Bring Your Own Device (BYOD)

Key Steps for an Effective Program

Gordon Braun
John Hollyoak

July 2012
## Agenda

- Introduction - What is BYOD?
- BYOD Trends
- So What’s the Problem?
  - The Fundamental Challenge
  - Risks and Threats
- Where Do We Go From Here?
  - Key Steps For an Effective Program
- Example Case Studies
- Conclusions & Takeaways
- Q&A

“...the times they are a-changin”
– Bob Dylan, 1964
The Consumerization of Business Technology
How Has Your Company Responded?

http://www.youtube.com/watch?v=98qKjTAUMbA
BYOD Trends

Smartphone sales in 2011

31% of all phone sales (472 million units) → Up 58% from 2010

Historic, limited-use “corporate”
Blackberry only 8.8% of market →
Sales down 10% in Q4 2011

Newer, “personal” Smartphone's
(Apple/Android) sales 75% of market →
Market share up 64% from 2010

Source: Gartner (February 2012)
BYOD: Did You Know?

Devices entering the marketplace:

Android and iOS Devices were activated on 12/25/11
(includes smart phones and tablets)

BYOD Practices in 2011

- 3% of employers Did Not Have a BYOD Policy
- 71% of employers Allowed Personal Devices

Who pays for data usage

- 28% of employers reimburse
- 72% of employers do not reimburse

Usage of Personal Devices by Employees

Many employees are using their personal devices for a variety of work related tasks – Voice calls, content creation and reviewing content top the list:-

Source: McKinsey 2012 iConsumer survey on the consumerization of mobile devices
The days of limited, corporate-provided Smartphone's . . .

. . . are coming to an end
Protiviti Webinar Polling Results

Q1. Does your organization have an existing BYOD program?

- Yes: 56%
- No: 44%

Q2. Do you use a personal device for work which is not currently supported by your IT department?

- Yes: 30%
- No: 70%
Protiviti Webinar Polling Results (cont.)

Q3. If you are in an IT or security role, have you felt pressure to support a specific device?

- Yes: 69% (63 Votes)
- No: 31% (28 Votes)

Q4. Do you have more than one device (excluding a laptop) that you regularly carry?

- Yes: 59% (57 Votes)
- No: 41% (40 Votes)
Protiviti Webinar Polling Results (cont.)

Q5. Do you use a device that is not RIM/Blackberry, Apple, or Android?

No: 91%
Yes: 9%
BYOD: Bring Your Own Device – Defined

Employees using their personal mobile device to access corporate resources such as email

Typically refers to smart phones such as the iPhone

Also includes other devices such as an iPad
Advantages of implementing BYOD

Advantages of BYOD – these include some motivating tangible and intangible benefits that are otherwise tricky to achieve:

- Improved Employee Satisfaction
- Lower Communication Costs
- Lower Support Costs
- Increased Productivity
- Increased WLAN Security Control
So What’s the Problem with BYOD?

- Devices present in riskier locations/situations
  - Expensive phone target for theft
  - Lost devices at bars

- End-user control over security
  - Freedom to install applications that may contain malware
  - Weak or no passwords/PINs
So What’s the Problem with BYOD?

- Multiple security trust levels on same device
  - Angry Birds and corporate secrets on same device
  - Millions of apps in app stores – are they all safe?

- Connecting to more untrusted networks
  - Wi-Fi hotspots
  - Lack of VPN

- Lack of predictability: You don’t know what the device will be, where it will be, or how it will behave
Key Steps to Building an Effective Program

- Establish Business Needs & Use Cases
- Evaluate Risks & Threats
- Consider Which Platforms to Support
- Consider Operational Impacts
- Understand Tools and Technology Available
- Understand Legal, Privacy, Other Considerations

Operationalize the Program
Decisions and conclusions need to be clearly documented in policies and procedures and communicated to employees.
Establish Business Needs and Intended Use Cases

- What devices and models do employees want to use?
- What enterprise resources are employees trying access?
- What applications do employees want to use on their mobile devices?
- Where do employees want to access these resources?
- What are employees’ expectations around usability?
- What are employees already doing today?
Evaluate Risks & Threats
Your Organization’s Risk Profile and Tolerance

- Review plans through the organization’s established risk assessment process
- Consult with key stakeholders
- Organizational size, industry, and desired use cases will vary
- What are the compliance implications?
- What are we most concerned about?
Evaluate Risks & Threats

What Are We Trying To Protect Against?

- Data leakage or data loss
- Direct attacks (e.g., un-patched OS’s/app vulnerabilities)
- Indirect Attacks (e.g., phishing)
- Bridging attacks (e.g., 3G network to corporate networks)
- Peer-to-Peer networks (e.g., Bluetooth, Wi-Fi, USB)
- Authorized apps that behave badly (e.g., grab contact lists or other information on the phone)
- Rogue or “jailbroken” devices
Consider Which Mobile Platforms To Support

- Some platforms are more "enterprise ready" than others
- Each platform presents a unique set of challenges or hurdles that must be considered
- How will older or outdated devices be handled?
- Will all makes/models be supported or only a few?
- Who supplies updates and security patches?
- How quickly?
- Are there limitations associated with each platform?
Consider Which Mobile Platforms To Support

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Rapid consumer growth and demand</td>
<td>• Still not enterprise friendly</td>
</tr>
<tr>
<td>• Tight “end-to-end” platform integration</td>
<td>• Lacking robust options for IT to control and secure</td>
</tr>
<tr>
<td>• Improved security controls/layers</td>
<td>• “Fragmentation” across vendors and carriers</td>
</tr>
<tr>
<td>• Rapid consumer growth and demand</td>
<td>• App eco-system not tightly controlled</td>
</tr>
<tr>
<td>• Open platform, lots of flexibility and customization</td>
<td>• Decentralized patch support</td>
</tr>
<tr>
<td>• Mature, established platform, built for the “enterprise”</td>
<td>• Closed platform</td>
</tr>
<tr>
<td>• Strong security &amp; controls</td>
<td>• Decline in consumer demand</td>
</tr>
<tr>
<td>• Granular management tools</td>
<td>• App “eco-system” is immature and lacking adoption</td>
</tr>
</tbody>
</table>

The Next Big Consumer Device . . .
Consider Operational Impacts

How will devices be provisioned or enrolled (e.g., employee self-enrollment, IT manual enrollment)?

How will users get support with issues or hardware/software problems?

How will the devices be managed?
• Minimal management
• Partial or hybrid management
• Full management
• How much control do we want to impose?
Balancing Flexibility vs. Management and Control

<table>
<thead>
<tr>
<th>Minimal Management Few Controls</th>
<th>Partial Management Basic Controls</th>
<th>Full Management Restrictive Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic management of devices and basic policies. Some functionality may be restricted.</td>
<td>Devices are heavily controlled with restrictive policies and granular management</td>
<td></td>
</tr>
<tr>
<td>Minimal management over devices. Little to no policies or controls restricting devices.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Control & Security vs. Cost & Complexity

© 2012 Protiviti Inc. CONFIDENTIAL: This document is for your company's internal use only and may not be copied nor distributed to another third party.
Understand Existing Technologies and Tools

- What existing enterprise IT solutions or technologies are already in place?
  - Microsoft ActiveSync
  - BlackBerry Enterprise Server (BES)
  - Remote access solutions
- Establish the gaps in current state vs. future state
  - Are my existing tools good enough?
- If needed, identify solutions to replace or compliment existing technology
  - Mobile device management (MDM) solutions
  - “Containerization” or “sandbox” solutions
### Example Vendor Solutions

#### Mobile Device Management (MDM) Solutions
- Tools to facilitate robust management of mobile devices in an enterprise environment.
- Can provide mechanisms for enrollment, policy enforcement, security, application deployment, and support.
- Supports wide range of mobile devices and OS's.
- Integrates with existing IT infrastructure

#### Containerization/Sandbox Solutions
- Solutions designed to segregate enterprise data into secure containers or “sandboxes”
- Does not leverage native or built-in device functionality
- Facilitates secure data storage and/or data transmission

### Example Vendors

- **MobileIron**
- **Maas360**
- **BoxTone**
- **Sybase**
- **airwatch**
- **Citrix**
- **vmware**
- **Pinecone**
- **Good**
- **Fixmo**

*Note: Protiviti is an independent firm with no relationship, ownership, or financial interest in any of the companies noted above.*
Other BYOD Considerations

**Legal/user privacy**

- Remote wiping a personal device
- Use/access of personal information on device(s)
- Device tracking information
- E-Discovery / Legal Hold
Other BYOD Considerations

Establish clear organizational position and policies

Which devices (make and models) will be supported?

Who will own the devices?

Who will pay for the devices?

Who will pay for the plans?

User agrees to abide by polices (e.g., acceptable use)

Consent form, acknowledging that restrictions will be placed on their device
Example Case Study – Global Law Firm

Key Program Highlights

- Implemented a BYOD program to accommodate growing demand from senior partners that wanted to use a non-RIM device
- Key concerns were centered around meeting contractual and confidentiality obligations with clients.
- Employed “containerization” software to achieve separation of user / corporate data.
- Developed custom iOS application(s) to bridge functionality gap and foster access to internal applications.
- Evaluating the feasibility of co-mingling user / corporate data (e.g., enabling “native applications” to be used).

Lessons Learned

- “Usability” was a critical success factor
- Access to critical internal document management systems and other firm-specific applications was the key driver
Example Case Study – Global Consulting Firm

Key Program Highlights

- Implemented a BYOD program to accommodate growing demand from highly mobile consultants / road warriors.
- Stipend was established for device reimbursement and monthly voice/data plans.
- Control framework was coupled with planned technology refresh cycles and projects (Exchange upgrades) and existing technologies (BlackBerry BES).
- Staged rollout of platform support, stringent requirements on version and hardware type (e.g., old devices are not supported).
- Minimal device support provided, employees are responsible for hardware and carrier bills.

Lessons Learned

- Users were willing to give up direct billing in exchange for device freedom.
- Basic device support and basic access to corporate resources (email, calendar) satisfied the majority of needs.
Example Case Study – Citrix

In 2008, Citrix launched a BYOD program for its worldwide employee base.

The program launched in 2008 provided full-time employees with a choice of either receiving the standard corporate IT-managed laptop or using a personal device, either a PC or Mac.

The employee can either purchase a new laptop or use an existing personal laptop, with the stipulation that they have a vendor maintenance program for the duration of their three-year enrollment in the program.

Reactions to BYOD were mixed. Some welcomed the approach. Others believed that users would not be able to manage on their own without some level of IT involvement.
Example Case Study – Citrix (cont.)

The approach that Citrix adopted was the reason for their success:

1. Survey the Employees

   - A prepilot survey gauged employee reactions to a BYOD program.
   - Twenty-three (23%) percent of employees responded, and the results helped Citrix to understand whether the program would be of interest, identified elements that influenced participation, and drove recommendations for the program components (i.e., what people wanted from the program).
   - Of those surveyed, the majority were enthused by the prospect of having a choice beyond the current slate of IT offerings.

2. Set the Stipend

   - To determine the stipend amount, existing device costs (including procurement, imaging, security, deployment, monitoring, and maintenance) were factored in.
   - The purpose of the stipend was to allow program participants to purchase a laptop that was comparable to a Citrix-managed device and for Citrix to realize savings of up to 18%.
Example Case Study – Citrix (cont.)

3. Review Corporate Policies

- The Citrix BYOD policy is less than two pages.
- They focused on keeping the rules the same for all, with the same policies in effect for both Citrix-managed and personal devices.
- As Citrix no longer owned the device, in the event of litigation employees would have to be subpoenaed to gain access to their devices.

4. Review Security

- Existing corporate security policies applied whether the employee had a Citrix-managed device or a personal device.
- On the device side, there is antivirus and two-factor authentication.
- Employees connect to their applications via the Citrix SSL/VPN, using Citrix Access Gateway coupled with perimeter firewalls, intrusion detection and prevention (IDS/IPS), web filtering, and overall threat management.
5. Draft the Program’s Rules

To keep the program efficient and easy to follow, Citrix made 10 rules which are as follows:

- Manager approval is required
- The employee receives a $2,100 stipend (minus applicable taxes) for a laptop and a three-year maintenance plan.
- If the employee leaves the company within the year, the stipend is prorated.
- Employees participating in the BYOD program must return their managed laptops to their manager(s).
- All BYOD hardware issues are to be addressed by the vendor.
- Antivirus software is required on all BYOD laptops.
- All personal devices must connect remotely through Citrix Receiver/Citrix Access Gateway.
- All applications must be delivered (online and offline) by the data center.
- Applications are to be provisioned through Citrix Receiver.
- All existing corporate policies apply.
Example Case Study – SAP

In a rapidly expanding list of companies, SAP offers the option to use either a corporate-owned or personally owned mobile device for work.

Employees can either purchase their device through a corporate catalogue or bring in their own device (from an approved list).

This BYOD approach was put in place to address the trend of consumerization of IT—allowing employees to own a single device for both business and personal use.

The program at SAP is driven and managed by IT and has a cross-discipline team with contributions from legal, human resources, finance, IT, and internal communications departments.
Example Case Study – SAP (cont.)

Key Program Highlights

- Managed data, not devices:
  - Focus on data management and flexibility in device choice
  - Reduce impact on security/legal/HR/regulatory issues
- Separated personal data from corporate data:
  - Reduced corporate liability associated with potential private-data impact
  - Improved ability to fulfill legal obligations associated with litigation-hold and e-discovery requests
- Ensured full security (encrypted, password-protected vault)
  - Implemented controls to protect corporate data in the event a device is lost, stolen, or used by non-employees

Benefits

The IT team recognized significant benefits including:

- Enrollment is 100 percent self-service
- It takes only one minute to decommission a service
- 92% reduction in provisioning and app-deployment cycle times
Conclusions & Key Takeaways

- Organizations must be proactive in addressing the BYOD demand

- It’s critical to clearly define business needs and intended use cases

- There’s no single “best” approach; however there are important steps and common strategies
Conclusions & Key Takeaways

- Flexibility vs. control will be unique to an organization’s risk tolerance and culture

- The tools and technology to manage and secure various mobile platforms are still immature and incomplete

- Decisions must be clearly defined and communicated
Contact Information

Gordon Braun
Director
Phone: +1 913.661.7406
gordon.braun@protiviti.com

John Hollyoak
Senior Manager
IT Consulting - Security & Privacy
Phone: +1.312.364.4907
john.hollyoak@protiviti.com
Powerful Insights. Proven Delivery.®