7 Steps to a Sensible BYOD Strategy

So You Can Sleep at Night

eGroup
Technology Solutions for Serious Competitors

Contents

eGroup Corporate Office
482 Wando Park Blvd.
Mt. Pleasant, SC 29464

1.877.eGroup.1 (1.877.347.6871)

www.eGroup-us.com

Introduction: The monsters under the bed

These days, IT leaders wake up in a world where one-third of young employees use three different devices. [1] For many, it's a nightmare because there's a gang of monsters hiding under the bed:

- The torment of lost devices bearing mission-critical data;
- The specter of 8,000 new types of mobile malware found in the first three months of 2012[2];
- The ghost of hidden costs;
- The stress of out-of-control device-support demands;
- The threat of legal and compliance issues.

No wonder 73% of UK IT directors surveyed said they are concerned BYOD will cause IT costs to "spiral out of control".[3] Their fears are supported by Aberdeen Group's finding that a company with 1,000 mobile devices spends an extra $170,000 per year, on average, when it uses a BYOD approach. [4]

Yet, most IT leaders aren't disputing the business case for BYOD. Eighty percent said they think enterprises with a BYOD policy gain a competitive edge over other organizations. In fact, the business reasons for BYOD are so compelling that, even despite the risks, four out of five companies from 11 different countries said they now allow BYOD or will within the next two years. [5]

Research shows employees are now using personal devices at work with or without the blessing of IT. [6] Here are seven steps to help develop a BYOD approach that will let you sleep at night.

Step 1: Confront the monsters

The blurring of boundaries between work and life has become the lifestyle of the modern employee. BYOD is a maturing of business infrastructure to incorporate this trend. If companies don't drive the change, executives and employees will.

Companies that don't adjust to the new reality may find themselves vulnerable: Juniper Networks found four out of 10 of 4,000+ respondents reported using their personal device for work without permission.[7]

Companies that wake up to BYOD attract top talent and handle change better

Even more disturbing, Osterman Research found that 44% of the workers it surveyed were using the cloud-based file storage system Dropbox without company approval.[8] Without a sound BYOD strategy in place, a company can quickly lose control over where its data resides.

Companies that wake up to the BYOD reality can attract and retain the top C-level and staff talent who demand it. They have the agility to handle today's fast pace of disruptive competitors, mergers and acquisitions, extreme climate events, and other sudden changes. They can find better ways to interact with customers. Their employees can innovate and find new efficiencies in their roles.

It's time to confront the monsters and create a BYOD strategy that is safe, cost effective, and focused on driving business results.

Step 2: Start with a security audit

Security is the number one concern when implementing BYOD. And the threats are real. One-third of IT leaders surveyed by Juniper Networks reported their company has already experienced a security threat as a result of personal mobile devices. [9]

You need a security plan that balances risks with benefits

But there is a danger in being too restrictive. Devices that are too difficult to use or slow defeat the purpose and undermine the business case for BYOD. You need a security plan that balances the risks with the benefits.

The ideal place to start is an audit of the company's entire network. Inventory all the locations where sensitive data are stored: filing cabinets, flash drives, desktop computers, and, yes, mobile devices. Talk frankly to staff from different departments to get a picture of where they keep data.

Then, take a look at how sensitive data comes into the company and consider the following questions:

- What kind of information is collected at each entry point?
- Who has access to this information?
- Where are the potential leaks?

While this task may seem daunting, a complete security audit may turn up leaks that should be plugged right away.

Step 3: Think beyond the desktop

A lot of sleepless nights can be relieved by a shift in IT thinking: away from routine hardware provisioning and maintenance toward more strategic application and activity management. Desktop virtualization, pioneered by VMware, is the simplest way to achieve this shift. Customized desktops link to user identities, not hardware devices. End users can access their data from any qualified device, regardless of where they are: a key requirement of mobile effectiveness.

For effective BYOD, IT should shift its focus from the mundane to the strategic

With the virtual desktop, corporate and personal data are kept separate in a secure and auditable way. This approach removes most security nightmares, plus many of the worries about legal liability. And it enables IT to maintain centralized control over security, policy enforcement, and delivery of content across devices.

When IT has central control over applications, networks that authenticate BYOD devices can be isolated so users access only the data and applications they should. Isolation also minimizes the risk of malware. IT can ensure that users who access sensitive data operate within stated guidelines and, for example, restrict USB capabilities for finance employees, or prevent credit card numbers from being copied or printed.

An effective BYOD strategy rests on a shift in thinking from provisioning devices to deploying applications and managing activity; in other words, a shift in focus from the mundane to the strategic.

Step 4: Don't foot the whole bill for BYOD

Hidden costs are another spooky factor preventing companies from addressing BYOD. Many hidden costs can be avoided with an app-centered vs. device-centered approach. For example, IT staff should look to certify operating systems, not devices.

Sand Hill Group reports that BYOD usually results in a short-term increase and a long-term decrease in costs—but only if employees are responsible for their own devices. [10]

BYOD usually results in a short-term increase but a long-term decrease in costs

Companies can ease the pain by providing stipends for device purchase and monthly bills. For example, VMware adopted a BYOD program that required all 6,000 employees to use their personal smartphones for work. The company capped reimbursements by job function: a salesperson was allotted $250 a month while most employees were capped at $70. In the end, VMware CIO Ron Egan reports a 30% saving on the company's phone bills.[11]

The onus must be on employees to get a warranty and access tech support through that warranty. Some may argue that employee downtime during device malfunction is another hidden cost, and "a CIO simply cannot expect executives to run to the Apple Genius Bar" every time a device doesn't do what they want it to do.[12]

This is where a little creativity comes in:

- Set specific times for IT to help with devices.
- Promote a self-help culture with internal Wikis.
- Hold lunch-and-learn sessions where people share device-knowledge and work-life balance strategies.

Another concern is a loss of control over software license fees. A key strategy here is to set up an in-house app store where employees can download corporate-approved apps they need and recommended apps they may want. This gives IT better control over app deployment and makes it easy to provision new employees or employees who need to replace lost or obsolete devices.

Shifting who-pays-what in your company may seem like another nightmare. But the business benefits are worth it. Depending on an employee's role, companies save $300 to $1,300 a year per employee. As well, Cisco estimates that every employee who tele-commutes only one day per week saves another $2,500 a head.[13]

If done right, the company will face some upfront costs for infra-structure, training, increased bandwidth and range, and accommodating the rush of employees who'll want to join. From then on, costs should be modest and the savings will accumulate.

How to keep BYOD costs under control

1. Certify operating systems, not devices.
2. Provide a stipend to help buy devices and pay monthly bills.
3. Put a role-based cap on monthly reimbursements.
4. Require employees to access warranty tech support.
5. Set up specific hours when IT can help with mobile devices.
6. Promote a self-help culture with internal wikis.
7. Hold lunch-and-learn sessions to share tips and ideas.
8. Set up an internal app store for downloading required and recommended apps.

Step 5: Involve your employees

Employee buy-in, particularly if the company has been paying all the bills, could lead to some tossing and turning. The best thing to do is involve employees from the beginning. Start by noting what they are already bringing into work. Let them take these devices out of hiding and talk about how they could use them with company support. Tap into employee insights about which apps are good.

The more people you bring in, the more people you'll have taking ownership and helping to drive end-user adoption when the time comes to introduce the program to everyone.

To gain employee buy-in, involve them from the start and ask their opinions

When VMware initiated its BYOD program, it was more radical than most. The company adopted an aggressive 90-day window for *all* employees to make the switch to personal smartphones. CIO Mark Egan admits some employees were angry about having to spend their own money on something that used to be covered.

Employees "lit up" the company's internal social network as they worked through the BYOD process. "They used it to pass along carrier information, such as when AT&T was running a special or when T-Mobile was offering a package with unlimited data," says Tim Young, VMware's VP Social Enterprise.[14]

Having employees share tips and bargains this way helped everyone settle down for the night.

Step 6: Devote time to policy development

Allow plenty of time in your schedule to develop sound policies. For example, have employees sign a clear understanding of their responsibilities and the consequences if breached. Consider a lost device: When should the company have the right to wipe its data? To ensure employees don't hesitate in reporting lost devices, think about creating a two-step procedure. First lockdown the device, and then after a certain delay, wipe it.

Employees must understand up front if the company needs to wipe data from a lost device

Other questions to consider include the following:

- **Devices**: Are all devices included in the program? What is the refresh cycle? Who bears the cost? What is the process?
- **Applications**: Which are forbidden and why?
- **Data plans**: Who bears the cost? Stipend? Cost limits?
- **Acceptable use**: Is there a penalty for using the device to badmouth the company or spread hate? Can a family member use the device?
- **Wipeout**: Secure the right to wipe data from a lost device. We can't repeat this enough.

Another key factor in policy development is making sure you have firm and consistent buy-in from C-level executives. If the company leadership flouts BYOD policies, these will be tough to enforce at the staff level.

Step 7: Educate everyone

Plan to spend part of your budget on education. Does your current IT staff have the know-how to lead the charge to BYOD effectiveness? What additional skills will they need?

The goal is a tech-savvy workforce that shares knowledge and discovers best practices

It's not enough to hand down policies to employees. Make sure they genuinely understand and take them seriously. In its study of 2,000 IT managers and users, BT Assure found that one in three employees were so uninformed they said there was "no risk" in using their own devices in a work context.[15]

Again, work with HR to identify the alpha-users who can drive change and the tech-evangelists who can spread the word. The goal is to hit a tipping point where your employees gel into a tech-savvy workforce that knows its responsibilities, shares tips, and discovers best practices that benefit the entire organization.

Conclusions

We are entering a new era where workers expect more freedom and independence over how they do their jobs. Nearly half of all college grads say they'd accept a lower-paying job with more flexibility around device-choice and social media access rather than a higher-paying job with less flexibility.[16]

So don't let the gang of monsters under the bed prevent your company from establishing an effective BYOD strategy. Help your company wake up to a world where most customers carry a mobile device in their pocket or purse. Tap the competence and knowledge in your workforce as you create a well-managed program that lets you sleep at night.

For help moving your company to an effective BYOD strategy, contact eGroup's End-User Computing Team at ApplicationServices@eGroup-us.com or call toll-free 1.877.eGroup.1.

About eGroup

Providing customers across the southeast with a distinct competitive advantage since 1999, eGroup is a visionary technology solutions and services firm with the ability to execute swiftly in a rapidly changing information technology landscape.

Our solutions drive customers' cost containment, revenue growth, and service objectives by addressing challenges associated with mobility, access to critical applications and data, and security.

eGroup's expertise and core competence is focused in three distinct areas: Cloud Services (public and private), Application Services, and End-User Computing. To deliver these solutions, eGroup has strategic partnerships with industry leaders that include VMware, Cisco, and EMC, along with Citrix, Microsoft, and Trend Micro, and a highly-skilled workforce trained in all of the latest developments in information technology.

For more information, visit www.egroup-us.com

Endnotes

1: “The New Workplace Currency —It’s not just salary anymore: Cisco study highlights new rules for attracting young talent into the workplace,” *Cisco News Release*, November 2, 2011
http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=532138
2: “A Global Study Indexing Consumer Confidence in Mobility,” *Juniper Networks Trusted Mobility Index*, May 2012
http://www.juniper.net/us/en/local/pdf/additional-resources/7100155-en.pdf
3: “73% of IT directors fear BYOD costs will ‘spiral out of control’,” *Damovo press release*, June 26, 2012
http://www.damovo.com/documents/BYODResearchPressRelease-June2012-FINAL.pdf
4: Park, Hyoun, “The True Cost of BYOD,” *Aberdeen Group Blogs*, February 6, 2012
http://blogs.aberdeen.com/communications/the-true-cost-of-byod/
5: “BYOD gives competitive advantage, say IT managers,” *BT Press Releases*, May 16, 2012
http://www.btplc.com/news/Articles/Showarticle.cfm?ArticleID=741139D3-592C-426E-9904-EB4540663C19
6: Ibid, *Juniper Networks Trusted Mobility Index*
7: Ibid, *Juniper Networks Trusted Mobility Index*
8: “Putting IT Back in Control of BYOD,” *Ostherman Research Inc.*, June 2012
http://www.ostermanresearch.com/whitepapers/download166.htm
9: Ibid, *Juniper Networks Trusted Mobility Index*
10: Rangaswami, M.R., “Hidden Cost Factors and Total Cost of Ownership for Enterprise Mobility,” *SandHill.com*, April 24, 2012
http://sandhill.com/article/hidden-cost-factors-and-total-cost-of-ownership-for-enterprise-mobility/
11: Kaneshige, Tom, “VMware Going ‘All In’ with BYOD,” *CIO.com*, May 11, 2012
http://www.cio.com/article/706274/VMware_Going_All_In_with_BYOD
12: Kaneshige, Tom, “The BYOD Troubleshoot: Security and Cost-Savings,” *CIO.com*, March 30, 2012
http://www.cio.com/article/703185/The_BYOD_Troubleshoot_Security_and_Cost_Savings
13: Barbier, Joel, Joseph Bradley, James Macaulay, Richard Medcalf and Christopher Reberger, “ BYOD and Virtualization,” *Cisco IBSG Horizons Survey Report*, 2012
http://www.cisco.com/web/about/ac79/docs/BYOD.pdf
14: Ibid, *CIO.com*, May 11, 2012
15: Ibid, *BT Press Releases*
16: Ibid, *Cisco News Release*