Leveraging and Securing the Bring Your Own Device and Technology Approach

Gaurav Priyadarshi, CISA, BS 25999 LI, ISO 27001 LA, ITIL V3, is a senior security consultant at TATA Consultancy Services, a leading IT service company with worldwide experience in the information security domain. Priyadarshi is a technology evangelist and a follower of trending security concepts. He can be reached at *gpriyadarshi@gmail.com.*

The IT infrastructure that was created at the beginning of the IT era remains a constant framework for the future. Just as everything in life evolves, the IT environment and its landscape transform. Today, IT must continue to grow.

The bring your own device (BYOD) trend of enabling and empowering employees to bring their own devices (e.g., laptop, smartphones, tablets) has expanded to bring your own technology (BYOT) including office applications (e.g., word processing), authorized software (e.g., data analytics tools), operating systems, and other proprietary or open-source IT tools (e.g., software development kits, public cloud, communication aids) to the workplace. This coupling has been coined as bring your own device and technology (BYODT). As BYODT becomes increasingly acceptable and popular, it is likely to be one of the biggest challenges for information security governance.

This article describes some of the pros and cons of BYODT and outlines the various security governance steps to be taken by enterprises that are considering adopting a BYODT approach.

PROS FOR IMPLEMENTING BYODT

Implementing BYODT can result in numerous benefits including:

- **Happy employees**—BYODT makes (most) employees happier and more satisfied as they prefer to use their own devices over the often budget-oriented and dull devices offered by the company. Employees may also prefer to reduce the number of devices they carry while traveling; before BYOD, traveling employees would carry their personal and company-provided devices (i.e., two mobile phones/smartphones, two laptops and so forth).
- **Cost savings**—Implementation of a BYODT program can also result in a substantial financial savings to IT budgets because employees can use devices and other IT components they already possess.[1] The savings include those made on the purchase of devices for workers, on the maintenance of these devices and on data plans (for voice and data services). These savings can then be utilized by the company to enhance its operating margins or to offer more employee benefits.
- **IT workload optimization**—The IT department can be freed from a myriad of tasks such as desktop support, trouble shooting and end-user hardware maintenance activities. This savings can then be leveraged by the IT department to optimize its budget and resources.
- **Faster adoption of new technology**—The BYODT trend is attributed, in part, to the fact that employees adopt technology well before their employers and subsequently bring these items to work. Thus, BYODT results in faster adoption of new technologies, which can also be an enabler for employees to be more productive or creative—one resulting area of competitive advantage for the business.
- **Increased employee efficiency**—Employees can use their own, familiar device to complete their tasks more efficiently as it gives them the flexibility to quickly customize their device or technology to run faster and per their requirements.[2] On the other hand, in the case of company-provided devices and technology, such customization is often time-consuming as the employees have to provide proper cost justifications and then seek authorization through change requests.

CONCERNS OF BYODT

As with all other evolutionary approaches, BYODT comes with its own set of concerns and objections:

- **Security governance and administration complexities**—By allowing employees to BYODT, companies are opening a new chapter for security managers and administrators. The security governance framework and corporate security policies will need to be redefined and a great deal of effort will be required to make each policy efficiently operational and streamlined.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

- **Increased concerns with privacy and data protection (PDP)**—This could be perhaps the biggest challenge for BYODT. In some industries that deal with sensitive and confidential data, PDP concerns will hamper a rollout of BYODT. Such enterprises will have to tread cautiously with this trend.
- **Increased challenges with ownership of data and regulatory compliance**—By adopting BYODT, organizational control over data is blurred. Objections are also raised when business and private data exist on the same device. This could interfere with meeting the stringent controls mandated by certain regulatory compliance requirements.
- **Lack of uniformity and compatibility issues**—Applications and tools may not be uniform on all devices, which can result in incompatibility when trying to, for example, connect to the corporate network or access a Word file created by another employee who has purchased a newer version.
- **Reluctance by employees**—There may be a lack of consensus among employees; some may not be willing to use their personal devices or software for company work.

THE VERDICT

This discussion of pros and cons is displayed through the schematic diagram in **figure 1**.

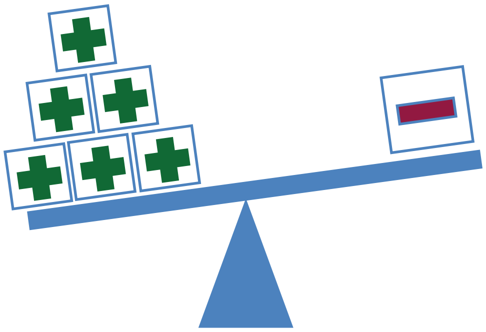
Clearly, the ongoing trend and the benefits realized from BYODT suggest that the concerns should be considered as challenges and companies should address BYODT implementation by leveraging these challenges.

LEVERAGING AND MITIGATING CHALLENGES AND OBJECTIONS OF BYODT

The following approach can assist in the successful implementation of a BYODT program that mitigates security challenges:

- **Establish a well-defined BYODT governance framework.** This can be done by soliciting input from various departments of the enterprise regarding how different areas use portable gadgets. This helps create a uniform governance strategy. Following are the essential steps for creating a BYODT governance framework:
  - **Network access control:**
    1. Determine which devices are allowed on the network.
    2. Determine the level of access (e.g., guest, limited, full) that can be granted to these devices.
    3. Define the who, what, where and when of network access.
    4. Determine which groups of employees are allowed to use these devices.
  - **Device management control:**
    1. Inventory authorized and unauthorized devices.
    2. Inventory authorized and unauthorized users.
    3. Ensure continual vulnerability assessment and remediation of the devices connected.
    4. Create mandatory and acceptable endpoint security components (e.g., updated and functional antivirus software, updated security patch, level of browser security settings) to be present on these devices.

Figure 1—Pros and Cons of BYODT



- Happy employees
- Savings for employers
- IT department workload optimization
- Faster adoption of new technologies
- Boost to employees' productivity

- Complex security governance
- Data privacy concerns
- Regulatory compliance
- Lack of uniformity and compatibility
- Reluctance by some employees

– **Application security management control:**

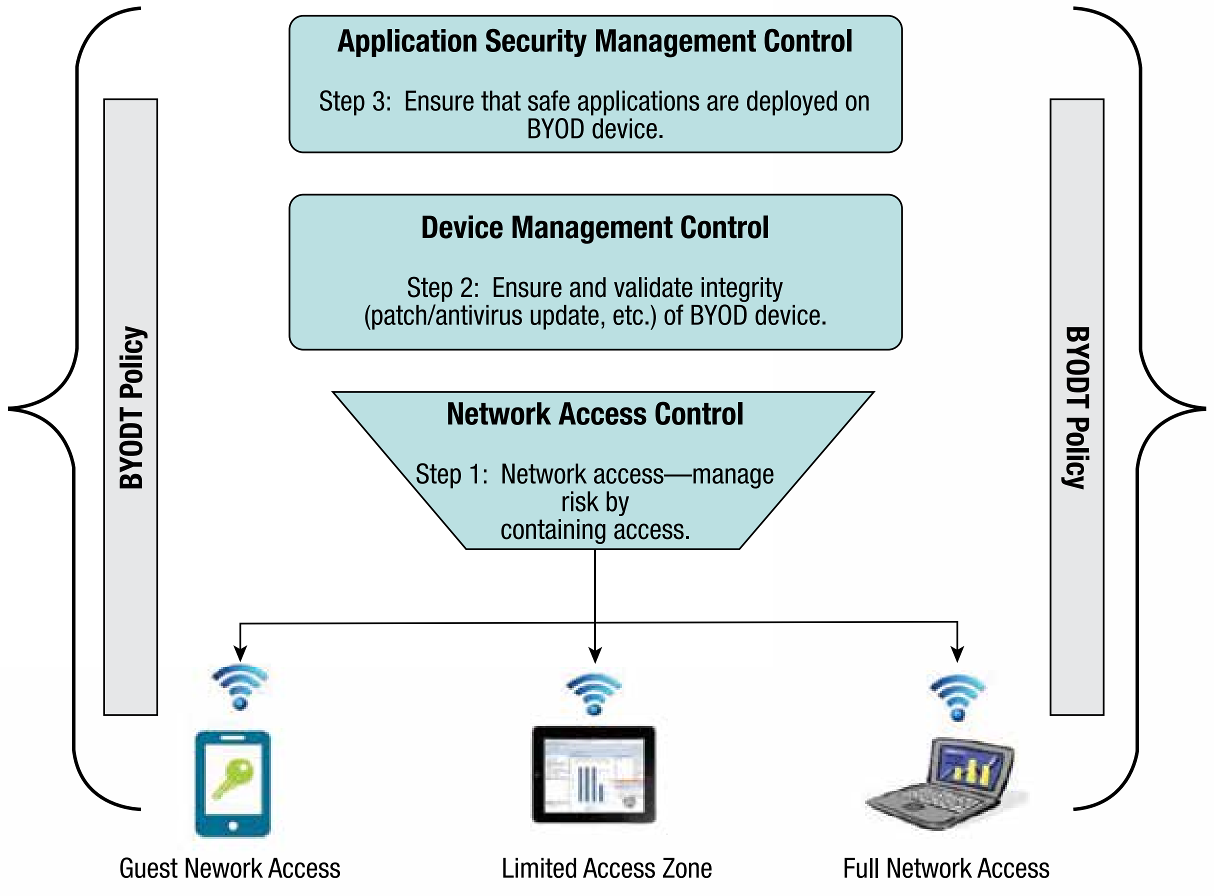
1. Determine which operating systems and versions are allowed on the network.
2. Determine which applications are mandatory (or prohibited) for each device.
3. Control enterprise application access on a need-to-know basis.
4. Educate employees about the BYODT policy.

Figure 2 schematically represents the steps to be taken to reach the maturity of BYODT governance in order to establish a BYODT program.

- **Create a BYODT policy.** Make sure there is a clearly defined policy for BYODT that outlines the rules of engagement and states the company's expectations. The policy should also state and define minimum security requirements and may even mandate company-sanctioned security tools as a condition for allowing personal devices to connect to company data and network resources.

BYODT security requirements should be addressed by having the IT staff provide detailed security requirements for each type of personal device that is used in the workplace and connected to the corporate network. For example, IT staff might require devices to be configured with passwords, to prohibit specific types of applications from being installed on the device, or require all data on the device to be encrypted. Other BYODT security policy initiatives might include limiting activities that employees are allowed to perform on these devices at work (e.g.,

Figure 2—Blueprint of BYODT Governance


BYODT Policy
Application Security Management Control
Step 3: Ensure that safe applications are deployed on BYOD device.
Device Management Control
Step 2: Ensure and validate integrity (patch/antivirus update, etc.) of BYOD device.
Network Access Control
Step 1: Network access—manage risk by containing access.
BYODT Policy
Guest Nework Access
Limited Access Zone
Full Network Access

limiting email usage to corporate email accounts only) and periodic IT audits to ensure the device is in compliance with the company's BYODT security policy.

Figure 3 provides a sample BYOD policy.

Figure 3—Sample BYOD Policy

Bring Your Own Device Policy

[Employer] would like to provide greater IT device choice to its employees and simultaneously reduce end-user IT device complexity…Thus, [Employer] is implementing a "Bring Your Own Device" (BYOD) program to permit [Employer] personnel to use personally owned smartphones and tablets for business purposes. This document applies to employees…

Current BYOD Approved for Use

1. Android smartphones and tablets (version 2.2 or higher)
2. …

Expectation of Privacy

[Employer] will respect the privacy of your personal device and will request access to the device by technicians only to implement security controls as outlined below…

Information Technology/Responsibilities

The information technology (IT) department is responsible for configuring and supporting the user's device to receive and access company email, calendar and contact data…

Employee Responsibility and Requirements for all BYODs Accessing [Employer] Network Services

1. User is responsible for using company email on his/her personal smartphone within the same constraints as on a company-owned device.
2. User agrees that he/she will password-protect the device via the device's operating system's available password-protection protocols.
3. User's device will be remote wiped if (i) you lose the device, (ii) your employment with [Employer] ends, or (iii) IT detects a data or policy breach or virus.

User Acknowledgment and Agreement

It is [Employer]'s right to restrict or rescind computing privileges or take other administrative or legal action due to failure to comply with the BYOD Policy. Violation of these rules may be grounds for disciplinary action up to and including termination.

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of [Employer] service.

Employee Name: ____
BYOD Device(s): ____
Employee Signature __________________________ **Date:** ___________

- **Use virtualization as a solution.** Windows 8, Windows Server 2012 and the Microsoft Desktop Optimization Pack (MDOP) provide virtualization solutions that can be used to enable BYODT. Windows Server 2012 enables the user to easily create a virtual desktop infrastructure (VDI).

  VDI is an alternative desktop delivery model that can help enable BYODT. It gives users secure access to centrally managed desktops running in the data center. With employees using their personal devices, they can access the hosted desktop for work while keeping their work and personal environments separate.

  VDI removes the limitations of maintaining a stringent acceptable client list for an organization (e.g., Dell Latitude 5400S and Mac Books only) and allows end users to use their preferred devices that ultimately connect back into a managed VDI. As long as the devices have a support view client, they should be permissible for use within the company.
- **Use the sandbox approach.** Organizations planning to allow storage of corporate data on mobile devices must assess the risk and classification of the data on those devices. Implementing a BYODT strategy should include considerations of data classification and different access methods for different types of data in the IT environment. One approach is sandboxed applications. This approach boxes corporate data into a separate container that can be secured with passwords and other authentication mechanisms; nonbusiness data are kept separate and users can continue to use their devices for personal use.

  Should the device be lost or the employee leave the company, corporate data can be wiped from the device while leaving personal data intact. The downside to this approach is that this method often limits the use of the phone for email and calendaring, often considered one of the greatest advantages of having an integrated device.
- **Separate personal and corporate data.** Some employers make connecting with an employee-owned device contingent on signing an agreement allowing the company to monitor compliance with acceptable-use policies and otherwise act to protect corporate data. In some cases, the agreement may include remote wiping of all data on the device—potentially including personal data—which can be a source of contention between IT and users if not properly managed.

- **Maintain secure access to the corporate network.** Device choice does not mean sacrificing security. IT must establish the minimum security baseline that any device must meet to be used on the corporate network, including Wi-Fi security, virtual private network (VPN) access and, perhaps, add-on software to protect against malware. In addition, due to the wide range of devices, it is critical to be able to identify each device connected to the network and authenticate both the device and the person using the device.

CONCLUSION

BYODT provides numerous benefits to the business, the key ones being reducing the IT budget and the IT department's workload, faster adaptation to newer technology, and making employees happier by giving them flexibility to use and customize their devices to enhance efficiency at work. Of course, various challenges come along with BYODT: increased security measures, more stringent controls for privacy and data protection, and other regulatory compliance.

These challenges provide a fundamentally new opportunity for innovation, redefining the governance structure and adoption of underlying technology. Clearly, the way forward for organizations is to mitigate the challenges of BYODT, align it with their future IT strategy and put it on the IT road map so that they can move ahead in the evolutionary cycle and thereby bring benefits and flexibility to one of their most important stakeholders—their employees.

REFERENCES

Bradford Networks, "Fallout of the iPod Holiday: The 10 Steps to a Secure BYOD Strategy," 20 December 2011, *http://www.slideshare.net/BradfordNetworks/the-10-steps-to-a-secure-byod-strategy*

Cisco, "Cisco Bring Your Own Device (BYOD) Smart Solution Design Guide," 20 December 2011, *http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html*

Honeycutt, Jerry; *Introducing Windows® 8: An Overview for IT Professionals*, Microsoft Press, USA, 2012

Hyman, Jonathan; *The Employer Bill of Rights: A Manager's Guide to Workplace Law*, Apress, USA, 2012

Mann, Andi; George Watt; Peter Matthews; *The Innovative CIO: How IT Leaders Can Drive Business Transformation*, Apress, USA, 2012

Meyler, Kerrie; Byron Holt; Marcus Oh; Jason Sandys; Greg Ramsey; *System Center 2012 Configuration Manager Unleashed*, Pearson Education Inc., USA, 2012

Moore, Connie; "Bring Your Own Technology: The Lines Between Work and Personal Technology are Blurring," Forrester, 26 November 2012, *http://blogs.forrester.com/connie_moore/12-11-26-bring_your_own_technology_the_lines_between_work_and_personal_technology_are_blurring,*

ENDNOTES

[1] Forrester, *Key Strategies to Capture and Measure the Value of Consumerization of IT*, May 2012, *www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf*

[2] *Ibid.*