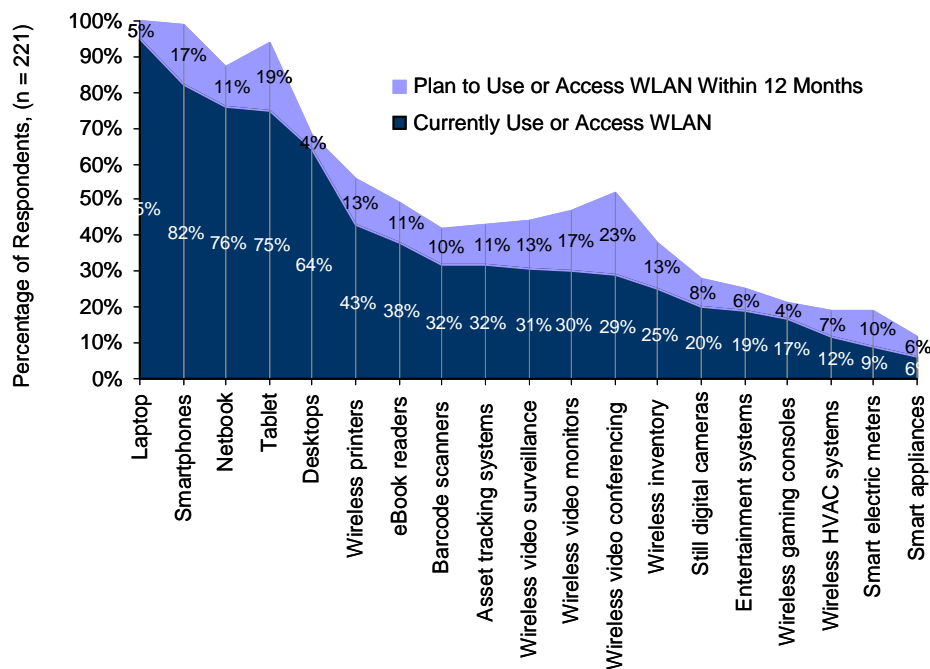
Prepare Your WLAN for the BYOD Invasion

The modern "smart device" (see sidebar) has had a transformative effect on the enterprise. As described in the May 2011 Aberdeen study *Wireless LAN 2011: Reaching the Invisible Network for the Smart Revolution*, initially driven by the broad adoption of smartphones, the "Smart Revolution" has rapidly expanded with the meteoric rise of the tablet computer. One result of this transformation of IT-supported mobile endpoints has been the rapid influx of employee-owned devices; sometimes know as "Employee-Liable" or E-L devices. This in turn has created new pressures and demands on the core enabling technology, the wireless LAN (WLAN) itself.

Increasing Demands on the WLAN

The *WLAN 2011* study found smartphones and tablets are just the beginning of a torrent of new device types expected to claim their share of wireless network bandwidth. The actual and planned penetration of these new smart devices entering enterprise wireless networks is illustrated in Figure 1.

Figure 1: The Smart Device Invasion



Source: Aberdeen Group, May 2011

Figure 1 represents the percentage of survey respondents whose organizations either currently or plan to use the identified smart device for

Analyst Insight

Aberdeen's Insights provide the analyst perspective of the research as drawn from an aggregated view of the research surveys, interviews, and data analysis

Smart Device Defined

Smart devices are a generation of portable or mobile devices from smartphones to control systems to remote sensors, which share the following characteristics:

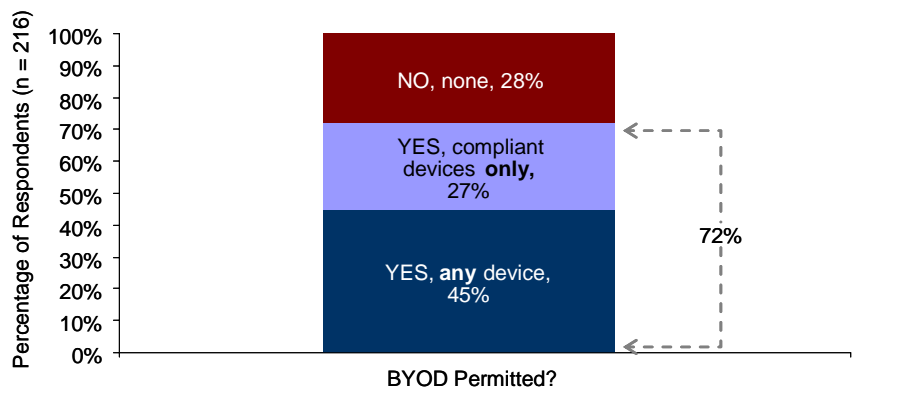
- ✓ **Self-monitoring** – enough on-board memory and processing power to remotely report on their status and performance
- ✓ **Self-identifying** – they have the ability to access and identify and authenticate themselves over wireless networks
- ✓ **Programmable** – often integrated using standard micro-components, they are typically based on standard operating systems which allow them to be customized by software and run software applications
- ✓ **Ubiquitous** – relatively inexpensive for their capability set, they quickly propagate through rapid end-user adoption

business purposes. The range of smart devices already accessing the WLAN is broader and deeper than Aberdeen had expected; especially noteworthy is the percentage of respondents currently using laptops (95%), smartphones (82%), netbooks (76%), and tablets (75%) on the WLAN. The dominance of these four device categories together represent significant usage demands that will be placed on the wireless network. In addition, it is precisely these device types that are typical of the employee-owned, Bring-Your-Own-Device invasion.

The Bring-Your-Own-Device (BYOD) Invasion

An increasing number of smartphones and tablets are owned by employees, often termed Employee-Liable or E-L devices. The March 2011 study *Enterprise Mobility Management 2011: Mobility Becomes Core IT* found that 72% of organizations were permitting the use of E-L devices for business purposes (Figure 2).

Figure 2: Personal Mobile Devices for Business Use



Source: Aberdeen Group, February 2011

When asked for the top reason why they permitted the "Bring-Your-Own-Device" or BYOD phenomenon, 57% of respondents stated that the business reduced costs by not paying for devices, and 51% that employees gained additional productivity.

This BYOD invasion is an inescapable result of the Smart Revolution, and challenges IT to maintain the performance and security of the wireless networks that make enterprise mobility possible.

Recommended Actions

In order to prepare for the BYOD invasion, Aberdeen recommends that IT take the following actions to address proactively the security and performance challenges to the organization's WLAN:

- **Ensure that compliance policy is in place and enforced:** It's not enough to develop a thorough IT policy on E-L devices – that policy must be communicated and enforced. For example, to allow

BYOD: Risk or Reward?

The financial rewards of a well-implemented BYOD strategy are relatively straightforward: a lower initial capital expenditure, balanced by potentially higher operational costs, as supporting a myriad of employee-owned devices is inherently more complex than a limited and controlled subset of corporate-procured devices.

Often overlooked, however, is the increased risk of financial exposure due to unauthorized access to protected data stored on mobile devices that are lost or stolen. In the March 2011 study *Enterprise Mobility Management 2011: Mobility Becomes Core IT*, respondents were asked to identify the maximum financial exposure to their organization caused by a lapse in compliance with local statutes and regulations from protected data stored on unsecured mobile devices.

At the low end of the risk spectrum, the exposure was **\$10,600 USD** per lapse; at the high end, **\$491,600 USD** per lapse. And a single compromised device can contain multiple compliance lapses. With this math in hand, how can one *not* address the security and compliance of wireless network?

only certain types of mobile platforms, while barring others. These activities should be automated whenever possible.

- **Create and maintain an up-to-date device inventory:** Fingerprint device types, as well as individual devices and users to gain full visibility and control of the devices attempting to connect to the network.
- **Control device access to the network:** Protect the network from compromised devices to minimize risk and exposure; for example, provision Internet and email-only access with limited or no intranet access for guest mobile access.
- **Automate authentication and authorization:** Use a role-based approach for both device and end-user authentication and authorization. Use PKI certificate-based authorization of devices with auto registration to minimize the impact on IT network support personnel.
- **Plan for density:** The number and variety of mobile endpoints attempting to access the WLAN is daunting. Ensure that network throughput and performance are up to the challenge. Intelligently control network bandwidth allocated to devices and users, automating wherever possible.
- **Ensure QoS:** Quality of Service is essential to maintaining the performance of the network and productivity of the workers. Provide adequate network bandwidth at the core and edge. Ensure applications run smoothly and that access is protected. These activities will also minimize the impact on helpdesk and support services.
- **MDM is not enough:** Although a crucial part of a well-integrated strategy for managing the BYOD invasion, Mobile Device Management (MDM) does not provide visibility to or control of network access. Comprehensive network management is also required.
- **Consolidate wired and wireless policies and management:** With the rapid influx of mobile devices, wireless management will become a primary focus. Combine wired and wireless network resources and personnel wherever possible to streamline operations. Propagate a unified view of network performance and security, and you'll lower maintenance and support costs as a result.
- **Extend content filtering to personal devices:** Protect the network from malware and unauthorized access. Make sure anti-virus, URL filtering, spam protection, Denial of Service (DoS) defense, and data leakage prevention measures are in place.

- **Plan for multiple smart devices per user:** The typical business user has more than one mobile device assigned to him or her (e.g. laptop, smartphone, and or tablet). Procure adequate network resources such as IP addresses, authentication, and WAN bandwidth; pool these resources wherever possible.

By taking these steps, IT organizations can regain control of their network, while simultaneously supporting the BYOD phenomenon. This will also serve to foster the visibility, influence, and ultimately the perceived value of the IT function itself.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
<i>Wireless LAN 2011: Ready the Invisible Network for the Smart Revolution</i>; May 2011	<i>Enterprise Mobility Management 2011: Mobility Becomes Core IT</i>; March 2011
<i>Aruba Networks' MOVE: Mobile to the Core</i>; April 2011	<i>Unchained: the Wireless Imperative in Network Integration</i>; October 2010
Author: Andrew Borg, Senior Research Analyst, Wireless & Mobility, andrew.borg@aberdeen.com	

For more than two decades, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.5 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen's research provides insight and analysis to the Harte-Hanks community of local, regional, national and international marketing executives. Combined, we help our customers leverage the power of insight to deliver innovative multichannel marketing programs that drive business-changing results. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 854-5200, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>.

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. (2011a)