BRING YOUR OWN DEVICE (BYOD): BEST PRACTICES FOR THE WORKPLACE

Not so long ago, the Bring Your Own Device (BYOD) movement was largely contested across enterprise organizations. Proponents of the BYOD trend focused the debate on the productivity benefits of BYOD. Opponents uncompromisingly considered it as a liability.

Both sides remained adamant until progressive organizations riding the wave of enterprise mobility took action, unleashing the value that BYOD has to offer. These actions involved strategic best practices and layers of risk mitigation activities that ultimately enable BYOD devices—and their users—to:

- Power workforce productivity
- Yield profitability for the organization
- Adhere to enterprise security needs

So, in this article, let's look at why more and more people want BYOD. Then, we'll consider the hard question: is BYOD really worth the security headache?

What is BYOD?

BYOD is a set of policies that allow employees to bring in and use their own personal devices. These devices can include laptops, smartphones, tablets, whatever is needed to complete the tasks they face.

The goal behind BYOD is straightforward: because workers use their personal devices to access company data and systems, employees should be more productive in the long run.

Today, of course, many companies are creating distributed workplaces, powered in part by more relaxed approaches to BYOD. When the pandemic hit, an employee might not have been able to easily work from their phone or tablet. Now a variety of software solutions support employees in the brave new world of remote work, making BYOD important in a way it had never been before.

BYOD practices thrive in Agile and DevOps-driven environments. Users should take advantage of well-integrated cloud solutions to facilitate collaboration, communication, and information access across otherwise siloed organizational departments.

Challenges of using personal devices for work

Although many find the idea of using a personal device quite attractive, BYOD initiatives need to be carefully considered. Employee satisfaction and overall enterprise agility needs to be carefully weighed against the risks and the necessary Mobile Device Management (MDM) that needs to happen before employees can download potentially sensitive data to their devices.

Other challenges of using personal devices for work include…

Poorly supported internally

BYOD falls somewhere between the business and IT functions, resulting in service desks that often fail to support the needs of the agile and mobile workforce. That's because service desks were mostly built to service on-premises employees using employer-provided equipment.

This stark divide leads to many data and security concerns for businesses, particularly when they cannot meet the demand of their employees.

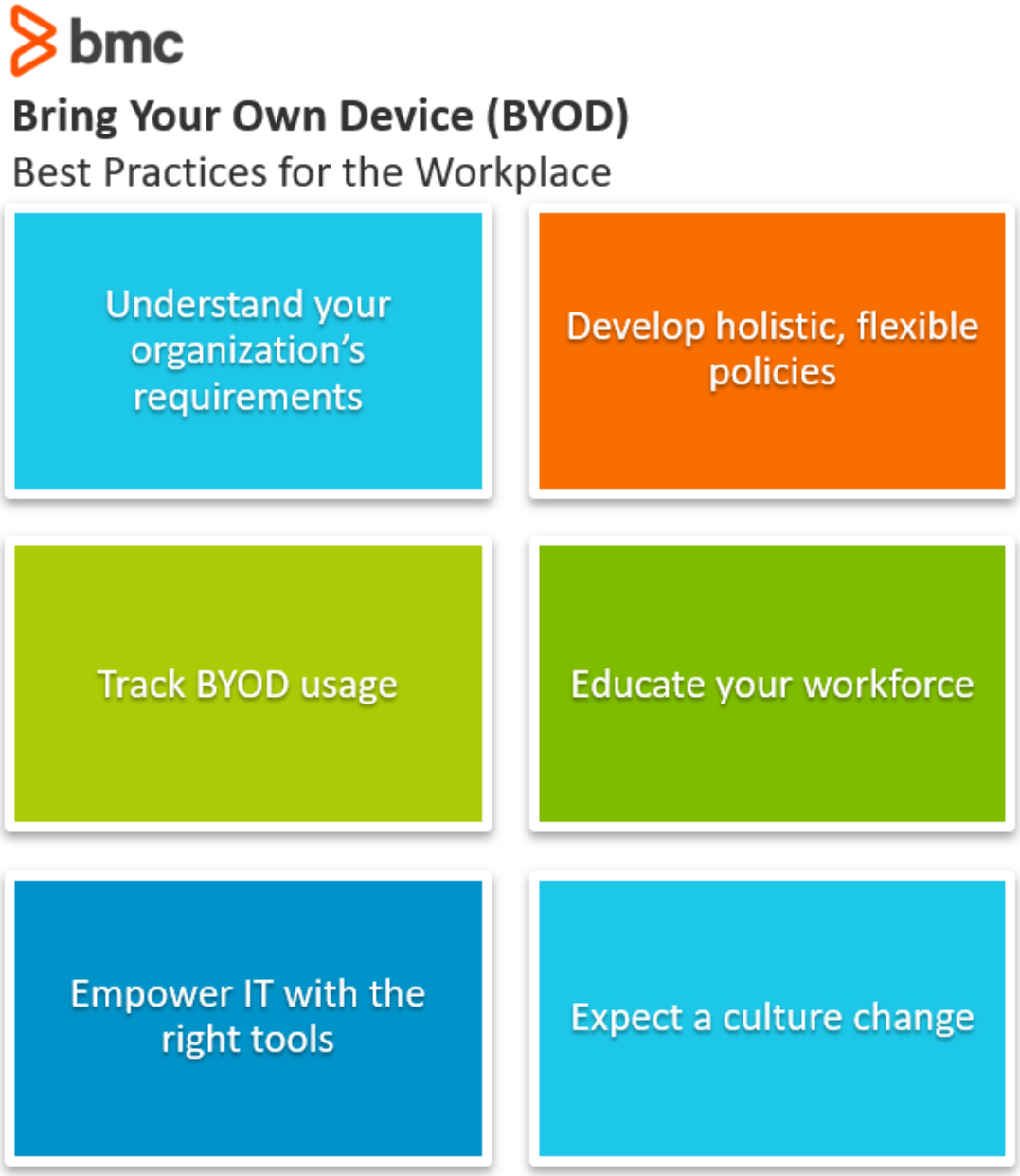
Shadow IT

Repeated requests, unfavorable governance, and slow request approval processes encourage the workforce to take matters into their own hands. Employees may adopt shadow IT—the grey area where users download or use software and apps that your organization hasn't approved. The risk here? These shadow IT practices bypass your security mechanisms.

Lost property

The elephant in the room is the lost/stolen problem. Although it's nice for your employees to complete work-related tasks with their own mobile devices, there is a serious risk of your employees losing the device and placing company data into the hands of possibly anyone, especially with cloud-native apps that make syncing and sharing data as easy as pressing a button.

For industries that need a high level of security on every single device, think about what you gain and what you have to trade. Are the benefits of BYOD solutions enough to warrant storing data on a device which might be secure? That's a question which a lot companies answer differently.



Best Practices for BYOD in the Workplace

To address these challenges, organizations must invest in the right skillset and advancement in IT transformation to align service management 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 regulatory compliance requirements. These differences are exacerbated due to your company's:

- Geographic location
- Industry vertical
- Size and age

As a result, every organization may have unique limitations on BYOD technology adoption, preferences, and requirements.

In DevOps environments, the organization must empower the service management function to develop protocols and procedures designed to facilitate their own unique BYOD requirements in the 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 a flexible BYOD policy

It is practically impossible to satisfy every member of the workforce with BYOD policies. Regardless of the device, BYOD policies should encompass different user roles, privileges, and controls as part of your mobility strategy.

The most engaging enterprise mobility strategies that facilitate effective collaboration, information access, and strict adherence to security best practices do take a flexible, user-centric approach:

- **Establish simple, 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.
- **Respect end-user privacy** by implementing the necessary protocols to segregate personal data from business information and apps on BYOD devices.

3. Track BYOD usage

BYOD employee-owned devices are common targets for adversaries, especially in the age of AI cyberattacks. Vulnerable personal devices with high-level user access and privileges can cause costly data leaks and potentially irreversible damage to the business.

With the enforcement of stringent data regulations like GDPR, 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 Verizon.

Managing corporate data through intelligent mobile device management is key to appeasing your employees who want to use their personal devices—without allowing said devices become an easy route for sensitive data leaks. Real-time security monitoring and detection become 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
- Restrict data consumption and information access based on organizational security and business policies through effective security measures

4. Educate the workforce

End users 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 when downloading malicious apps, accessing rogue websites, or clicking links in phishing attempts.

Train and convince your workforce to comply with your organization's security and BYOD policy in a few ways:

- **Educate employees** on the security risks associated with Shadow IT practices.
- **Provide adequate reasons and pathways** to avoid security malpractices.
- **Establish a culture of trust and loyalty** among the workforce to reduce the possibility of employees going rogue against the organization.

When devices may become the agents of your downfall, the last point is especially important. If you are going to trust your employees to bring their own tablets, laptops, and phones to work with, you need to trust your employees generally too. The technology is a risk, but so are the people you trust to use them!

5. Empower IT with the right tools

Forward-thinking business organizations transform their IT to meet the mobile device 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.

- **Automate device enrollment and configuration** as well as real-time troubleshooting in order to reduce the number of headaches that personally owned devices will give you service desk.
- **Adopt 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 enables IT admins to facilitate the evolving and diverse BYOD needs of the agile workforce.
- **Implement multiple layers of security** to protect BYOD devices; protect corporate data; facilitate effective communication and collaboration; and manage access controls and risks.
- **Include the tooling necessary for risk mitigation** on devices and damage limitation in response to security infringements.

(Read more about enterprise mobility management.)

6. Expect a culture change

Finally, 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.

Design your BYOD policies to identify and eliminate the inhibitors to BYOD success, such as:

- Isolated IT departments
- Siloed business and IT operations
- Slow and inadequate governance procedures
- The unnecessary walled gardens that force employees to adopt shadow IT alternatives

Do I need to implement BYOD?

Mobile devices are everywhere, and they bring the amazing potential to do something great. Personal devices not only improve employee output and happiness, but they bring cost savings too.

For companies that want to enable employees to use their own mobile devices to connect to the work network, think about your security posture and failsafes. Although you have the technology to implement the policy, could your organization suffer data loss through lost or stolen devices? Do you have enough security responders to put out the fire if something compromises a laptop that isn't secure?

If you're working in an agile environment, employees often expect to bring their own devices. Think about the benefits that your employees will bring, but not before you sort out your security posture, MDM, and other issues that could be stoked by an employee using a personal device for work.

Related reading

- BMC Business of IT Blog
- BMC Service Management Blog
- Best Practices for Organizational Change Management
- 5G for Companies: Hype, Reality & Potential
- IT Best Practices: The Best Introduction