

# The ultimate guide to mobile device security in the workplace

April 2024

## **In this guide:**

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

Organizations must lock down all endpoints that access business data and put measures in place to ensure the data doesn't fall into the wrong hands. When it comes to mobile devices, however, there are unique security challenges for organizations to mitigate. This guide covers the ins and outs of mobile device usage in the workplace, with an emphasis on mobile device security policies, including the steps for implementation and best practices.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

# The ultimate guide to mobile device security in the workplace

*JOHN POWERS, SENIOR SITE EDITOR*

Organizations must lock down all endpoints that access business data -- including mobile devices -- and put measures in place to ensure the data doesn't fall into the wrong hands.

This general goal applies to all types of enterprise security -- network, PC, laptop and application -- but [mobile security](#) offers unique challenges for organizations to grapple with. For example, device loss and theft are far more of a concern for mobile devices than other types of endpoints. Mobile devices can also operate without traditional Wi-Fi or Ethernet connections and in any location that has a decent wireless signal.

Organizations should turn to mobile-specific tools, products and policies that enable workers to be productive on their mobile devices while ensuring the security of the device and its data.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

## WHAT ROLE DO MOBILE DEVICES HAVE IN BUSINESS?

The modern workforce is more mobile than ever due to remote work and the proliferation of laptops, hybrid devices, tablets, smartphones and other mobile devices. These devices enable workers to be productive from a variety of locations, such as at home, at an airport or in transit.

Working remotely and while on the go is a well-established concept in organizations of all sizes. Mobile devices such as smartphones and tablets play a major part in enabling workers to do this. For example, many workers carry around smartphones with access to work email and business applications everywhere they go. The most common smartphone operating systems are Apple's iOS and Google's Android.

But mobile devices can enable more than just on-the-go work. Businesses can use tablets and smartphones for point-of-sale (POS) terminals, record-keeping, data logging and custom form submissions. Mobile devices can even serve as full workstations with the proper auxiliary device support.

When it comes to securing mobile devices, personal devices have far more security concerns and complications compared to single-use kiosk approaches. The attack surfaces for kiosk devices are far smaller than those of employees' personal smartphones due to the latter's wider array of applications and freedom to browse the

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

Internet. As such, mobile security policies should focus predominantly on securing these types of devices.

Another common type of mobile device in the enterprise is a corporate-owned mobile device. Some organizations have the capital to purchase mobile devices for certain employees. Securing these devices is relatively straightforward -- especially compared to personally owned devices accessing corporate data -- and IT admins can apply strict security controls to these devices.

## WHAT ARE THE BENEFITS OF MOBILE DEVICES IN THE WORKPLACE?

The simplest benefit of mobile devices is the flexibility they provide for employees to be productive from various locations. In general, mobile devices enhance connectivity, communications, collaboration and networking due to their portability and access to cellular networks.

Users can access business email, [unified communications](#) (UC) mobile apps such as Microsoft Teams and Slack, custom business applications and other apps or services that enable productivity. This benefits knowledge workers and executives especially, as they might need to respond to critical emails or approve certain workflows while on the go or from remote locations.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

[Kiosk devices that serve a single purpose](#) are also a key part of numerous types of organizations. Tablets, smartphones and other mobile devices can assist with POS needs, customer or client registration, digital waiver signage, data input and much more.

## WHY DO BUSINESSES NEED A MOBILE SECURITY POLICY?

It can be easy to overlook mobile devices in a security policy; after all, they are rarely a user's main workstation. This is especially the case when it comes to users connecting personal devices to work applications and services, such as an organization's email server or UC platform.

However, organizations that permit any access to sensitive data on mobile devices must have a mobile security policy. It can be helpful to think of it as the "weakest link in the chain" principle: Company data is only as secure as the least secure device accessing it.

Neglecting mobile device and data security leaves more openings for data breaches in an [organization's overall security architecture and policy](#). Therefore, a security architecture that includes mobile-specific policies such as acceptable use guidelines for mobile device users, [mobile security best practices](#) and security platforms or services is essential for organizations that rely on mobile devices.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

## COMPARING CORPORATE-OWNED VS. BYOD FOR MOBILE DEVICES

One of the first steps in establishing a mobile policy is determining whether users' devices will be corporate-owned or user-owned. Each approach has its strengths and weaknesses that organizations must factor in. Generally, corporate-owned devices provide more certainty and simplicity from a management and security policy perspective, but [BYOD](#) enables more user choice and flexibility.

### HOW TO CHOOSE BETWEEN CORPORATE-OWNED VS. BYOD MOBILE DEVICE OWNERSHIP

Issuing corporate-owned mobile devices to users is the more straightforward and expensive option for organizations. The biggest benefits of a corporate-owned approach are IT's security and management capabilities. Organizations can maintain as restrictive a device policy as they want without worrying about invading users' privacy on their personal devices. Users are more likely to be understanding regarding a strict policy if they didn't purchase the device themselves. The process of [deploying app and OS updates](#) is also easier with full device control because users typically prefer to update their personal devices on their schedule.

A company-owned device program isn't perfect for every situation, especially considering the price tags that flagship smartphone models come with. Organizations can negotiate deals with smartphone manufacturers -- but even with discounts, the cost of all that hardware can add up quickly. Larger organizations might not have this

## **In this guide:**

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

issue when it comes to resources for mobile device purchases, but small or tight-budgeting organizations might not want to incur this cost.

Additionally, organizations must decide if corporate-issued devices are allowed to serve as users' personal devices as well. Users might appreciate the lenience of having a corporate-owned, personally enabled ([COPE](#)) device for the flexibility. However, plenty of users have their own smartphone or other mobile devices before joining an organization, so this might not be necessary. The corporate-owned, business-only (COBO) approach grants organizations a very high level of control over the device, its security and privacy policies, its update schedule and much more.



## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

# BYOD vs. CYOD vs. COPE vs. COBO

BYOD gives employees freedom of choice for mobile devices at work. But that isn't always the best option.

	BYOD	CYOD	COPE	COBO
PROS	<ul style="list-style-type: none"><li>■ Employees have control over device choice.</li><li>■ Employees have one phone for work and personal tasks.</li><li>■ A BYOD policy improves data protection and privacy.</li></ul>	<ul style="list-style-type: none"><li>■ Employees have a degree of choice among devices.</li><li>■ IT sets the scope of device variety, for example only working with Apple iOS products.</li></ul>	<ul style="list-style-type: none"><li>■ Employers control the device range they support, including only one device option.</li><li>■ Employees receive the benefits of a mobile device without all or some of the associated costs.</li></ul>	<ul style="list-style-type: none"><li>■ IT controls the device and applications on it for maximum security and ease of management.</li><li>■ Workforce is mobile.</li></ul>
CONS	<ul style="list-style-type: none"><li>■ IT must secure and manage an unlimited range of devices and OSes.</li><li>■ Cost-sharing contentions.</li></ul>	<ul style="list-style-type: none"><li>■ Employees might already have a personal mobile device.</li><li>■ Organizations are responsible for devices hosting personal information and apps.</li></ul>	<ul style="list-style-type: none"><li>■ Employees expect freedom to choose, upgrade and share mobile devices—restrictions are unwelcome.</li><li>■ Cost and management tradeoffs of a mobile device plan.</li></ul>	<ul style="list-style-type: none"><li>■ Employees have limited flexibility and control.</li><li>■ The company is responsible for devices' cost and management.</li></ul>
USE CASES	<ul style="list-style-type: none"><li>■ In organizations where employees already install work email and other apps on personal devices.</li></ul>	<ul style="list-style-type: none"><li>■ In organizations where employees do not already have personal mobile devices or IT must streamline mobile device management.</li></ul>	<ul style="list-style-type: none"><li>■ In organizations with security and compliance restrictions that still want to enable a mobile, flexible workforce.</li></ul>	<ul style="list-style-type: none"><li>■ Jobs that require specific applications/mobile device capabilities away from a desk. Devices can be shared among employees.</li></ul>

©2021 TECHTARGET. ALL RIGHTS RESERVED. 

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

Many organizations might [see BYOD as the most straightforward device deployment option](#). The organization doesn't have to purchase new mobile devices for each new hire, and users can have a single device for both work and personal matters. This eliminates the poor user experience and employee frustration caused by carrying around multiple mobile devices. Though [the BYOD approach is straightforward](#), it can prompt more complicated security policies and management compared with [COPE and COBO](#).

For example, users must agree to the organization's terms of device use and mobile policy before they start using their personal devices for business tasks. This could include forced OS or app updates for security, on-device management agents and an [overall decrease in the users' privacy](#). There is also the issue of cost sharing. Some users -- especially those who work with their mobile devices quite a bit -- might incur additional costs, such as data use, device repairs or even device replacement. If organizations can shape a policy to [account for these BYOD factors](#), then BYOD could be an ideal option.

### COMPARING BYOD VS. CORPORATE-OWNED FOR SECURITY

In very general terms, corporate-owned devices provide stronger security for organizations. This is due to the IT administrator's ability to control devices more closely [compared to BYOD deployments](#). A BYOD security policy needs to account for users accepting the level of device control that an organization asks for. As such,

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

organizations are more likely to offer more lenient security policies to ensure user acceptance.

Corporate-owned devices don't have this level of ambiguity when it comes to user acceptance. For example, IT admins can deploy a policy that allows for remote device wipes without worrying about deleting a user's personal device data.

IT should note that a mobile policy's level of security is determined based on the controls IT implements and not the device ownership model. But the path to a strong mobile security policy is simpler for corporate-owned devices.

## WHAT ARE THE RISKS AND CHALLENGES OF MOBILE DEVICE CYBERSECURITY?

The benefits of mobile devices are widespread and can fit within a huge amount of use cases. However, mobile devices bring more attack surfaces and other challenges that IT and end users need to address.

While there is a perception that mobile devices aren't susceptible to security threats, this is categorically not the case. Like any endpoint, hackers can intercept incoming and outgoing traffic from the device, trick users into downloading malware or ransomware and gain unauthorized access to users' data through a compromised network connection.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

Further, [mobile devices face additional threats](#) that typical endpoints do not. Device loss and theft are more common with mobile devices, and social engineering attacks are extremely common with the numerous vectors that mobile devices provide. Phishing attacks that target certain employees' mobile devices can use SMS messaging, email accounts, messages from social media applications or even malicious links in browsers.

There also might be challenges with integrating mobile devices into existing back-end systems, legacy and custom applications, and services tailored to endpoints such as PCs and laptops. Most business technology vendors are aware of the role of mobile devices and provide products and services that accommodate mobile devices, but mobile support isn't universal.

These compatibility issues can morph into larger issues of compliance as well. Highly regulated fields, such as government, finance and healthcare, might have difficulty enabling mobility while abiding by each sector's regulatory laws.

## STEPS TO DEFINE AND IMPLEMENT A MOBILE SECURITY POLICY

Organizations can mitigate the security risks and shortcomings of mobile devices with a specific and effective mobile device policy. This is especially true with the mobile security components of that policy.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

Mobile policies should be detailed, comprehensive and largely customized based on an organization's needs. While it can be helpful to [start a mobility policy from a template](#), organizations have to define certain components, including acceptable device use, device ownership policy, privacy policy and disclosure of what data the organization can view. The policy should also explain what on-device security and management agents will be present and what measures an organization can take to ensure [data security](#). For example, can an organization run a remote device wipe if it is compromised or remotely lock the device if it is at risk?

Additionally, organizations must find the best way to outline this policy and communicate it to end users; a policy is only effective if users understand and adhere to it. Ideally, users should review the documentation during the onboarding process.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

### Top cybersecurity training topics

Here are three crucial topics that should be explored in any security awareness training effort.

- Phishing attacks**  
One of the oldest and still most effective threats, employees must be educated to recognize and handle these security threats appropriately.
- Social engineering attacks**  
Social engineering attacks don't just come in emails, but also from behind a customer service desk, via telephone calls or from the next cubicle. Teach employees to recognize all types.
- Password hygiene**  
A constant battle but a winnable one if you encourage the use of password managers and strong, unique passwords for each site employees visit.

SOURCE: MIKE CHAPPEL; ICONS: MIKIEVYVGETTY IMAGES

©2023 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Organizations should track who needs to review the mobile policy and verify that each user accessing business data with a mobile device has read the necessary documents and completed any security awareness training.

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

## ADDITIONAL MOBILE SECURITY BEST PRACTICES AND MEASURES TO CONSIDER

Mobile devices are more susceptible to theft than laptops and PCs, so ensuring that mobile devices have robust authentication requirements is essential. Organizations can require stronger mobile authentication strategies, such as an eight-character minimum for device passwords instead of numeral-only PINs or even two-factor authentication. The two-factor approach could supplement a passcode with additional measures, such as biometric factors -- usually a fingerprint or iris scan -- a user

location verification or a secondary authentication device, such as an ID card or chip.

Cybercriminals often target mobile devices over public Wi-Fi networks because these networks don't require any authentication. Some hackers set up their own public Wi-Fi networks that imitate free Internet from businesses such as coffee shops or restaurants. Organizations should restrict access to unsecured public Wi-Fi using a management console if possible and, at minimum, explain these dangers in mobile security training and documentation.



## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

These best practices can make up a strong mobile security policy, but IT administrators also need to think about how they can enforce these controls. One common approach to mobile policy enforcement is implementing a mobile device management (MDM) platform. Vendors often bundle these management platforms into larger offerings, such as enterprise mobility management (EMM) and unified endpoint management (UEM).

Most EMM and UEM platforms [include both MDM and mobile application management \(MAM\) capabilities](#). Organizations might also want to consider [mobile threat defense](#) (MTD) platforms, which offer more advanced security management capabilities than MDM or MAM. For example, some MTD platforms offer phishing and spam filters, device health reports, malware scans and behavior analysis.



## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)




[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

# The evolution of endpoint management: MDM, EMM and UEM

	 <b>Mobile device management (MDM)</b>	 <b>Enterprise mobility management (EMM)</b>	 <b>Unified endpoint management (UEM)*</b>
DESCRIPTION	Tools that manage mobile devices, mobile users' data and some basic mobile application controls	Tools that manage everything that MDM does, plus offer more granular control over mobile applications	Tools that manage everything that EMM does, plus offer full desktop management including desktop OSes, apps and data
CHARACTERISTICS	<ul style="list-style-type: none"><li>■ Enforce passcodes</li><li>■ Install applications</li><li>■ Perform remote device wipes</li><li>■ Configure corporate profiles for BYOD, COPE</li></ul>	<ul style="list-style-type: none"><li>■ Enforce multifactor authentication</li><li>■ Manage enterprise file sync and share</li><li>■ Deploy device web browser security settings</li><li>■ Apply conditional access policies</li></ul>	<ul style="list-style-type: none"><li>■ Apply EMM controls to PCs and desktops</li><li>■ Configure and update desktop and mobile apps at the same time</li><li>■ Manage IoT devices and printers</li></ul>
PRODUCTS	<ul style="list-style-type: none"><li>■ VMware AirWatch MDM</li><li>■ Citrix XenMobile</li><li>■ MobileIron MDM</li></ul>	<ul style="list-style-type: none"><li>■ VMware AirWatch EMM</li><li>■ Citrix Endpoint Management</li><li>■ MobileIron EMM</li></ul>	<ul style="list-style-type: none"><li>■ VMware Workspace One</li><li>■ Citrix Workspace</li><li>■ MobileIron UEM</li></ul>

\*UEM PLATFORMS REFLECT CURRENT OFFERINGS, AS VENDORS DISCONTINUE THE OLDER VERSIONS OF THEIR TOOLS

## In this guide:

[What role do mobile devices have in business?](#)

[What are the benefits of mobile devices in the workplace?](#)

[Why do businesses need a mobile security policy?](#)

[Comparing corporate-owned vs. BYOD for mobile devices](#)

[What are the risks and challenges of mobile device cybersecurity?](#)

[Steps to define and implement a mobile security policy](#)

[Additional mobile security best practices and measures to consider](#)

IT administrators must find an MDM platform and other supporting technologies that can meet their device security and management needs. IT administrators should work with executives and perform diligent market research before selecting the ideal product. This could include working with product demos, talking directly to vendors and consulting with independent researchers who evaluate mobile security and management offerings.

*John Powers is the senior site editor for TechTarget's Enterprise Desktop, Virtual Desktop and Mobile Computing sites. He graduated from the Philip Merrill College of Journalism at the University of Maryland.*

---

### CONTINUED READING

- [BYOD security risks and how to prevent them](#)
- [What can organizations do to address BYOD privacy concerns?](#)
- [Mobile device security best practices for businesses](#)