MOBILITY AT WORK: MAKING PERSONAL DEVICES A PROFESSIONAL ASSET
INTRODUCTION

Half of U.S. adults connect to the Web through either a smartphone or tablet,* and many are looking for ways to increase efficiency and effectiveness on the job by using those devices. Millions of workers are now bringing their own devices to work and using them to connect to their employers’ networks, complicating already-complex computing systems.

Mobile computing taps and taxes every aspect of information technology management, and the Bring Your Own Device (BYOD) phenomenon represents one of the greatest challenges for IT professionals: empowering worker choice and productivity while protecting the organization’s network, data and assets.

To examine this critical issue and better understand how to successfully integrate personal devices into total mobility management, CDW surveyed 1,200 workers that use personal tablets and smartphones for work and 1,200 IT professionals across eight industries. The resulting report identifies key needs to address in ensuring security and success, and outlines a path to total mobility management.


Throughout this report, we define “BYODers” as those who use a personal smartphone or tablet for work purposes at least once a week.
FIVE PILLARS OF MOBILITY MANAGEMENT

- This report uses the following icons to tie research findings and recommendations to the five critical facets of mobility management:

  1. **Planning**: Laying the groundwork for success with policies and plans for security and an end-to-end network strategy
  2. **Enabling**: Procuring and provisioning devices efficiently, whether employer- or employee-owned
  3. **Protecting**: Integrating security and real-time centralized management of mobile devices, applications and content, as well as real-time monitoring and expense management
  4. **Supporting**: Supporting help desk services for end users, supporting employer- and employee-owned devices alike, and administration and management tools for IT
  5. **Empowering**: Enabling employee collaboration, productivity and efficiency with cross-platform integration, applications, browser-based access and virtualization
• IT professionals expect the number of personal smartphones and tablets accessing their networks to more than double in the next two years. But, the devices are only a fraction of the challenge:

of IT professionals surveyed say their organization has encountered challenges with personal device adoption.

Top challenges include securing data on personal devices (55%), securing network access (54%) and network performance (39%)

Looking ahead, nine out of ten expect the growth of personal mobile devices to have major network impacts, primarily:*  

- Increased bandwidth requirements 63%  
- Increased server requirements 44%  
- Increased network latency 39%  
- Increased storage requirements 37%  

*Respondents asked to select all that apply
DATA (AND ORGANIZATIONS) AT RISK

• Increased access means increased risk:

54% of BYODers say they use their devices for business applications beyond phone calls and email

86% of BYODers say they access or save work-related information on their mobile device

52% of BYODers say they use more than one device

And 5% have lost the personal mobile device they use for work, or had it stolen

That’s a one in 20 chance for a leak
INITIAL EFFORTS IN PLACE

Organizations are trying a variety of very basic measures to increase security:

According to IT:*

- **76%**
  - More than three quarters implement guidelines for the use of personal mobile devices

- **69%**
  - More than half require a user password for network login

- **42%**
  - And, nearly half enforce the use of a screen lock on personal mobile devices

*Of those respondents whose organizations have security policies or measures in place
• There are many other, more effective measures, but their adoption is more complex and they lag even further behind the simpler ones. Several examples:

According to IT professionals,* only:

15% use partitioning, or securing and controlling a portion of personal mobile devices

22% limit the applications employees can load on personal mobile devices

24% use location tracking to recover lost or stolen personal devices

Additionally, more than half of IT professionals say their department recommends specific mobile applications or devices for employee use.

*Of those respondents whose organizations have security policies or measures in place
THREE CRITICAL MANAGEMENT GAPS

• Broad mobility programs require A-level support, but even IT says that is hard to provide:

**Awareness**

Does your organization offer guidelines for the use of personal mobile devices?

- BYODers: 42% say yes
- IT*: 76% say yes

**Trust**

Do you think the IT department should help secure personal mobile devices used for work?

- BYODers: 38% say yes
- IT: 75% say yes

**Support**

On a scale of A-F, please grade the effectiveness of your organization’s BYOD policies and technical support:

- BYODers: 41% say A/B
- IT: 64% say A/B

*Of those respondents whose organizations have security policies or measures in place
WHY YOU NEED A PLAN

- Smart devices need genius infrastructure:

BYODers: How can IT better support you?

- “Have a site on the agency intranet to explain what is allowed and instructions on uses. Security backup would be great”
- “Make it clear how IT can be of assistance with a personal device if it is being used for work purposes”
- “Allow us to access apps which could be used for work so we aren't as dependent on our PCs”
- “Improve IT’s availability for technical issues, including faster response times”
- “Offer training to show what devices are available and how to use them (including software, apps, devices) to make my job easier”
- “Employ better IT security and encrypt work-related data and information”

**Bottom Line: Employees need support and empowerment**
RECOMMENDATIONS
STUDY USER NEEDS; PLAN LASTING SUPPORT

- IT professionals have concerns, but lack real dialogue with users:

What functions is your organization most concerned with supporting via the personal mobile devices employees use for work?*

<table>
<thead>
<tr>
<th>Function</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core messaging (email, text, voice/voicemail)</td>
<td>48%</td>
</tr>
<tr>
<td>Accessing organizational data</td>
<td>47%</td>
</tr>
<tr>
<td>Storing organizational data or documents</td>
<td>36%</td>
</tr>
<tr>
<td>Viewing/creating documents</td>
<td>33%</td>
</tr>
<tr>
<td>Collaboration (conferencing, webinars, document sharing)</td>
<td>33%</td>
</tr>
<tr>
<td>Managing processes or projects</td>
<td>27%</td>
</tr>
</tbody>
</table>

*Respondents asked to select all that apply

But, only half (51%) of IT professionals say they actually talk with employees about how they use personal mobile devices.
SECURITY SOLUTIONS SHOULD BALANCE EMPLOYER AND USER CONCERNS

• BYODers are open to additional security measures, but some of the most effective measures make them the most uncomfortable:

BYODers: How comfortable would you be with your employer taking or requiring the following steps to secure your personal mobile device(s)?*

<table>
<thead>
<tr>
<th>Security Step</th>
<th>Comfortable</th>
<th>Neutral</th>
<th>Uncomfortable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required password for network login</td>
<td>63%</td>
<td>23%</td>
<td>14%</td>
</tr>
<tr>
<td>Guidelines for use</td>
<td>54%</td>
<td>28%</td>
<td>18%</td>
</tr>
<tr>
<td>Encryption of stored information</td>
<td>47%</td>
<td>30%</td>
<td>23%</td>
</tr>
<tr>
<td>Enforced use of a screen lock</td>
<td>46%</td>
<td>28%</td>
<td>26%</td>
</tr>
<tr>
<td>Location tracking</td>
<td>41%</td>
<td>27%</td>
<td>32%</td>
</tr>
<tr>
<td>Ability to lock or completely erase your device wirelessly</td>
<td>41%</td>
<td>26%</td>
<td>33%</td>
</tr>
<tr>
<td>Partitioning</td>
<td>28%</td>
<td>32%</td>
<td>40%</td>
</tr>
<tr>
<td>Limiting access at work to guest networks only</td>
<td>25%</td>
<td>35%</td>
<td>40%</td>
</tr>
<tr>
<td>Application management</td>
<td>20%</td>
<td>30%</td>
<td>50%</td>
</tr>
</tbody>
</table>

*Full definitions provided to survey respondents; see slide 17 for details
Current efforts fall short – **36%** of organizations have not planned or deployed an MDM solution:

**IT: Where does your organization stand with Mobile Device Management?**

- **Fully deployed**: 15%
- **Deploying**: 22%
- **Planning**: 27%
- **Considering**: 25%
- **Not Considering**: 11%

Currently, **half** of the existing or planned MDM systems do not cover personal mobile devices.

Of those not considering an MDM solution, **20%** plan to prohibit the use of personal mobile devices and **32%** plan to do nothing.

Slightly **more than one-third** of respondents (36%) are currently deploying or have completed deployment of a mobile application management (MAM) solution.

Of those considering or making a plan for an MAM solution, just **11%** will begin deployment within the next 6 months.
INTEGRATE, INTEGRATE, INTEGRATE

• Develop an integrated management solution to:

» **Identify** impacts of mobility adoption on your IT infrastructure and address them in your plan through dialogue with users and across IT

» **Address** the impact on your IT team’s time of procuring and provisioning devices and supporting mobile users; simplify use of mobility for employees to gain the most return on investment

» **Optimize** your voice, data and text plans to minimize expense

» **Integrate** commonly used mobile apps with your core applications, but do so securely

» **Monitor** how many devices are accessing your network and what they are doing there

» **Improve** mobility’s ROI through development and use of custom apps to address key internal processes

» **Capture** the leverage that mobile apps can give you with your customers
MANAGING THE FUTURE OF MOBILITY

• Consider an integrated management solution addressing the five critical components of mobile adoption:

  **Planning:** Only half of IT professionals say their department actually speaks with users to understand how they use personal mobile devices – but that is essential to development of a mobile strategy and technology road map, data and device policies, security and network integration.

  **Enabling:** Implement your policies through automated procurement, provisioning and deployment of devices, all integrated through a management portal tailored to your needs.

  **Protecting:** Integrate security and real-time centralized management of your mobile devices, applications and content, with real-time monitoring and expense management.

  **Supporting:** Live and self-service help desk services for end users, supporting employer- and employee-owned devices alike, as well as MDM administration.

  **Empowering:** Enabling employee collaboration, productivity and efficiency with cross-platform integration, applications, browser-based access and virtualization.
METHODOLOGY & DEMOGRAPHICS

- CDW surveyed* 1,200 IT professionals and 1,200 non-IT professionals who use a personal smartphone and/or tablet for work purposes at least once a week. The total sample for each group represents eight industries and equates to a margin of error of ±2.7% at a 95% confidence level. Individual industry samples equate to a margin of error of ±8.0% at a 95% confidence level:

<table>
<thead>
<tr>
<th>BYODers</th>
<th>Personal mobile device</th>
<th>Gender</th>
<th>Age</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>100% of respondents use a personal mobile device for work purposes at least once a week</td>
<td>43% smartphone 9% tablet 48% both</td>
<td>44% male 56% female</td>
<td>7% 18-25 24% 26-35 18% 36-45 23% 46-55 21% 56-65 7% 66 or older</td>
<td>Small business n=150 Medium business n=150 Large business n=150 Federal government n=150 Healthcare n=150 Higher education n=150 K-12 public school district n=150 State and local government n=150</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT professionals</th>
<th>Title</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>100% of respondents work in a role involving the oversight, management or support of mobility initiatives or devices</td>
<td>CIO/CTO Deputy CIO/CTO IT Director/Supervisor IT Manager Network Administrator Data Center Manager Other IT management</td>
<td>Small business n=150 Medium business n=150 Large business n=150 Federal government n=150 Healthcare n=150 Higher education n=150 K-12 public school district n=150 State and local government n=150</td>
</tr>
</tbody>
</table>

*Research conducted by O’Keeffe & Company
How comfortable would you be with your employer taking or requiring the following steps to secure your personal mobile device(s)? Please rate each of the following on a scale of 1-5, where 1 is “very uncomfortable” and 5 is “very comfortable.”

a. Guidelines for use  
b. Enforced use of a screen lock on your device(s)  
c. Required user password for network login  
d. Encryption of information stored on your device  
e. Location tracking (ability to track or locate your device if it’s lost or stolen)  
f. Ability to lock or completely erase your device wirelessly if it’s lost or stolen  
g. Limiting your personal device’s access at work to guest networks only  
h. Partitioning (your employer secures and controls the portion of your mobile device that supports work applications, while you control the rest)  
i. Application management (your employer limits applications you can install, OR deploys, secures and maintains specific work-related applications on your mobile device, leaving you in control of all other applications and functionality of your device)
THANK YOU.

FOR ALL MEDIA QUESTIONS AND INQUIRIES, PLEASE CONTACT:

KELLY CARAHER
CDW PUBLIC RELATIONS
847-968-0729
KELLYC@CDW.COM

MARTY NOTT
O’KEEFFE & COMPANY
585-271-1141
MNOTT@OKCO.COM