# Managing Mobile Device Mayhem

## COMPREHENSIVE MOBILE DEVICE MANAGEMENT STRATEGIES HELP IT KEEP CONTROL, LIMIT RISK

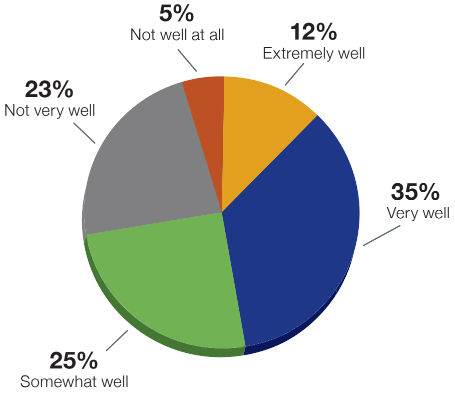
COMPUTERWORLD
Custom Solutions Group

SPONSORED BY:
BlackBerry.

Personal mobile device use in the workplace has gone from occasional to constant as the benefits are becoming clear. It's now commonplace to find many types of mobile devices in use by employees at the office, on the road or in remote locations for accessing corporate data and applications, regardless of whether these devices are owned by the employees or the company.

This trend, referred to as "bring your own device" (BYOD), benefits enterprises in several ways—higher productivity, lower hardware costs and greater employee satisfaction, to name just a few—that are driving more corporate leaders to sanction mobile device use in the workplace. According to the Computerworld "Consumerization of IT" study that was published in October 2011, about half of the 604 respondents said their organizations allow employees to do work with their own devices, either away from the office or at work.

How well organizations mitigate IT risks introduced by personal mobile devices



Source: IDG Research, April 2012

Yet the advantages this trend brings are not without risks, and IT stakeholders are keenly aware of them. In an IDG Research survey conducted in early April 2012, 69 percent of the IT leaders who responded said they are extremely or very concerned about the risks posed by the use of personal mobile devices to access corporate IT assets.

"Clearly, and as everyone knows, security is a weak area here, particularly within the parameters of BYOD. Other challenges include the IT support headache, since many of these devices are inherently consumer-oriented, as well as the lack of functionality to be truly useful for work," says Emile Rashkovich, senior vice president and CIO of Sentinel Real Estate Corp. in New York.

And although the vast majority of the 113 survey respondents said that their organizations have put in place policies for managing mobile risks, fewer than half of these respondents said these policies are extremely or very effective. The consequences of not managing these devices well are real; two-fifths of the survey respondents said their organizations had experienced at least one tangible loss attributable to personal mobile device use by employees.

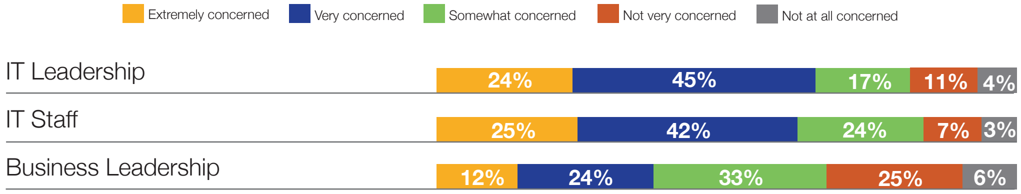
### The Case for Mobile Device Management

Policies and guidelines aren't enough to keep company data safe in the face of increased mobile device use in corporate settings. What's more, policies can't help IT departments grapple with the management and control of these devices. Comprehensive mobile device management strategies are needed to give employees the freedom and flexibility to use the device of their choice but also to enable IT departments to streamline management and reduce the risks these devices introduce.

"There's some complacency. People say, 'It's just a phone. How much risk can there be?' But then they see the statistics and realize they can lose control," says Deanne Taenzer, senior product marketing manager with Research in Motion (RIM). "Organizations really need to get a handle on these devices, from both a security and a productivity perspective."

BYOD becomes particularly troublesome when employees have to keep corporate information and personal information separate on the same device. Regardless of whether a device is corporate-issued or belongs to the employee, most users

**Level of concern within organizations regarding IT risks posed by personal mobile devices**



Source: IDG Research, April 2012

today want to be able to have both their personal information and access to corporate data and applications on one device, so they don't need to carry two devices around. But many IT leaders have found that establishing policies for the separation of personal and corporate information is complicated, and they would rather use a tool that can distinguish between the two types of data and treat the information accordingly.

"We really need to be able to separate the corporate apps and data from the personal and be able to manage and delete only the corporate part," says Bud Conlin, director of Information Technology at Sennheiser Electronic Corp., an audio specialty company based in Old Lyme, Conn.

Given the importance of managing mobile devices in the workplace today, the following features have emerged as essential components of mobile device management solutions:

- Be operating-system-agnostic – so that employees can freely choose their own device
- Provide remote wipe and remote locking capabilities – giving IT departments control and security in case of the loss or theft of devices
- Enforce passwords – for security and data protection
- Separate personal and corporate data – so that corporate data is subject to the same security policies on the device as those implemented on company-issued hardware
- Provide over-the-air application installation, updating and auditing – to make device management and upgrades easier
- Back up and restore device data – for fast recovery from failure
- Offer a familiar and seamless user experience – to limit training time and enhance employee use

## The BlackBerry Advantage

BlackBerry® Mobile Fusion extends the flexibility and familiarity of the BlackBerry solution to make managing mobile devices faster, easier and more organized than ever before. Now IT administrators can support BlackBerry, iOS and Android devices from one unified interface, protecting business information while giving mobile workers easy access to the information they need.

BlackBerry Mobile Fusion provides inventory and asset management and offers a single, unified interface that enables IT departments to manage company- as well as employee-owned mobile devices within their organizations, including functions such as creating and managing groups, managing user profiles and provisioning mobile devices. It also provides connectivity management for Wi-Fi and virtual private network (VPN) connections, implements policy definition and management, provides security through remote lock and wipe capabilities and offers application management.

Enterprises that use BlackBerry smartphones with BlackBerry Mobile Fusion will also benefit from BlackBerry Balance™ technology, which supports the use of a single device for both work and personal purposes by separating the two types of data and treating them accordingly. What's more, BlackBerry Mobile Fusion comes from a company that has proven its excellence in delivering secure, enterprise-class solutions for mobility.

For more information visit **www.blackberry.com/mobilefusion**