



WHITEPAPER

BYOD vs COPE

Selecting the Right Mobile Strategy

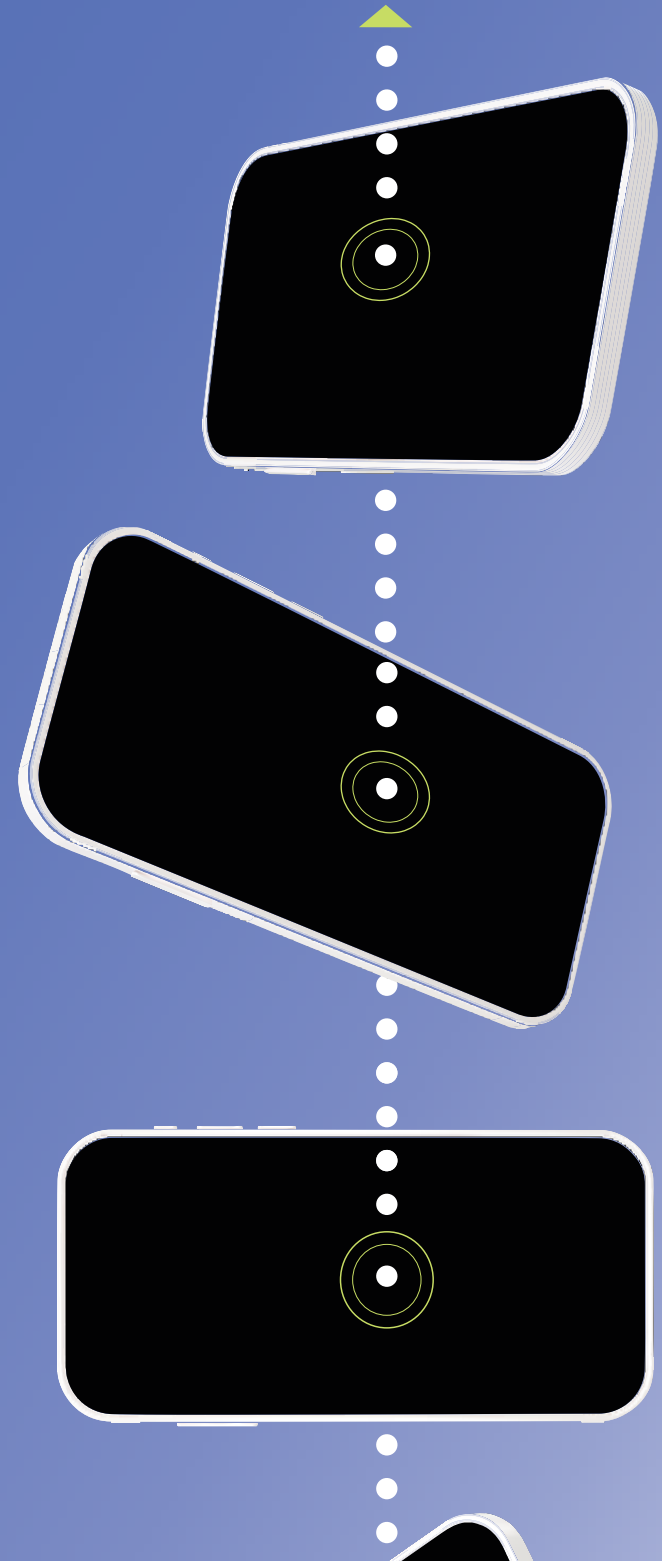


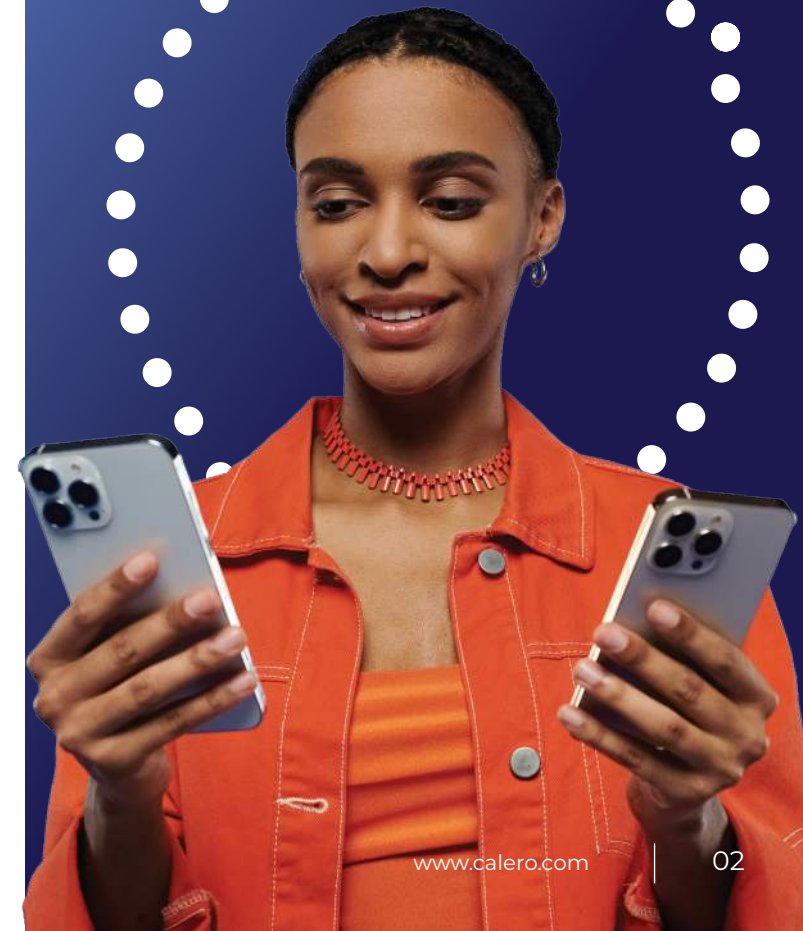


Table of Contents

- 01 Introduction 02
- 02 BYOD Pros & Cons 03
- 03 COPE Pros & Cons 04
- 04 The Market Perspective 05
- 05 Why COPE is the Better Option 06
- 06 The Cost Outweigh the Savings 07

01 Introduction

Businesses face an array of choices when implementing mobile strategies, but which one is right for your organization? Two prevalent approaches are Bring Your Own Device (BYOD) and Corporate-Owned, Personally Enabled (COPE). As companies like yours grapple with the need for security, compliance, and employee satisfaction, selecting the appropriate mobile strategy is crucial. This whitepaper aims to help you understand the pros and cons of each approach so that you can select a strategy that is right for your organization.



02 BYOD Pros & Cons

Pros

1. **Upfront Cost Savings:** BYOD can reduce upfront costs for businesses, as employees use their personal devices for work-related activities.
2. **Employee Satisfaction:** Allowing employees to use familiar devices can lead to increased satisfaction and productivity.
3. **Flexibility:** BYOD offers greater flexibility for employees to work from anywhere, using devices they are comfortable with.

Cons

1. **Security Risks:** Personal devices often don't have the same level of security as company-provided devices, leading to vulnerabilities. A Ponemon Institute study found that **67% of companies** reported data breaches due to employee-owned devices.
2. **Compliance Issues:** Certain industries have strict security certifications and compliance requirements that may not be compatible with BYOD. For example, the healthcare sector, governed by HIPAA, often restricts the use of personal devices. In 2022, the SEC issued \$1.8B in fines for using personal devices to discuss regulated work matters.
3. **Management Challenges:** IT teams may find it challenging to manage and support a wide variety of personal devices, often encountering slower troubleshooting resolution, device compatibility issues with corporate applications, and irregular update cadences due to the lack of control over personal devices. According to a report by Gartner, **38% of IT professionals** identified device diversity as a significant challenge in managing BYOD.
4. **Ongoing Costs:** While initially BYOD programs may have a lower cost of entry, recurring costs and costs from potential security breaches can quickly add up. Monthly stipends, UEM licenses, and regular auditing costs often rival and outpace the cost of a right-sized COPE program.

**67%**

of companies reported data breaches due to employee-owned devices

**38%**

of IT professionals identified device diversity as a significant challenge in managing BYOD

03 COPE Pros & Cons

Pros

1. **Enhanced Security:** COPE allows organizations to maintain control over the devices, enabling better implementation of security measures. A study by Verizon found that companies using COPE experienced **45% fewer security incidents** compared to those with BYOD policies.
2. **Compliance and Oversight:** With COPE, companies can ensure that devices meet industry-specific compliance requirements. **80% of organizations** reported improved compliance with COPE, as per a report by Frost & Sullivan.
3. **Streamlined Support:** Standardizing devices can simplify IT management and support. This can result in a **30% reduction** in support costs, according to a study by Forrester.

Cons

1. **Higher Initial Costs:** Providing devices to employees can be a significant upfront investment. However, the long-term benefits, such as reduced security incidents, often outweigh these initial costs.
2. **Potential Employee Resistance:** Some employees may prefer their personal devices over company-issued ones.
3. **Limited Flexibility:** COPE may offer less flexibility in terms of device choice and usage. However, it still allows for a degree of personal use, balancing security with employee satisfaction.

**45%**

fewer security incidents
compared to those with
BYOD policies

**80%**

of organizations
reported improved
compliance with COPE

**30%**

reduction in
support costs

04 The Market Perspective

Small to lower mid-sized organizations often gravitate towards BYOD due to cost considerations. However, these companies also face unique challenges, such as smaller IT teams and limited resources, which can exacerbate the impact of security breaches. The potential loss from data breaches can be particularly devastating for smaller organizations, making security a critical concern. A report by the National Cyber Security Alliance indicated that **60% of small to mid-sized businesses that experience a data breach close their doors within six months.**

For certain industries, security certifications and compliance standards explicitly prohibit the use of personal devices for work-related activities. In such cases, COPE not only becomes a viable option but a necessary one. By equipping employees with company-owned devices, businesses can enforce security policies more effectively, reducing the risk of data breaches and ensuring compliance with industry standards.



60%

of small to mid-sized businesses that experience a data breach close their doors within **six months**



05 Why COPE is the Better Option

- 1. Security and Compliance:** COPE provides a more secure and compliant framework for managing mobile devices. Organizations can enforce strict security protocols, ensure devices are up-to-date with the latest software, and maintain control over data access and usage.
- 2. Risk Mitigation:** With COPE, the risk of security breaches is significantly reduced. Organizations can quickly respond to security incidents, take action more readily to remotely wipe compromised or stolen devices, and maintain comprehensive oversight of the mobile ecosystem. According to IBM Security, the average total cost of a data breach to a company in 2023 was **\$4.45 million**, underscoring the importance of robust security measures.
- 3. Consistency and Efficiency:** COPE allows for standardized devices and configurations, simplifying IT support and management. This consistency leads to greater efficiency in managing the organization's mobile strategy, with some companies reporting a **25% increase** in IT efficiency, as noted by TechTarget.
- 4. Boost Employee Loyalty:** Employee loyalty and a sense of appreciation are crucial in today's work culture, where maintaining work-life balance is a priority. Many employees view mobile devices like laptops—tools that should be provided and maintained by the company. By supplying corporate-owned devices, companies demonstrate they value their employees, which strengthens the connection between them. Employees are also more likely to respond to work-related tasks, like after-hours calls, when using company devices, as it reinforces the separation between work and personal life. This leads to higher satisfaction, productivity, and loyalty, ultimately reducing turnover and associated costs.



**\$4.45
million**

average total cost
of a data breach

06 The Costs Outweigh the Savings

While BYOD offers certain advantages, such as cost savings and flexibility, it also presents significant security risks and compliance challenges, particularly for mid-sized organizations. On the other hand, COPE provides a more secure, compliant, and manageable solution, making it a better option for companies prioritizing data protection, regulatory compliance, and effective issue resolution. By adopting a COPE strategy, businesses can equip their employees with devices that meet the highest security standards, mitigate risks, and ensure smooth, efficient operations.

No Matter the Strategy, We Can Help You Manage It

How Calero can help

Chat with our team of experts to learn how to implement these strategies through a single platform that gives you comprehensive visibility to your entire mobility estate.

Book a Demo →

