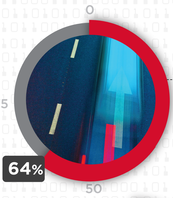
IRONKEY™ by imation

An IronKey Infographic

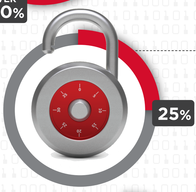
MOBILE WORKERS:
CONSIDERABLE OPPORTUNITY REMAINS TO BOOST SECURITY

Many Devices and Workspaces Unmanaged

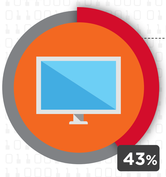


More than 64% said a majority of their mobile workforce can access their organizations' high value data remotely while only **1 in 3** devices are unmanaged.

More than half reported mobile media (i.e. USB drives) are unmanaged while less than **25%** said sufficient policies/controls are in place for mobile media.



An additional 25% admitted to having no controls (no policy or technical controls enforced by centralized management) in place.



43% do not manage the desktops used by mobile workers.

Unmanaged devices and workspaces (including BYOD) used to access corporate data, combined with the lack of controls, leave organizations VULNERABLE.

Greatest Data Exposure Risks in Mobile Device Usage

A top data exposure risk was from malware introduced via unmanaged devices **13.6%**.

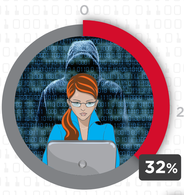
Loss or theft of corporate devices was also a major concern for **12.6%** of respondents.

BYOD came into play with companies identifying an inadvertent use of infected personal devices **7.9%** and loss or theft of personal devices **3.7%** as top exposures.

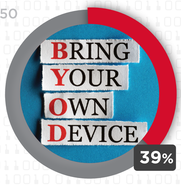
Only **13%** of firms with more than 10,000 employees and **7%** with 500 to 10,000 employees said they encrypt data on their USB devices.

Responses in this area suggest that, while enterprises intend to practice good security, there's a gap in the actual implementation.

BYOD Continues to Grow Despite Most Organizations' Lack of Readiness To Support Mobility



32% of organizations expect at least **60%** of their workforce to be mobile in the next 12 months.



In organizations with 500 and 10,000 employees, **20%** to **39%** of their mobile workers use personal laptops for work purposes.

BYOD is a huge burden on IT. Organizations should look for management solutions that have capabilities such as remote lock and remote wipe.

Secure Mobile Workers with Windows To Go

19% are already using or planning to use Windows To Go features in Windows 8.x or higher.

Windows To Go allows IT to securely replicate desktop environments on mobile workspaces and provides a secure managed alternative for BYOD and mobile workers. Enterprises can realize the benefits of enterprise mobility with the convenience and ease of access of desktop and laptop environments.

How was the research conducted?

The survey, "Securing Portable Data and Applications for a Mobile Workforce," was sponsored by IronKey by Imation and conducted by the SANS Institute between January 2015 and April 2015. 330 IT security professionals representing a broad spectrum of industries, including the technology, government, financial, education and healthcare sectors, as well as organizations of all sizes, completed the questionnaire on their insider threat awareness and posture.

SANS defines a mobile worker as an individual who may periodically work remotely/offsite as well as in the office, mobile between organization locations or use mobile technology exclusively for work-related activities.

For the full SANS Institute report, download here.

IRONKEY™ by imation

Imation's IronKey solutions meet the challenge of protecting today's mobile workforce, featuring USB solutions for data transport and mobile workspaces.

www.ironkey.com