BYOD AND SMALL BUSINESSES:
ENSURING SAFE AND SECURE MOBILITY

SAFARI solutions
STRATEGIC TECHNOLOGY PARTNER

7 Ridgedale Avenue
Cedar Knolls, NJ 07927
201.934.7400

www.safari-solutions.com

Today's workplace looks significantly different than it did a decade ago. The traditional 9-to-5 has evolved into a more flexible approach, with businesses and employees alike embracing remote and hybrid work models that offer the freedom to work outside the office. **An estimated 32.6 million Americans will work remotely by 2025, which equates to around 22% of the workforce.[1]**

The advancement of technology, particularly cloud-based applications and high-speed internet, has made remote work more accessible. These tools help employees stay connected, collaborate, and access the work resources they need to stay productive from virtually anywhere. One of the most effective ways to support flexible work models is to implement a Bring Your Own Device (BYOD) policy.

BYOD policies can vary depending on industry and business size, but they all share the same goal: to allow employees to use personal devices – including smartphones, laptops, or tablets – for work. By implementing BYOD, you're allowing employees to use their own devices to access company resources and applications from anywhere, facilitating employee mobility and introducing many other business advantages.

While BYOD isn't a new concept, it's received much attention over the past few years. **A reported 85% of businesses implemented BYOD policies in response to the COVID-19 pandemic,[2] and the global BYOD market is projected to surpass $587 billion by 2030.[3]**

In this white paper, we'll explore the benefits and challenges of introducing BYOD to your workforce, best practices for developing a successful BYOD policy, and how you can start using BYOD with expert guidance today.

WHY SHOULD YOU SUPPORT BYOD?

When implemented correctly, a BYOD policy offers many benefits to businesses and employees alike. Some of the biggest advantages of embracing BYOD in the workplace include:

Employee Mobility

BYOD empowers your employees to work anywhere. Your road warriors can stay connected on the go, whether attending a conference, meeting with clients, or commuting. Improving mobility is also essential for supporting remote workers since BYOD enables your teams to respond to work-related questions or complete tasks quickly outside of the office. Regardless of your employees' physical locations, they can provide customer service, participate in virtual meetings, collaborate with coworkers, and much more using their own devices.

Improved Productivity

According to 53% of businesses, mobility has improved employee productivity.[4] One study even found that **BYOD helps employees work an extra two hours daily.[5]** While providing your teams with the ability to work anywhere is valuable, another reason BYOD enhances productivity is device familiarity. Employees are more comfortable using personal devices, resulting in higher efficiency and reduced learning curves. And because workers can customize their devices to suit their preferences and work habits, they can get more done in a comfortable, more effective work environment.

Cost Savings

Outfitting your workforce with equipment like desktop computers and desk phones is expensive. **By switching to BYOD, businesses can save up to 11%.[6]** Allowing employees to use their devices for work means you don't need to purchase and maintain specialized devices, and on-site IT infrastructure is no longer required. Additionally, employees typically cover the costs of their data plans.

Easier Onboarding

When you allow staff to use their own devices for work, they're already familiar with how to use them. Onboarding new

employees takes less time since you don't need to train them on using BYOD devices, and the resources needed for training are reduced.

Better Work-Life Balance

Improving work-life balance has become a primary focus for many business leaders since **77% of workers say they've experienced burnout at their current job.**[7] BYOD fosters a flexible work environment, allowing your employees to easily switch between personal and professional tasks. This flexibility improves work-life balance, increasing job satisfaction and reducing employee stress levels.

WHAT SECURITY RISKS DOES BYOD INTRODUCE?

While BYOD offers plenty of benefits for small businesses, it has its share of disadvantages. A recent survey found that **43% of employees have been the target of a work-related cyber attack on their personal devices.**[8] And because **employees use 2.5 devices for work on average,**[9] monitoring and managing every network-connected device can be overwhelming for IT teams.

Some security risks associated with BYOD include:

Malware

Personal devices typically don't have the same level of protection as company-owned devices, leaving them vulnerable to malware and other cyber security threats that could compromise your company's network.

Data Breaches

BYOD can expose your business to a higher risk of data breaches if your workers' personal devices aren't properly secured. **86% of IT managers say attacks targeting mobile devices are becoming more frequent,**[10] so strong encryption and security measures are essential.

Unsecured Networks

Many remote or on-the-go employees connect to public Wi-Fi networks or unsecured networks. These networks are vulnerable to issues like eavesdropping and man-in-the-

middle attacks, potentially exposing your network and sensitive data to attackers.

Lost or Stolen Devices

Lost or stolen personal devices are a top concern for 55% of organizations.[11] If someone accesses a personal device connected to your network, they can potentially steal corporate information or infect your network via your authorized employee's accounts.

Shadow IT

Employees using personal devices may use unauthorized apps or services when completing work-related tasks, which can potentially bypass your company's security controls and expose your business to additional risks.

Device Management

Without proper device management tools, enforcing security policies, tracking devices, and ensuring your employee devices are updated can be a challenge. Proper device management is also necessary for keeping track of the applications and systems your employees can access from their devices. If an employee leaves your company and their access isn't revoked, your network could be at risk of tampering or data theft.

BEST PRACTICES FOR A SUCCESSFUL BYOD POLICY

Whether your business supports remote workers or not, many employees use their mobile devices to check work emails, access company resources, or communicate with coworkers and clients when outside of the office. This unregulated usage can present major security risks, but introducing a formal BYOD policy can help you establish a framework for keeping personal devices – and your sensitive data – secure.

Clearly Define Acceptable Use

Set a baseline reference for any questions your employees may have about device usage by creating an acceptable use policy. This policy should outline the work-related tasks your employees can perform, what they can access, and what

their responsibilities are when using their personal devices for work. Make sure to address issues such as data privacy, inappropriate content, and application usage, and limit which devices your employees can use when working.

Use Mobile Device Management

Around **80% of all personal devices in a company are unmanaged,**[12] which likely contributes to the rise in cyber attacks targeting remote workers. But because managing dozens, or potentially hundreds, of personal devices connected to your network can be time-consuming, mobile device management (MDM) is a must. MDM solutions streamline BYOD device management, making it easier for your IT team to enforce security policies and monitor devices company-wide or remotely wipe data if a device is stolen or misplaced.

Implement Strong Security Measures

Securing BYOD devices is crucial to protecting your business's sensitive data and ensuring employee privacy. Access and authentication tools, such as multi-factor authentication (MFA), can help ensure that only authorized staff can access company resources from their devices. You can also up the security of your employees' personal devices by requiring device encryption, which makes corporate data unreadable to any cyber criminals that might intercept it.

Educate Employees on BYOD Security

Most data breaches (74%) involve the human element.[13] By educating your employees on cyber security and BYOD best practices, you can help them identify and avoid potential risks when using their devices for work. Conduct regular security training on topics like proper password hygiene, how to recognize phishing attempts, and the safe use of public Wi-Fi networks.

Focus on Security Awareness

Creating a culture of security can help your employees understand and prioritize data protection when working on their personal devices. Foster a security-conscious culture by recognizing staff who demonstrate good security practices and comply with the BYOD policy. Make sure to establish clear channels for reporting to ensure your teams feel comfortable

reporting any security incidents or device-related risks without fear of repercussions.

EMBRACE BYOD THE RIGHT WAY WITH EXPERT GUIDANCE

BYOD can be a game-changer for small businesses, unlocking a world of opportunities and efficiencies. By embracing BYOD, you can offer flexible work opportunities, cut IT costs, and gain a competitive advantage. Implementing a well-defined BYOD policy is an often-overlooked necessity to combating the challenges associated with personal devices.

Partnering with an experienced IT advisor and investing in mobile device management solutions can help your business get the most value from BYOD. If you're ready to leverage the benefits of BYOD, contact our team today. Our experts can provide the guidance you need to develop a BYOD policy that meets your unique business needs and helps you confidently embrace the future of work.

SAFARI solutions
STRATEGIC TECHNOLOGY PARTNER

7 Ridgedale Avenue, Cedar Knolls, NJ 07927
201.934.7400
www.safari-solutions.com

SOURCES

1. https://www.forbes.com/advisor/business/remote-work-statistics
2. https://financesonline.com/byod-statistics
3. https://www.globenewswire.com/en/news-release/2022/09/27/2523496/0/en/BYOD-Market-Projected-to-Reach-at-a-USD-587-3-Billion-by-2030-With-Healthy-CAGR-of-16-20-Report-by-Market-Research-Future-MRFR.html
4. https://www.securitymagazine.com/articles/96102-find-the-balance-between-security-and-privacy-in-a-byod-world
5. https://blog.lastpass.com/2022/01/how-to-manage-the-risks-of-byod-in-a-work-from-anywhere-world
6. https://techjury.net/blog/byod-stats
7. https://www.zippia.com/advice/work-life-balance-statistics
8. https://www.prnewswire.com/news-releases/slashnexts-2023-mobile-byod-security-report-reveals-71-of-employees-have-sensitive-work-information-on-their-personal-devices-43-were-the-target-of-phishing-attacks-301785360.html
9. https://www.digitalinformationworld.com/2021/08/more-professionals-prefer-apple-for-work-devices-than-dell-microsoft-combined.html
10. https://www.nist.gov/news-events/news/2022/12/spotlight-cybersecurity-and-privacy-byod-bring-your-own-device
11. https://marketsplash.com/byod-statistics
12. https://99firms.com/blog/mobile-device-management-statistics
13. https://www.verizon.com/business/resources/reports/dbir

7 Ridgedale Avenue, Cedar Knolls, NJ 07927
201.934.7400
www.safari-solutions.com

7 Ridgedale Avenue
Cedar Knolls, NJ 07927
201.934.7400
www.safari-solutions.com

SAFARI solutions
STRATEGIC TECHNOLOGY PARTNER