The Current State of BYOD

This paper, produced by the analysts and researchers of CTOlabs.com, provides context you can use on the topic of enterprise mobility, with a focus on the trend towards Bring Your Own Device (BYOD).

Overview

Bring your own device, or BYOD, is one of the fastest growing trends in information technology. Much of the workforce now owns their own mobile devices, typically referring to smartphones and tablets but also, in some cases including laptops, and has incorporated them into their daily workflows, checking email, the news, and communicating with friends and family. They want these capabilities at work as well, and while some government and industry enterprises provide employees with devices, they would rather use their preferred device, which they can access anywhere and anytime. Employers have found that they can sometimes increase productivity and satisfaction while decreasing costs by allowing employees to bring their own devices and use them for work, causing a boom in BYOD in government and industry.

BYOD has a number of advantages over traditional IT policies. A recent study by the Aberdeen Group found that in the top 20% of firms implementing BYOD successfully, there was a 90% success rate of accessing critical information within the necessary timeframe which is a 42% year-over-year improvement, as well as a 72% year-over-year improvement in productivity. Some firms, such as Cisco, also saw major savings compared to using only company-provided information technology. When enacted carefully, the added mobility, familiarity, and connectivity of BYOD can be revolutionary for IT.

The Risks of BYOD

BYOD is not without risks and disadvantages. Even with employees purchasing their own devices, BYOD is not significantly cheaper, and can often be more expensive because of the difficulty of managing a variety of different platforms. If those devices are mismanaged, the costs can be staggering due to information leaks. According to the same Aberdeen report, the cost of compliance lapses ranges from $10,000 to $491,000 per instance, with one lost, stolen, or hacked mobile device now powerful enough to cause several lapses. Violations of the Health Insurance Portability and Accountability Act (HIPAA) are some of the most costly, averaging over $147,000 per lapse and, according to the 2012 HIMSS Analytics Report on Security of Patient Data, 22% of respondents with healthcare data breaches said that lost or stolen mobile devices were the cause.
An influx of employee-owned mobile devices increases risk to an enterprise for multiple reasons. Mobile operating systems are not yet as mature as their PC counterparts, with less robust built-in security and many unpatched or undiscovered vulnerabilities. Mobile applications are also notoriously insecure, with infected apps spreading on the poorly regulated Android Market and reports of applications screened for Apple’s App Store accessing private data without consent. Even trusted applications may access private data, with Facebook, Apple, Twitter, and Yelp among 18 companies named in a recent lawsuit.

True BYOD initiatives that allow the full spectrum of Android devices and operating systems instead of only Apple and Blackberry requires securing a very broad array of platforms, perhaps with separate solutions. Managing diverse user devices becomes especially difficult if Android devices are rooted, which allows further customization of the operating system and greater privilege to applications, or Apple devices have been jailbroken, which similarly allows root access for iOS. This diversity of devices and operating systems, combined with employee ownership, makes it hard for the IT department to control what happens on the device or enforce security policy. This in turn enables risky behavior and makes support difficult. Mixing personal and professional use on a device also increases risks. Some of those risks are physical, as a device constantly in use in a variety of locations and settings is more likely to get lost or stolen. Others involve cybersecurity, such as users being more lax with their own data, which has less value than business data, or downloading more unverified applications to one device, increasing the attack surface.

Despite these risks, the potential productivity boost has led to an explosion of BYOD policies in government and industry. The Aberdeen Group reports that over half of 415 respondents from 39 countries worldwide permitted any employee-owned device to access their network, with a survey from the SANS Institute showing that over 60% of organizations allow employees to bring their own devices for work, with both of those figures increasing yearly. A third survey by ESET and Harris Interactive found that 80

**Government Leading The Way**

The US Government has funded research into security solutions for mobility in three broad areas:

1) Concepts and best practices, including coordination of collaborative community standards maintained by NIST and DISA
2) Technologies for encryption, including encryption of data in transit and at rest, and
3) Technologies for configuration management and risk reduction on mobile devices.

The US Government has also lead in establishing visions and goals for enhanced secure mobile access for an extended workforce and through the President’s May 2012 Federal Government Digital Strategy is the latest example of this visionary push for mobile, calling for establishment of a Digital Services Innovation Center chartered to coordinate issues like these across agencies we expect this leadership to continue.
percent of employed adults use some kind of personally-owned electronic device for work-related functions, with 24% of those who use their smartphones accessing or storing company information on their device along with 41% for personal laptops and 47% for personal desktops.

While government has been more cautious, there has been a large push towards implementing BYOD wherever possible, with some agencies such as NASA, the GSA, and the Department of Agriculture embracing the policy, others, such as the Department of Veterans Affairs, more hesitant but pursuing pilot programs, and only a few, such as the NSA, ruling using employee devices out entirely for the foreseeable future.

**Security Policies Not Keeping Up**

The adoption of personal devices in the workplace has been so rapid that security policy has not kept pace. According to Aberdeen's survey, even among those the top performers, 75% did not have basic security measures such as passwords in place for tablets. 72% of top performers required secure
authentication before allowing personal devices on to corporate networks, 70% had clear policy and compliance standards, 63% had policies that covered the entire lifecycle of compliant mobile devices, and only 55% enforced compliance for enterprise data on employee devices.

The SANS Institute looked more broadly at enterprises implementing BYOD and found an even greater lack of oversight. Less than 10% of respondents were fully aware of the mobile devices on their networks, 31% said they did not have BYOD usage and security policies, 26% only “sort of” had policies in place, 24% said that BYOD policies were added to existing security regulations, 17% had stand-alone BYOD policies, and 3% did not know what rules, if any, governed BYOD at their organization.

While half of organizations had stored data and malware protection policies, only 40% had policies dealing with applications. And though over half the organizations said that user education was part of their mobile device security policies on the SANS survey, for the ESET-Harris survey 64% of employees claimed to have gotten no security training from their employers. The survey also confirmed that many devices were missing the most basic security measures. Less than half of BYOD laptops had auto-locking with password protection, less than a third of smartphones, and only one in ten tablets.
In the rush to adopt BYOD in the private sector, security has fallen behind. We know forward thinking planners in the federal government have been diving into this issue and are generating promising approaches. And we believe mobile risk management is not necessarily complicated, and solutions are available to mitigate most threats to a wide variety of personal devices, going beyond traditional mobile security tools. Mobile risk management aims to balance freedom with mitigation so that users can still take advantage of the overwhelming productivity and convenience benefits of BYOD while decreasing the inherent threat, as opposed to restrictive risk avoidance policies.

Though Bring Your Own Device shows great promise, its explosion in use means extra thought should be placed in approaches to take for reducing risk. With the high cost of breaches and the increased threat of theft, loss, or malware from employee devices, mobile risk management is a crucial though often underutilized part of implementing BYOD. Developing a good mobile risk management plan and the right mobile security toolset can not only help make BYOD more successful but also help government agencies benefit from this revolution in IT.
More Reading

For more federal technology and policy issues visit:

- **CTOvision.com** - A blog for enterprise technologists with a special focus on Big Data.
- **CTOlabs.com** - A reference for research and reporting on all IT issues.
- **J.mp/ctonews** - Sign up for the Government Technology Newsletters.

About the Authors

**Bob Gourley** is CTO and founder of Crucial Point LLC and editor and chief of CTOvision.com. He is a former federal CTO. His career included service in operational intelligence centers around the globe where his focus was operational all source intelligence analysis. He was the first director of intelligence at DoD’s Joint Task Force for Computer Network Defense, served as director of technology for a division of Northrop Grumman and spent three years as the CTO of the Defense Intelligence Agency. Bob serves on numerous government and industry advisory boards.

Contact Bob at bob@crucialpointllc.com

**Alexander Olesker** is a technology research analyst at Crucial Point LLC, focusing on disruptive technologies of interest to enterprise technologists. He writes at http://ctovision.com. Alex is a graduate of the Edmund A. Walsh School of Foreign Service at Georgetown University with a degree in Science, Technology, and International Affairs. He researches and writes on developments in technology and government best practices for CTOvision.com and CTOlabs.com, and has written numerous whitepapers on these subjects. Alex has worked or interned in early childhood education, private intelligence, law enforcement, and academia, contributing to numerous publications on technology, international affairs, and security and has lectured at Georgetown and in the Netherlands. Alex is also the founder and primary contributor of an international security blog that has been quoted and featured by numerous pundits and the War Studies blog of King’s College, London. Alex is a fluent Russian speaker and proficient in French.

Contact Alex at AOlesker@crucialpointllc.com
For More Information

If you have questions or would like to discuss this report, please contact me. As an advocate for better IT in government, I am committed to keeping the dialogue open on technologies, processes and best practices that will keep us moving forward.

Contact:
Bob Gourley
bob@crucialpointllc.com
703-994-0549

All information/data ©2011 CTOlabs.com.