# Research Findings

## 1.1 PRODUCTIVITY

Data from various recent surveys associated with BYOD and productivity in the workplace are listed below. Due to the relative newness of this issue, there is not a lot of research to be found outside of that from vendors.

- 81% of college students believe they should be able to choose the devices they need to do their job ("Cisco 2011 Annual Security Report," December 2011)
- 58% of IT decision makers think mobility and consumerization can deliver increased productivity and efficiency ("BT Assure: Rethink the Risk Summary," April 2012)
- 84% of IT decision makers believe companies allowing employees to use personal devices for work enjoy a competitive advantage ("BT Assure: Rethink the Risk Summary," April 2012)
- Nearly 4 in 10 of enterprise organizations surveyed have a history of BYOD-related breaches in security ("BT Assure: Rethink the Risk Summary," April 2012)
- 62% of surveyed enterprises pay for employee devices and voice data plans ("BYOD and Virtualization, Insights from the Cisco IBSG Horizons Study," May 2012)

- 72% of survey respondents are already formally supporting a BYOD program (“Good Technology State of BYOD Report,” October 2011)

## 1.2 PROS AND CONS

### 1.2.1 Pros

- Improved user experience due to device familiarity and device singularity (one device)
- Potential hardware cost transfer from company to employee
- Improved work from anywhere/anytime opportunities
- Workplace draw for young professionals, e.g., “Best Places to Work”
- Increased workplace productivity

### 1.2.2 Cons

- Potential loss of company purchasing power related to a reduction in bundling of traditional technology services (software/hardware/usage)
- Increased difficulty for in-house IT user support due to multiple platforms and devices
- Hardware and software compatibility issues with device to organizational software and infrastructure
- Increased mix of personal and company information; blurring the lines of company vs personal property
- Introduction of new data security/privacy threat opportunities

### 1.2.3 Pro/Con

- Hardware refresh: more frequent device upgrades containing the latest features and capabilities (depends on the equipment life cycle of the specific company)

## 1.3 MUST-HAVES

A clearly communicated BYOD program should contain the following elements:

- Definition of program eligibility: people, devices, and data/program/application categories
- Who pays and how? Device and plan usage (employee or company, full or partial, stipend [%] or expense)

- Who provides IT support? In-house or employee/device carrier?
- User responsibilities (rights, privileges, expectations)
- Company rights and privileges
- Security requirements
- Employee user agreement to manage expectations, clarify responsibilities, and address potential legal, employment, and privacy-related issues
- A Mobile Device Management (MDM) program (onboarding, tracking, identification, management)
- Employee awareness training and certification program
- A mobile security audit program (for tracking devices, users, and applications)
- Ability to remotely find (GPS), wipe, and/or kill all lost, stolen, or terminated devices
- Clear device and operational security requirements

## 1.4 CHALLENGES

When instituting a new BYOD program, companies may experience challenges related to the following:

- Gaining physical access to devices
- Installing and managing device security software upgrades and patches
- Wiping devices of company data associated with user-initiated device upgrades
- Recovering proprietary information from terminated devices and third party (cloud) storage
- Confiscating devices associated with investigations and/or legal discovery/holds
- Enforcing and monitoring acceptable use, data storage, software and hardware security compliance

## 1.5 RISKS AND LIABILITIES

The following risks and liabilities are possible when instituting a new BYOD program:

- Loss of security control; greater risk related to intrusion control/detection and malware susceptibility
- Data breach risk and related legal liabilities

- Managing and maintaining legal, regulatory, and contractual obligations
- The increased risk of external software applications (apps) introducing malware
- The risk for exposure of company data due to increased device use for non-business-related activities