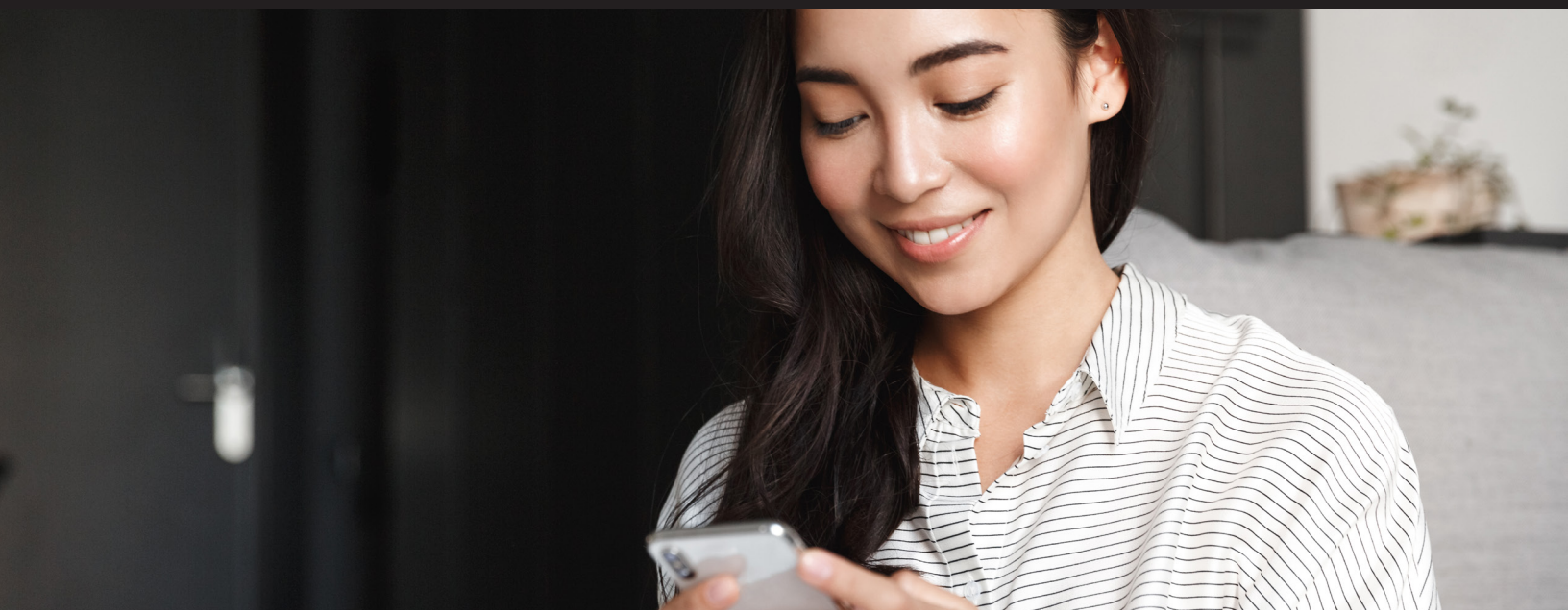
EBOOK

vMOX



WHAT TO KNOW BEFORE YOU GO BYOD

Considerations for switching to a Bring-Your-Own-Device (BYOD) strategy for your mobile environment

Implementing a BYOD (Bring Your Own Device) policy can seem like a simple solution.

While companies that adopt BYOD can potentially benefit from reduced hardware and software costs, it can bring significant security and productivity concerns and place additional responsibilities on IT departments, which must set up the devices as well as provide ongoing support and monitoring.

At the end of the day, adopting a BYOD policy can be an expensive mistake and companies need to think through all the implications. It might seem like trivial decision in the moment, but it can have lasting impact on time and money. And it doesn't stop and start with IT — running a successful BYOD program touches every department from legal to HR, finance, business units, even maybe customers.

Learn what BYOD risks you should be aware of and the right questions to ask yourself if your company is considering moving from a corporate-liable to an individual-liable mobile environment.

TABLE OF CONTENTS

PART 1

12 Common Challenges of BYOD

PART 2

Controlling Costs

- Management Costs
- Hidden Costs

PART 3

Shadow IT

PART 4

Data Protection and Security

PART 5

End User Support

- Keeping Your Phone Numbers

PART 6

Employee Experience and Rights

PART 1

12 Common Challenges of BYOD

While allowing employees to buy and use personal devices for work-related activities seems like a win-win, there are a number of potential risks and obstacles that companies will need to overcome. Ultimately, teams that run a BYOD network should recognize and take care of these issues, or you might find yourself betting more than what you bargained for — and not in a good way.

1. INCREASED SUPPORT COSTS FROM MULTIPLE DEVICE TYPES AND OPERATING SYSTEMS
2. PROTECTING CORPORATE DATA AND INFRASTRUCTURE
3. GLOBAL DATA PROTECTION AND LEGISLATION
4. MEETING LEGAL AND CONTRACTUAL OBLIGATIONS TO EMPLOYEES AND CLIENTS
5. EMPLOYEE WORK-LIFE BALANCE AND RIGHT TO DISCONNECT
6. SHADOW IT COSTS
7. PRODUCTIVITY IMPACT FROM USERS HAVING THE WRONG DEVICES AND/OR AIRTIME PLANS
8. MANAGEMENT COSTS OF BYOD PROGRAM
9. LOSS OF KEY PHONE NUMBERS WHEN EMPLOYEES LEAVE
10. IMPACT TO EMPLOYEE BENEFITS AS NEGOTIATED WITH UNIONS/WORKERS COUNCILS
11. REPUTATIONAL AND FINANCIAL IMPACT OF DATA BREACHES
12. EMPLOYEE ABILITY TO AFFORD AND MAINTAIN DEVICES

PART 2

Controlling Costs

MANAGEMENT COSTS

At face value many companies will consider a BYOD program as a "set and forget" strategy which will reduce management overhead and bring cost savings. However, BYOD programs are often complex and need to balance the needs of the business, employees, and clients, with regulatory and security requirements. There are many costs to the business, in both time and money, associated with the management of a BYOD program.

THE IMPACT OF MANAGING BYOD

- Time spent on the design, planning, and development of the BYOD program and the associated policies often requiring cross-departmental expertise and paid external consultants.
- Most BYOD programs involve an employee stipend typically made monthly to all eligible employees. There is cost involved with managing these monthly payments to a large group of employees as well as investment needed in tools and systems to track, authorize and manage the stipends.
- Launch and rollout costs related to the BYOD program including employees education/awareness, HR policy updates, IT policy updates, updating of IT and asset tracking systems, updating of Active Directories and contact information.
- Cost of managing employee disputes or resistance to the move to BYOD, especially in locations with strong labor unions or workers' councils.
- Risk and cost associated with recovering company-owned assets as you move from corporate-liable to individual-liable devices ensuring all company data is recovered and securely disposed of.

> **The results show that for most organizations, adopting BYOD results in only modest savings in the total cost of mobile enablement for employees. More significantly, businesses adopting blanket BYOD policies reported obtaining the least business value from mobile.**

Oxford Economics / Samsung, *Maximizing Mobile Value Report*

Employees use an average of **2.5 devices for work**, including computers, smartphones, tablets, and e-readers.

Zippia.com

HIDDEN COSTS

Most of your employees will not be well educated on mobile plans, usage patterns, and coverage. Employees will typically choose their plan and device based entirely on cost and personal preference, which may not meet the needs of their role or the business.

DID YOU KNOW?

- **Employees who select a mobile plan with a low allowance for voice or data may find themselves without connectivity or with speed throttling which will impact their ability to do their job or be contactable by the company or your clients. Think about the cost impact to the business if an employee cannot be reached because they wanted to save themselves a few dollars on their mobile plan.**

- **Employees may select smaller carriers which do not offer the coverage needed to allow them to be contactable or do their job while traveling.**

- **While BYOD may remove some direct costs, the need for your company to support multiple device types, and employees selecting inappropriate devices or plans will have an impact of productivity. Any BYOD program should be assessed for the risk of increased indirect costs through reduced productivity.**

- **Inflation is a hot topic around the world and with a global supply shortage of semi-conductors the price of mobile devices continues to increase. Companies need to ensure their BYOD program, including any stipend is regularly reviewed and adjusted.**

PART 3

Shadow IT

The move to BYOD offers the opportunity to reduce obvious costs around the purchasing of hardware and airtime, however, often hidden costs creep up overtime via shadow IT. Here are four areas you should review carefully:

DEVICE PURCHASES

Purchasing of accessories such as phone cases, chargers, wireless headsets etc. via company expense processes and approved by managers. Just because the company does not have a formal mobility acquisition program does not mean employees will not try and claim for accessories through other means.

PLAN SELECTION

Corporate mobility programs strike a balance between cost and productivity, making sure users have the right plans to do their jobs. Many employees may opt for personal plans that are low costs but do not meet their needs. Should a user have high unexpected overage by exceeding their device plan will you allow them to reclaim the overage costs?

OVERSEAS TRAVEL

How will you cover roaming and International dialing charges? Many personal phone plans will not have the right travel plans meaning users could incur high charges when traveling for work. Will you allow them to claim for these charges? Or will users opt to not use their mobile device to save their personal costs at the expense of productivity while traveling?

DEVICE REPLACEMENT

If an employee loses their device or has it stolen is the expectation that they fund a replacement device? What if the employee cannot (or will not) afford the replacement? What if the loss happens while on business travel, will the company cover the cost?

PART 4

Data Protection and Privacy

A key challenge when considering any BYOD program is meeting the companies (and your clients) data protection and security requirements. Companies should consider the cost of a data breach (regulatory fines and reputational) and the impact of losing sensitive IP versus the cost savings from a BYOD program. Below are key questions to ask yourself:

- **How will you protect corporate data and infrastructure across multiple different devices type, operating systems, and connections?**
- **Will your users have hardware which supports the latest security updates ensuring your company infrastructure is protected?**
- **Corporate data will inevitably contain Personally Identifiable Information (PII) which needs to be protected to meet strict data protection requirements which vary by country and region. Do you have the right tools and policies, and can you enforce them to stay compliant?**

  The European Unions General Data Protection Regulations (GDPR) impose fines of up to €4M or up to 4% of global turnover if you are found guilty of a data breach.

- **How will you distribute, manage, and enforce corporate security and mobile polices across your devices?**
- **Have you reviewed your client contracts to ensure a BYO program is in line with contractual commitments? Your clients will want to know you are protecting their sensitive data and that your corporate infrastructure and tools meets their high standards.**
- **Your employees may also be concerned that they are sharing their personal information with you when using a personal device for business which may impact how they use (or not use) their device. How will you address these concerns and prevent impact to productivity?**

71%

of employees access more company data, more frequently, from home now than they did pre-pandemic – the most common types of data being customer and operational data (43% each) and financial and HR records (23% each).

HP Wolf Security, *Blurred Lines and Blindspots Report*

97%

of employees' devices contained privacy issues

75%

of employees' devices lacked adequate data encryption

PART 5

End User Support

In a corporate-owned and managed mobility program the company will define the devices and operating systems which the employees can use. This allows the company to maintain only a small number of device types which are typically up to date meeting the latest security requirements. **A move to BYOD means that your IT support and helpdesk will now have to service a much wider range of device types and operating systems. You should consider:**

- How do I ensure our IT support and helpdesk can be successful in supporting our user base across an ever growing list of devices and operating systems? What is the hidden extra cost of having to train the IT team and develop processes to support the users?

- How do I support the onboarding and offboarding of employees using their personal devices which we may not have direct access to?

- Will we allow users with older devices which do not support the latest software updates to access corporate data and infrastructure? What is the balance between employee productivity and security?

- If an employee has an issue with the carrier (such as disconnected/suspended device) how will the IT support team manage this when the company does not own the phone line or plan? Do not assume your employees will be able to solve this independently. There will also be an impact to productivity if your employees are on the phone with carriers solving problems rather than doing their day job.

SAY GOODBYE TO YOUR PHONE NUMBER

If your BYOD program includes Bring Your Own Line/SIM then it's important to remember that the company no longer has ownership of the phone number attached to that device. This is particularly important for employees who represent your company with clients, suppliers and other external parties.

> *For example, a member of your Sales or Client Account team leaves the company and takes their phone number with them to their new company. This could potentially mean that your clients call into a competitor in the future. Yikes!*

There is also the risk that a phone number associated to one of your critical business processes walks out of the door. What happens if a Support Engineer leaves the company and take the phone number used to raise alerts for critical system outages with them and the teams involved don't update their processes?

80%

of employees say they'd prefer to use separate devices for work and personal activities.

Beyond Identity, *BYOD: Exploring the Evolution of Work Device Practices in a New Remote-Forward Era [Survey]*

PART 6

Employee Experience and Rights

A move to BYOD can have a positive impact on your employee experience empowering them to use the devices they are most familiar with and allowing choice. **However, not every employee will view BYOD as positive and there are many areas relating to employee experience and rights that companies should examine closely:**

- What is the impact on work life balance of employees who now have their work emails and communication tools on their personal devices? How will you help your employees avoid burn out because they are constantly reachable?

  Countries such as France, Italy, Spain, Portugal and Belgium have implemented legislation giving employees the "right to disconnect" creating a clear separation of work and personal. A move to a BYOD program needs to be compliant with current and future legislation around employee rights.

- Was being provided with a corporate device a 'perk' (contractual or otherwise) offered to new employees joining the business? Be careful that you are not breaching employment contracts or impacting your staff acquisition and retention potential.

- Large organizations need to assess any concerns raised by employee labor unions or workers' councils which include the removal of an employee benefit or blurring the lines between personal and work life.

CONCLUSION

Picking the Right Path

Fueled by hybrid working environments and new users entering the workforce, most agree that BYOD will continue to exist in some form. However, it brings with it its own unique hype and headaches. Companies need to find ways to address the related challenges and risks, especially as it relates to legal, privacy and security concerns.

It can be difficult for teams to decide what program and policy variation makes the most sense for their company, whether Bring-Your-Own-Device (BYOD), Choose-Your-Own-Device (CYOD), Company Owned/Personally Enabled (COPE) or Company Owned/Business Only (COBO). That's why it can pay dividends to work with an expert like vMOX to better understand the differences, advantages and drawbacks of each mobile strategy.

At the end of the day, whatever you choose, make sure you consider the long-term consequences of your decision and strike the proper balance between what employees want and what IT and security require. Due to the critical nature of mobile devices and their growing complexity, enterprise mobility will truly never be hands off. Your end goal should match your level of investment in applications, support and devices. If not, the risk to your business and bottom line is substantial.

> **BYOD has not been a free lunch.**
>
> It's important to remember here that many shops originally took up BYOD (or, as was often the case, simply allowed it to take over) because it seemed like it would eventually turn into a huge cost-saver.
>
> But in practice, BYOD has not been a free lunch at all. Significant legwork, time and money can go into a secure and scalable implementation, as Joe Foran pointed out in a Community overview of a BYOD deployment that required remote wipe, app push, VPN auto-configuration when out of the office, various usage reports and separate policies for each SSID, among other features.
>
> Spiceworks, "Is BYOD a Thing of the Past"

Need help with your mobile strategy?

Contact a vMOX enterprise mobility specialist today to understand BYOD better and the respective pros and cons.

vMOX.com
2 SEAVIEW BLVD, SUITE #104
PORT WASHINGTON, NY 11050
646. 795. 2000
INFO@VMOX.COM

vMOX