BYOD - Consumer driven IT

Today, consumers possess powerful devices for their personal needs. Often, the computing power and features of the devices bought by employees, is much higher than that of similar devices provided by their organization. Organizations are therefore trying to leverage this computing capability to augment or supplement their information technology (IT) needs. Leveraging of employees devices for enterprise purposes is known as Bring Your Own Device (BYOD). We are observing an increase in organizations adopting the BYOD philosophy, although the percentage is still very small.

BYOD trends have evolved over time. Business phones have provided mobile email for a decade, but the market has moved from business phones complete with corporate controls to consumer devices such as tablets and smart phones. These devices enable easy Internet access anywhere-anytime, with sophisticated applications that allow true mobile productivity. In addition to the above, BYOD also helps brings unique operating system (OS)/ software / app platforms to accomplish tasks. Hence, BYOD leads to Bring Your Own Technology (BYOT) and these terms are often used synonymously.

BYOD - Benefit or Bane?

BYOD adoption brings forth benefits as well as challenges to an enterprise. A common concern that BYOD poses to an organization is the security challenge of introducing a non-trusted and unmanaged device. There could be additional risks and overheads in managing them.

However, BYOD offers a wide range of benefits such as improved productivity of the mobile worker and an opportunity to contain costs on end user computing environment. Further, with rapid advancements in the technology world and an organization’s need for frequent refresh cycles (hardware, OS and software), - we observe that a typical consumer refreshes his/her devices in less than 2-3 years, which relieves the additional burden of technology refresh on the organization.

- Ecosystem Definition
- BYOD Policy
  - Inventory coverage
  - Usage Policy
  - Security Policy
  - Support Policy
  - Device Termination/ withdrawal Strategy
  - Governance
- Deployment Planning & Considerations

BYOD Strategy
Despite the challenges, we observe that it is imperative for organizations to prepare themselves for BYOD adoption. Organizations have to lay down a clear adoption strategy and plan for its implementation and it is important to create and reuse existing assets/framework for designing/managing the BYOD environment. The following sections focus on the strategy and key considerations for organizations to adopt BYOD.

**BYOD – Strategy for adoption**

BYOD brings with it a wide range of new and advanced OS technologies, powerful computing on smart devices and multiple options for wireless connectivity. While these are attractive to tap into, organizations need to focus on the following points while defining the strategy:

- **Ecosystem definition and segmentation** - This involves the identification of the stakeholders, device types and access to be supported. User types should be segmented to decide on the device and determine access needs. It is also important to define the business capabilities that need to be available through these devices. As a starting point, organizations can start with the existing remote user/connectivity definition that was created with corporate devices in mind. The existing system can be reviewed and enhanced to close gaps. Figure 2 gives an example of how BYOD ecosystem and roles can be profiled.

<table>
<thead>
<tr>
<th>Role Profile</th>
<th>BYOD Device Type</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive User</td>
<td>Tablets, Smartphones</td>
<td>Email, Critical Reporting application and Dashboards, Workflow, Document Management Systems etc</td>
</tr>
<tr>
<td>Management Team (Product Management, Managers etc)</td>
<td>Tablets, Smartphones</td>
<td>Email, Workflow, Document Management Systems etc</td>
</tr>
<tr>
<td>Mobile User (Sales)</td>
<td>Laptop</td>
<td>CRM and related DMS, and access to Enterprise Network</td>
</tr>
<tr>
<td>Production Support/Remote User/Home User (Tech support, developers, operations etc)</td>
<td>Desktop/Laptop</td>
<td>Access to Enterprise Network</td>
</tr>
</tbody>
</table>

**Typical Ecosystem & Role Profiling**

- **BYOD Policy** - Post the ecosystem definition, a BYOD policy comprising inventory coverage and usage, security and support policy should be developed to help achieve the following objectives:
  - Secure, reliable, speedy access to the enterprise environment
  - Skills, technologies, processes, methods of managing new devices
  - Methods for building and deploying applications for these new devices

A comprehensive BYOD policy should define the following:

- Inventory coverage and usage
- Security and controls
- Support for the ecosystem
- Device termination/withdrawal process
- Governance
These aspects of a BYOD policy are elaborated below:

- **Inventory Coverage and Usage policy** - While the existing policy for devices can be leveraged, it is important to lay down the accepted list of device vendors, network vendors, device and network coverage plans, alternate plans (including loaning policies for devices and secondary network coverage where ever applicable) and expected device backup strategy. A mapping of all users to the actual device, based on their role, profile and segmentation, should be carried out. (For e.g.: restricting laptop as an accepted BYOD for a role that will require intense computing). A sample stage-wise coverage roadmap is depicted below:

- **Security controls/policy** - Security policies should consider the following key aspects:
  - Password policies for devices (desktop / BlackBerry/ mobile).
  - Policies for secure online/offline transfer of information through applications on BYOD devices.
  - Restrictions on applications that can run on the BYOD device (apps running process and data - hardening the device).

Existing corporate/enterprise security policy can be enhanced. It is important to provide centralized and simplified management of BYOD devices. To summarize, while reaping the benefits of a diversified BYOD ecosystem, an effective security policy should balance the risks to the organization.

---

**Recommended Roadmap for Coverage**

---

**Balancing IT Security vs. Needs**
Support for the ecosystem – With the expanded ecosystem and its impact on the organization, a clear definition of the boundaries of who owns the support of each of the components is important. In a BYOD environment, organizations need to focus on application/data/device/network ownership and support. Organizations typically leave the device and network management to their service providers. As a prerequisite to onboard a device, the organization could review service provider reliability and device provider coverage mandatorily. The ability to define a visible service level agreement (SLA) for the entire ecosystem with appropriate backup strategies is important. Organizations should evolve a centralized management for multiple devices and multi-platform devices.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Managed Devices</th>
<th>Unmanaged Devices</th>
<th>SLA (sample and role dependent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner of the Device</td>
<td>Enterprise</td>
<td>Employee</td>
<td>NA</td>
</tr>
<tr>
<td>Device Support</td>
<td>Enterprise</td>
<td>Employee/Vendor</td>
<td>24 hours turnaround or alternate device availability</td>
</tr>
<tr>
<td>Network &amp; Network SLA (For remote user)</td>
<td>Enterprise</td>
<td>Employee/Service Provider</td>
<td>4 hours or Alternate mode of connectivity for access</td>
</tr>
<tr>
<td>Network &amp; Network SLA (For campus user)</td>
<td>Enterprise</td>
<td>Enterprise</td>
<td>30 minutes or alternate mode of access thru secondary link/network</td>
</tr>
<tr>
<td>Application &amp; Enterprise Data support</td>
<td>Enterprise</td>
<td>Enterprise</td>
<td>30 minutes or turnover to DR site</td>
</tr>
<tr>
<td>Backup strategy/execution (for laptop/workstation based users or thin client users)</td>
<td>Enterprise</td>
<td>Employee</td>
<td>Weekly Backup strategy</td>
</tr>
<tr>
<td>Backup strategy/execution (Mobil, Tablet etc. or thin client users)</td>
<td>Enterprise</td>
<td>Enterprise</td>
<td>Daily Backup Strategy</td>
</tr>
</tbody>
</table>

**Recommended boundary definition**

- **Device termination/withdrawal strategy or process** - Following the definition of on-boarding and support processes, it is mandatory to clearly define the exit strategy for on-boarded BYOD devices. This should include ways to automatically blacklist devices, applications, and profiles from a centralized gateway. This can be linked to device change or retirement strategy.

- **Governance** - A good governance system to facilitate, deploy and monitor the entire ecosystem is the key to successful BYOD implementation. It is recommended to successfully build and digitize the entire BYOD life cycle - starting from on-boarding, management, withdrawal etc. - from the user's perspective. This system should have the following features - on-boarding process (request, review, approval), withdrawal/retiring process, usage policies, support process (self help, assisted help), enterprise app mart (facilitating easy installation and management of applications).

Following the definition of a BYOD adoption strategy, its successful deployment is of critical importance. While the segments on both high-end computing platforms and smart computing platforms are evolving, there are many products that provide pointed solutions and wide coverage for organization-wide BYOD adoption.

**BYOD Deployment Plan Considerations**

Many organizations possess strong in-house capabilities in managing high-end computing devices and traditional OS segments (Windows, UNIX flavors). However, companies should also focus upon the area of smart devices and associated technologies. Unlike the traditional OS segment, this is fast evolving and building an in-house custom capability could consume precious resources and time. Considering this, Mobile Environment Management (MEM) is very important.
Like BYOD, Mobile Environment Management is also an evolving term. It has gained significance with the continuous evolution of BYOD devices, platforms, technologies and the different adoption use cases. While managing BYOD devices, control policies should not restrict personal use of the devices.

MEM should provide management of device, app and data management layers to ensure secure access to corporate data from personal devices. MEM should encompass the following areas:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Mobile Data Management

To summarize, the above management layers attempt to give fully centralized/remote management layers to manage devices, application and data respectively. While there is limited availability of a single suite of products in the market to cover the entire spectrum, there are products that provide pointed solutions.

On the device side, strategies are evolving at the hardware level to provide segregation of personal and corporate processes.

All personal and corporate activities are stored in two different locations:

- A highly secure and accessible location for a corporate gateway app with multifactor authentication and
- A widely accessible location for personal use

On the enterprise side, as we move away from traditional email access (Blackberry or any other device) and provide access to enterprise capabilities (app and data), many design principles evolve on both the network and application design layers. One such recommended network deployment setup is given in Fig.6 where an isolated private network houses applications designed for this purpose. Application streaming and desktop streaming (virtual desktop environment) are two different patterns which dominate the segment.

To start with, the use of Virtual Desktop Infrastructure (VDI) is recommended for BYOD adoption. For organizations that do not have VDI, application streaming or application adaptation path needs to be adopted. Enterprise applications such as workflow notification/approval and dashboards are good candidates to be early movers into this segment.

It is important for organizations to assess the costs associated with BYOD implementation (custom/product based approach) and the potential benefits (for e.g. productivity, innovation, employee satisfaction). This analysis could form the basis for developing and implementing an appropriate BYOD strategy.

**BYOD - A mandate:**

We see a strong need for organizations to prepare themselves for a new phase where the use of personal devices within the enterprise ecosystem - BYOD - will be the norm, rather than an exception. Organizations need to be ready for this eventuality and prepare accordingly. This could involve extending the existing building blocks within the organization and accommodating the needs of new and non-managed devices. A phased approach can be adopted for execution depending on the maturity level of the organization. Organizations should not regard BYOD as the implementation of one more control policy, but rather as a way of opening up an appropriate segment of enterprise applications (mail, workflow, thin client access for specific purpose etc.) and providing simplified ways to access/use personal devices for day-to-day activities.
About the Author

Annamalai Anbukkarasu (Anbu) is an enterprise architect with the Banking and Financial Services (BFS) unit of TCS focusing on Mobile and Channel solutions. His current responsibilities include consulting, architecture design, solutions, pre-sales and sales support for the BFS Mobile solutions. His 14+ years of IT experience includes working on large IT projects/programs and Transformations and Channel solutions. He has played key roles in the Contact Center space as a part of Channel Solutions for large banking and financial customers. His expertise in this space includes speech-enabled (recognition and authorization) and open standard based applications (VXML). He holds a Masters degree in Engineering with specialization in Optical Communications.
Contact
For more information about TCS’ Banking & Financial Services, email us at bfs.marketing@tcs.com

About Tata Consultancy Services (TCS)
Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com