BYOD POLICIES: BEST PRACTICES FOR BYOD IN THE ENTERPRISE

Not so long ago, the Bring Your Own Device (BYOD) movement was largely contested across the enterprise segment. Proponents of the BYOD trend focused the debate on the productivity benefits of BYOD while the polar opposites uncompromisingly considered it as a liability in context of the inherent security challenges. Both sides remained adamant on their stance until progressive organizations riding the wave of enterprise mobility took the action, tamed the beast within and unleashed the unprecedented value propositions that BYOD has to offer. These actions involved strategic best practices and layers of risk mitigation activities that enabled BYOD devices to power workforce productivity and yield profitability for the organization without compromising security.

Preparing to Support Innovation

The concept of BYOD thrives in Agile and DevOps-driven environments where users take advantage of well-integrated cloud solutions to facilitate collaboration, communication and information access across otherwise siloed organizational departments. However, the movement falls short between business and IT as the IT service desk fails to support legitimate needs of the increasingly agile and mobile workforce. BYOD enhances the responsibilities of ITSM to incorporate quality assurance, audits and control; security, updates and vulnerability management; and support for new apps, platforms and devices, among others.

Repeated requests, unfavorable governance and slow request approval processes encourage the

workforce to adopt Shadow IT practices bypassing the security mechanism designed to reduce risks associated with BYOD. In order to address these challenges, organizations must invest in the right skillset and advancement in IT transformation to align ITSM capabilities with the BYOD needs of fast-paced DevOps-driven processes. From a strategic perspective, the following policy best practices can empower organizations to achieve these goals:

1. Understand Organizational Requirements

Every organization differs in structure, culture, diversity, workforce preferences, IT policies and even the regulatory compliance requirements. These differences enhance between geographic location, industry vertical, size and age of the organizations. As a result, every organization may have unique limitations on BYOD technology adoption, preferences and requirements. In DevOps environments, the organization must empower ITSM to develop protocols and procedures designed to facilitate their own unique BYOD requirements in context of the challenges they face. This approach will ensure smooth BYOD adoption that leads to workforce productivity without disrupting the behavior, compliance and security posture of the organization.

2. Develop Holistic and Flexible Policies

While it may be practically impossible to satisfy every member of the workforce with BYOD policies, the organization must establish BYOD policies designed for every user, department as well the diverse tech-business and compliance requirements. The BYOD policies should encompass different user roles, privileges and controls necessary as part of the organization's mobility strategy. The most engaging enterprise mobility strategies that facilitate effective collaboration, information access and strict adherence security best practices focus on flexibility and a user-centric approach. Establish simple and automated workflows that make it easier for internal customers to enroll their devices and request approvals for new apps and solutions. Outline the security requirements with clear, simple and easy-to-understand details. Future-proof your BYOD strategies to address the upcoming needs of internal customers and the business landscape. Finally, respect end-user privacy by implementing the necessary protocols to segregate personal data from business information and apps on BYOD devices.

3. Keep Track of BYOD Usage

BYOD devices are common targets for sophisticated security attacks. A vulnerable BYOD device with high-level user access and privileges can cause costly data leaks and irreversible damages to the business. With the enforcement of stringent new regulations such as the GDPR in EU, organizations must balance workforce demands for BYOD against regulatory compliance and security threats.

The security risk and implications of BYOD adoption have emerged as a top concern among business organizations according to a recent Verizon report. Real-time security monitoring and anomaly detection therefore becomes critical to ensure secure enterprise mobility practices with BYOD. IT needs to track a range of metrics pertaining to network traffic and security, understand how users and apps access corporate information and restrict data consumption and information access based on organizational security and business policies.

4. Workforce Education

End-users have the potential to act as the first line of defense against cyber-attacks or the first loophole in BYOD security. Knowledgeable and security-aware professionals can help ward off a majority of cyber-attacks that initiate with downloading malicious apps, accessing rogue websites or clicking links on unsolicited phishing email attempts. Train and convince your workforce to comply with your organization's security and BYOD policy. Educate them on the security risks associated with Shadow IT practices. Provide them with adequate reasons and pathways to avoid security malpractices. Finally, establish a culture of trust and loyalty among the workforce to reduce the possibility of employees going rogue against the organization. This is especially critical, since BYOD devices with access to corporate the network grant disgruntled employees the opportunity to cause real damages the organization.

5. Empower IT with the Right Tooling

Forward-thinking business organizations transform their IT to meet the enterprise mobility and BYOD needs of today and tomorrow. Organizations need to understand their current working environment and clarify the desired future state of enterprise mobility. BYOD policies should be designed to engage internal customers with the right processes, data and technologies to transition between the current and desired future states. Employ capabilities such as automated device enrollment and configuration, and real-time troubleshooting to reduce service desk interactions. Adopt ongoing app vetting processes based on simple and automated workflows that make it convenient for ITSM to comply with app approval requests.

Invest in advanced Enterprise Mobility Management (EMM) that enable IT admins to facilitate the evolving and diverse BYOD needs of the agile workforce. Multiple layers of security should be in place to protect BYOD devices; protect corporate data; facilitate effective communication and collaboration; and manage access controls and risks. BYOD policies should also include the tooling necessary for risk mitigation and damage limitation in response to security infringements.

Lastly, an effective BYOD policy should be designed to instigate a cultural shift toward secure and productive enterprise mobility practices. DevOps already brings best practices that facilitate strong interdepartmental collaboration, integrated business and IT operations, and automated workflows that streamline the adoption of new apps, technologies and processes. For organizations yet to adopt DevOps, BYOD policies should be designed to identify and eliminate the inhibitors to BYOD success including isolated IT departments; siloed business and IT operations; slow and inadequate governance procedures; and the unnecessary walled gardens that force employees to adopt Shadow IT alternatives.