Learn:

- The basics of BYOD and enterprise mobility
- To control how a mobile device interacts with your corporate data
- Ten good reasons you need a BYOD and mobility plan

Brought to you by

Acronis

Gill Borniche
Derick Naef
Ryan Williams
About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the Acronis AnyData Engine and set apart by its image technology, Acronis delivers easy, complete, and safe backups of all files, applications, and OS across any environment — virtual, physical, cloud, and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis’ products have been named best product of the year by Network Computing, TechTarget, and IT Professional and cover a range of features, including migration, cloning, and replication.

Acronis Mobility Solutions

Acronis Access Advanced

Acronis Access Advanced is an easy, complete, and safe access, sync, and share solution, providing IT with complete control over business content to ensure security, maintain compliance, and enable BYOD. Employees use any device to securely access corporate files and share content with other employees, customers, partners, and vendors. Designed to meet the needs of enterprise organizations, Acronis Access Advanced allows IT to easily implement policies across users/data/applications, drive employee productivity, and transform mobile devices, including BYOD, into a natural extension of your business.

Acronis Access Connect (formerly ExtremeZ-IP)

Acronis Access Connect enables seamless integration of Macs into Windows environments and includes file access for mobile devices. This solution enables Macs to connect to file servers and NAS by using their native Apple Filing Protocol (AFP). By using the Acronis Access Connect optional Network Reshare feature, Macs can use AFP to access files on a collection of Windows servers and NAS devices, through a single Access Connect server. This eliminates incompatibilities with file and print services, adds support for nearly instant Network Spotlight search of files shares, and greatly reduces help desk/support requests.

For additional information on Acronis Mobility, Backup, Cloud, and DR solutions, including industry use cases, please visit www.acronis.com. Follow Acronis on Twitter: http://twitter.com/acronis.
Enterprise Mobility & BYOD

by Gill Borniche, Derick Naef, and Ryan Williams
# Table of Contents

## Introduction ................................................................. 1

## Chapter 1: Understanding the Basics of Enterprise Mobility ......................................................... 3
- What the Heck Is BYOD? ............................................... 3
- Why Do You Need BYOD? .............................................. 4
- What Are the Risks? .................................................... 7

## Chapter 2: Surveying the Solution Landscape ................................................................. 9
- Mobile Device Management ......................................... 9
- Mobile Application Management ................................. 11
- Mobile Email Management ......................................... 11
- Mobile Content Management ....................................... 12
- Accounting for the Needs of Your Customers ................ 13

## Chapter 3: Creating, Defining, and Implementing Your BYOD Policy ........................................ 15
- Assessing the Needs of Your Business ......................... 15
- Heading to the Workshop ............................................ 19
- Making Your Employees Mobility-Aware ....................... 20
- Setting Your Mobility Adoption Curve ......................... 21
- Communicating Your Mobile Strategy ......................... 22
- Measuring the Effectiveness of Your Methodology ........ 24

## Chapter 4: Setting the Bar for Your Mobile Content Management Strategy ................................ 25
- Driving End-User Productivity ..................................... 25
- Enabling Productivity for Your Users ......................... 27
- Securing Data, Users, and Devices .............................. 28
- Managing the Mobile Environment ............................... 34

## Chapter 5: Key Considerations for Implementing a BYOD Policy ............................................ 37
- Ensuring Compliance ................................................... 37
- Setting Acceptable Use Policies ................................. 38
- Enforcing BYOD Policies ............................................ 39
Chapter 6: Ten Reasons You Need a BYOD and Mobility Plan

BYOD Makes Employees More Productive
BYOD Enhances Security
You Can Install BYOD Solutions Easily
Small- and Medium-Sized Businesses Benefit Greatly from BYOD
BYOD Solutions Require (and Enhance) Communication
BYOD Allows Easy Access, File Edit, Sync, Share, and Control
BYOD Enforces Active Directory Policies
BYOD Helps Maintain Compliance
BYOD Helps You Track Access
BYOD Policies Standardize the Devices on Your Network
Many experts believe that there’s a connection between the business performance of an enterprise and the technology investment that business makes. The most profitable companies invest more in technology and use it as a competitive advantage versus their less profitable counterparts whose technology investments are flat or declining.

But what if you’re a small or medium business that can’t make a huge technology investment? Or what if you want to take advantage of existing resources to optimize your productivity and ease of access to data?

The concepts of mobility and mobile technology offer organizations the ability to empower remote, traveling, telecommuting, and field employees and make their jobs easier. Through real-time collaboration, these employees become more productive and can respond faster to the customer — all of which can improve customer retention, customer acquisition, and revenue.

You also get to take advantage of existing mobile devices to extend the reach of your workforce. Bring Your Own Device (BYOD) enables your employees to be much more productive without saddling your IT staff and your budgets with a lot of extra time and money.

About This Book

This book is about enterprise mobility, and it’s your guide to putting a competitive mobile infrastructure in place. Whether you’re a small- to medium-sized business or a large enterprise, you will find helpful use cases as well as tips on planning, implementing, and using a sound BYOD policy.
Foolish Assumptions

When we wrote this book, we assumed the following things about you, the reader:

✓ You’re familiar with BYOD and mobility, but not a mobility expert.
✓ Your business is looking to improve employee productivity and growth, and to boost revenue.
✓ You’re looking for some tips on how to implement a simple, complete, and safe mobility or BYOD strategy.

Other than those assumptions, we work from the ground up to make sure you understand everything that enterprise mobility and BYOD have to offer your organization.

Icons Used In This Book

From time to time while reading this book, you may see some icons in the margins, just begging for some attention. Take a little time to introduce yourself to these icons so you can be prepared for just such an encounter.

This handy little tidbit adds some insight and information to your reading experience.

If we need to emphasize a point a little more, we use this icon to make the emphasis happen.

Sure, you’re already reading a book all about technology. But sometimes we need to dig a little deeper, and that’s when you see this icon.

Where to Go from Here

Like all For Dummies books, this one can be read in whatever order is most helpful to you. Start with Chapter 1 and go straight through, or skip around. It’s up to you.
Chapter 1

Understanding the Basics of Enterprise Mobility

In This Chapter
- Bringing employee mobile devices into the workplace
- Understanding why you need the benefits of a BYOD policy
- Ascertaining the risks of a BYOD policy

When you think of a company or business, you probably think of a single large entity, looming over the landscape of its chosen field. While enterprises can look large, even monolithic from the outside, the reality is rather different. Instead, modern business relies on smaller entities within the larger whole, with separate teams working on smaller goals that contribute to the larger mission. And these teams can work from more than just the standard desktop in the standard office. Today’s reality includes teams of workers collaborating across locations, time zones, and corporate networks.

This chapter takes a look at the larger concept of enterprise mobility and breaks down the concepts you need to familiarize yourself with to fully understand your needs and the applicable solution. Let’s get mobile!

What the Heck Is BYOD?

While the BYOD acronym may conjure up directives to bring the food and beverage of your choice to a party, Bring-Your-Own-Device (BYOD) policies actually govern how you integrate employee-owned vs. company-assigned and -owned
devices into your larger corporate data network. Smaller companies may need to implement BYOD policies out of necessity (“Hey, do you own your own laptop and smartphone? You’re hired!”), while larger businesses may use BYOD to help their employees remain productive while away from the office. We discuss more specific BYOD goals in Chapter 4, but for now you review exactly what devices are included in BYOD:

- **Smartphones:** The indispensable business tool, the irreplaceable connection to social media, the sometimes pacifier of small children needing to play a video game
- **Tablets:** Larger than a smartphone and useful for a variety of business applications, up to and including laptop replacements
- **Laptops (PCs and Macs):** The standard tool of business because you can actually lug your computer home with you

Because more and more employees own their own devices (and don’t really want to lug around multiple laptops, tablets, and smartphones), BYOD policies allow companies to integrate mobile devices into their standard business procedures.

And the number of companies implementing BYOD policies increases as time goes on. Gartner predicts that four in ten companies will exclusively rely on BYOD policies by 2016, and 85 percent of businesses will use some form of BYOD program by 2020.

**Why Do You Need BYOD?**

IDC reports that by 2016, employee-owned smartphones, tablets, and PCs in the workplace will grow from 2 billion to more than 5.25 billion. It’s virtually impossible for most organizations to prevent employees from bringing their own devices to work. The need to control IT budgets, enhance productivity, and support flexible working hours (in the office and remotely) are forcing IT departments to allow staff to use their own smartphones, tablets, and even PCs.

Of course, a BYOD policy isn’t just about securing mobile devices; a well-crafted BYOD solution includes a layer dedicated to securing your organization’s sensitive data and
content. A Mobile Content Management (MCM) solution empowers your employees to be able to access, create, edit, save, and share content and files securely. In this section, we’ll take a closer look at some use cases.

**Productivity and collaboration**

A good BYOD solution permits you to send the right content to the right person at the right time, whether that person works for you or interacts with you as a customer or partner. The solution helps you set up the best location for the information and grants access and editing rights appropriately. For example, you can have a folder containing marketing materials that your marketing department can edit but that the entire company can distribute and share. Your employees can send or display these files from a mobile device, and nobody loses data or content if a single mobile device goes missing during, say, a tropical vacation or a long air trip.

**Mobilize desktop-centric data sources and workflows**

Organizations of all types typically employ standard Windows network features such as personal network home folders assigned to each user, and network file shares that are automatically displayed in Windows when users log into the network. These data stores are most commonly presented as “network drives” that can be found in Windows Explorer and are often labeled with drive letters. Users might have an H: drive that is their personal home directory, an S: drive that is their departmental file share, an M: drive that is their company-wide file share, and so on. MCM systems that integrate with Active Directory and allow access to these existing file shares can be used to provide access to the same data sources using the same terminology that users are familiar with. This lets them adopt convenient mobile access with minimal training or modification to the way they already work with their files.

**Distribution of file content**

No matter your industry sector, having the latest version of presentation materials, price lists, order status, and so on at
hand is invaluable for any sales meeting. Also, think about the benefits of having immediate access to a library of large files (manuals, plans, architectural drawings, and so on) without the lag of having to download large files on demand or while away from a network connection (beneficial for field service personnel, airlines/pilots, energy, and construction companies).

This file distribution can target mobile devices with MCM apps or laptops with MCM sync clients installed.

**Consolidate multiple data sources into one easy solution**

Businesses often run multiple file servers and store data on Network Attached Storage (NAS) and SharePoint servers. In most cases, your employees rely on their colleagues to learn the existence of many of these resources and keep track of file share names and addresses. Those employees may also try to build up a collection of shortcuts to keep track of them all, but often they must hunt around for the locations they need to get their work done.

MCM solutions provide a way to present all these dispersed data sources in one managed solution that gives users access to all of the relevant file shares they need, based on their Active Directory (AD) group membership, from within a mobile app, desktop app, or web portal. This benefit eliminates the complexity of managing and interacting with file shares located on multiple servers using various storage technologies.

**Reduction in printing needs and costs**

Tablet access to files for consumption in meetings, away from the office, or when you know you’ll be offline alleviates the need to print out documents. This benefit reduces printing costs, is better for the environment, and lightens the load you have to carry around. Your information remains secure because it makes it harder to misplace your sensitive presentation or customer details, and you don’t have to worry about shredding these documents before discarding them.
Meeting materials distribution

Rather than printing a bunch of documents that each person in a meeting needs to have, you can use MCM instead. You can give automatic access to the appropriate folder of meeting materials at the beginning of the meeting and remove access at the end if it’s sensitive data. By using MCM policies that restrict actions that can be taken within the MCM mobile app, the folder can be protected from edits or even from having data copied and pasted out of the documents.

Elimination of duplicate versions of files

Without a solution to co-edit and share files with external consultants or partners, users may take it upon themselves to find a way to get this work done. This process can involve, sharing copies into Dropbox or Google Drive and using collaboration features in that service to work on files. You may expect the definitive version of your files to reside on the company file server, but a newer revision may exist in Dropbox, or people may be working on many versions, making for a messy job of merging the changes in both versions at some point in the future. One of your employees could end up presenting without the entirety of the slides she should use.

What Are the Risks?

You may be wondering what the risks of a BYOD policy are, so in this section, we show you.

According to InfoWatch’s First Half 2014 Global Data Leakage Report, employees are responsible for 71 percent of data leaks. Having several BYOD mobile devices linking to a corporate network without the correct security implementation will give many IT directors some sleepless nights. The fact is that every single mobile device represents a point where data can be lost, stolen, or compromised.

The correct BYOD solution offers IT departments the ability to monitor and correct security situations remotely, preventing unauthorized individuals from gaining access to private
information. With the number of smartphones and tablets on the rise and a decrease in traditional PC sales, attacks on mobile devices are maturing. By 2017, Gartner predicts that the focus of endpoint breaches will shift to tablets and smartphones from traditional PCs.

A good BYOD solution also prevents your employees from accidentally sharing information with others by implementing permissions and sharing restrictions.
Chapter 2
Surveying the Solution Landscape

In This Chapter
▶ Managing all aspects of mobile devices
▶ Controlling your apps on a mobile device
▶ Regulating how a mobile device interacts with a corporate email account

If implementing a BYOD policy were as simple as saying “Hey everybody, just start working on your mobile devices,” you wouldn’t need a book to describe all of the concepts and requirements you should cover, right? The fact is BYOD requires you to search out software solutions that provide you with some basic functionality. Otherwise, you lose the benefits of productivity and efficiency that BYOD can provide (and probably expose yourself to security problems down the road). In this section, you take a look at what functionality a good BYOD solution includes.

Mobile Device Management

Mobile device management (MDM) helps you administer all facets of working with mobile devices:

✔ Deploying mobile devices for use in the field
✔ Securing the data on those mobile devices
✔ Monitoring the location and usage of those mobile devices
Integrating different types of mobile devices into your network

Managing the tools and apps on those mobile devices

MDM includes all types of mobile devices: smartphones, tablets, and often laptops. MDM helps you optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network.

Mobile device management software allows distribution of applications, data, and configuration settings and patches for such devices. Ideally, MDM software allows administrators to oversee mobile devices as easily as desktop computers and provides optimal performance for users. MDM tools often include application management, file synchronization and sharing, and data security tools, and will support either corporate-owned or personally owned devices.

The ideal mobile device management tool:

- Offers compatibility with all common handheld device operating systems and applications
- Functions through multiple service providers
- Implements directly over the air, targeting specific devices as necessary
- Helps you deploy next-generation hardware, operating systems and applications quickly
- Helps you add or remove devices from the system as necessary to ensure optimum network efficiency and security

Mobile device management includes many features to help you manage all the gadgets that need to access your data:

- Device encryption
- Requirement of a device lock passcode
- Data backup
- Remote wipe (totally clearing the device of all data, apps, and information)
Mobile Application Management

Mobile application management (MAM) describes software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings on both company-provided and BYOD smartphones and tablet computers.

MAM differs from MDM in a couple of different ways. As the names suggest, MAM focuses on application management. It provides a lower degree of control over the device and a higher level of management and control of applications. MDM solutions manage everything down to the device firmware and enable your IT staff to implement important security measures.

Work with your users to ensure they know exactly how this software will affect their devices. A little knowledge goes a long way toward bringing users into your BYOD plan.

Analytics information

Good MAM solutions provide insight into how users actually use and interact with your app. This information (including time spent in the app, which sections of the app got the most usage, and any crashes or errors) helps you determine how your app functions and what you may want to change.

Push messaging

You can use some MAM solutions to send messages to mobile devices via the app. These kinds of messages can include instructions, update notifications, or special alerts.

Use push messages judiciously — too many, and you run the risk of becoming the equivalent of email spam.

Mobile Email Management

Mobile email management (MEM) solutions deliver a complete security layer for corporate emails. You can configure
advanced compliance policies to manage user credentials, and prevent data breaches by allowing, removing or blocking mobile devices that access corporate email.

A good MEM solution lets you execute some power tasks:

✓ Configuration of enterprise-wide fleet of mobile devices to authenticate users for granting access to corporate email
✓ Remote lockdown, complete wipe of mobile device, or selective wipe of corporate email from stolen, lost, or compromised devices
✓ Standardize security protocols across a range of mobile devices and platforms to comply with corporate policy
✓ Monitoring and managing over-the-air, real-time provisioning to enable, disable, and remove users and devices from accessing corporate email

Mobile Content Management

Mobile content management (MCM) enables employees using any device – desktop, laptop, tablet or smartphone – to securely access, sync and share corporate content while IT maintains control over security and compliance.

Key benefits include:

✓ Secure access to corporate content for mobile users
✓ A secure method for users to share content with internal and external constituents across their desktops, laptops, tablets, and smartphones
✓ A viable alternative to end-users using insecure and unauthorized cloud file sharing services such as Dropbox to access and share content
✓ Complete visibility into access, sync, and share activities for auditing purposes
✓ Features that complement your MDM solution for basic device and applications security

We discuss this functionality in depth in Chapter 4.
Accounting for the Needs of Your Customers

If you’ve ever taken to social media or email to express rage, frustration, or (hopefully) transcendent joy with a product or service, you’re one of many consumers that expect companies, large or small, to remain connected to their customers whenever a customer needs assistance. Or a shoulder to cry on. Or a target of scorn, unfortunately.

BYOD policies can help your business stay connected to that customer, whether you need to access a social media account or pull up valuable documents and data. With a portable device like a smartphone or tablet, that information lies just a few taps away. And because the employee uses his own device, he’s more likely to have the device ready to go at a moment’s notice.

The added interactivity means teams can collaborate to put together a winning product as well. Just because your team doesn’t interact with customers directly doesn’t mean that it can’t help put a deal over the edge or finish a vital project. BYOD encourages collaboration and ease of use, and both customers and your business can benefit.

Security

Having several BYOD mobile devices linking to a corporate network without the correct security implementation will give many an IT director some sleepless nights. The fact is that every single mobile device represents a point where data could be lost, stolen, or compromised. The correct BYOD solution offers IT departments the ability to monitor and correct security situations remotely, preventing unauthorized individuals from gaining access to private information.

A good BYOD solution also prevents your employees from accidentally sharing information with others by implementing permissions and sharing restrictions. You should be able to tell who accessed what information and when.
Easy to use

No BYOD policy helps out a company if employees or IT staff members find the solution difficult to use. BYOD enables real-time collaboration and should enhance productivity, not create a drag on your business processes. Your solution should quickly integrate with your existing data and allow the correct access without hassle or a lengthy installation process.

Installation times may differ depending on the amount of data you manage, but the goal here is to keep the time at a minimum and not involve a lot of complicated processes.

Check regulations to make sure you store your data in the correct locations. Banking, health, and other regulated industries may require additional configuration to meet all applicable laws.
Chapter 3

Creating, Defining, and Implementing Your BYOD Policy

In This Chapter
▶ Accounting for your business tasks and needs
▶ Determining how you implement your BYOD policy and adoption
▶ Evaluating the success of your policy achieved

Every plan requires a checklist of goals and tasks to accomplish to achieve success, and your BYOD policy deserves nothing less. This chapter takes a look at what you need to put in place to make sure your newfound enterprise mobility helps everybody involved. Grab a piece of paper (real or virtual) and start your list now.

Assessing the Needs of Your Business

No matter the size or type of your business, you need to address a few standard concerns to create and implement a successful BYOD plan.
Putting your team together

Creating a BYOD policy requires input from several different teams, including Business, IT, Legal, Human Resources, and Sourcing and Procurement. And, of course, you need executive buy-in and endorsement. Obviously, depending on the size of your company, these departments may utilize the same representative (or not exist at all), but the names given here should give you some indication of the issues you need to deal with:

- Integration into business workflows
- Integration into the existing data networks
- Meeting all security, legal, and regulatory requirements
- Honoring your commitment to your employees and getting them the right information
- Making sure your employees access (or receive) the correct devices

Getting your team together starts you on the right path to adopting a functional BYOD policy.

Standardized devices

Sure, BYOD implies that employees can use their own personal devices with your data, but you need to set some standards. Older devices may not be able to handle the technological or security requirements your BYOD policy demands. You also need to standardize the policies around these devices:

- Who is ultimately responsible for the device
- Any costs or reimbursements required by mobile device usage
- Allowable phone and data plans

By getting a clearer and defined picture of the allowable devices, plans, and costs involved with your enterprise...
mobility strategy, you will better understand how to implement your policy and make it work for your company.

**Users**

Map out the employees in your business and determine which ones need access to your business data and resources. If everybody has to access everything, this may be a very short step. But if you have to parcel out permissions and access, a complete user map allows you to better assign these permissions and get a handle on what needs to be accessible and where.

This step includes evaluating your current Active Directory implementation (or other authentication and authorization system) to make sure that each user has only the necessary privileges and no more. This can include outside consultants or partners.

**Content and data**

Determine which resources will become available to mobile devices as part of your BYOD policy. Your business processes (or applicable laws and regulations) may not allow you to make some information accessible to mobile devices. Evaluate where you keep your information and create a strategy that analyzes your information architecture. After you know where your information resides (including mobile devices, computers, servers, and external storage like flash drives), you can determine where it should reside and if a change is needed.

Your BYOD policy helps ensure security for information accessed on mobile devices, but that policy may include keeping especially sensitive information out of circulation entirely.

**Policies and standards**

Mobile devices are different from desktop computers, servers, and other fixed locations. Quite simply, mobile devices can interact with your enterprise data anywhere that device can access a cellular data network or a WiFi connection. That’s a lot of power for tiny devices that users can easily lose. Your
updated policies and standards should address these new realities and outline appropriate behavior:

- Where and when employees can use mobile devices
- What kind of connections those mobile devices can use, including what kind of Wi-Fi networks are appropriate and when to use a VPN connection
- How to address device loss or theft
- How to address accidental exposure of sensitive data

Ultimately, you want to cover both your business and your employees with policies that ensure the safety and security of your devices, your data, and your legal and ethical concerns.

**Mobile management**

Depending on the amount of control you want to exercise over your business data, you may need to take additional measures to make sure that content accessed on mobile devices stays within your reach at any time.

You can use mobile management services to help you control that data:

- **Mobile content management (MCM):** Allows employees using any device – desktop, laptop, tablet or smartphone – to securely access, sync and share corporate content while IT maintains control over security and compliance.
- **Mobile device management (MDM):** Allows you to remotely administer mobile devices, including any applicable data, configuration, and applications
- **Mobile application management (MAM):** Allows you to remotely push, manage, or remove apps on a mobile device
- **Mobile email management (MEM):** Allows you to administer corporate email accounts on mobile devices securely

If you require access to sensitive data on mobile devices, and you need to ensure that you keep control of that data even on
personal devices, one or more of these methods could help you achieve all the necessary goals.

Make sure that these applications do not adversely affect how the mobile device functions. Employees are more likely to adopt your BYOD policy if their mobile devices don’t crash or slow to a crawl.

**Heading to the Workshop**

After you get your checklist together, you can start applying your findings to your actual business plans. This step involves matching your guidelines to your actual business practices. The theoretical needs and the realities of your business need to meet at some point, and this step is where that meeting happens.

**Workflow**

Research how your business actually operates and see how BYOD policies can enhance that workflow. For example, your sales reps may need updated information in the field, or your IT workers could get to the next task without having to return to the desk to review the ticket queue. Look for ways where BYOD moves things along without compromising data security.

**Data locations**

Place your data where you need to have it in order to make it available while maintaining proper security. This step may involve removing old devices, centralizing servers, and tracking down unsecured USB drives. Take the necessary steps.

**Applications**

Determine which applications you need to use as part of your strategy and make sure you can push those applications to the devices when needed. You need to automate this process as much as possible — the amount of applications, data, and configuration information you need to manage just doesn’t scale correctly when you handle everything manually.
Making Your Employees Mobility-Aware

Sure, your employees already know about mobile devices. They own their own devices, after all, and they probably stare at them for a large portion of their day. But you need to make your employees aware of exactly how they use their devices and how their behavior affects the security and productivity of their work.

Access

Make sure your employees implement a secure method of access to their devices (passcodes or biometric access, like thumbprints) to keep data secure and safe. Ensure that they use passwords as directed in your security policy.

Networking

Working outside of the office demands that employees make use of wireless networks outside of your precise control. From home networks to coffee shops or hotel hotspots, devices that can access your data will connect to possibly unknown networks just to conduct daily business. Make sure your employees know to only use trusted networks and use a VPN connection to your servers when necessary.

A criminal could steal data from your employee’s device if connected to an untrusted Wi-Fi network, such as a fake Wi-Fi hotspot. Employees need to assess the safety of the networks they use (don’t automatically trust “We promise this is free Wi-Fi” in the airport), but you can also provide VPNs to help them stay secure and regulate access to your data.

Correct app and data usage

Make sure your employees use only approved channels and apps to work with business data. Emphasize that commercial cloud services don’t offer the best security options and that you need to keep business data in secure locations.
Device location

Make sure your employees always keep their mobile devices under their control, no matter where they are. They probably already do that (because they’ll be staring at their phones anyway), but remind them of the necessity.

One of your strongest assets is an aware and informed employee. Take the steps necessary to educate your workers properly, and that effort will pay off.

Because you rely on personal mobile devices to make an effective BYOD policy work, you obviously need to take steps to work closely with your workforce to implement that policy successfully. Communicate your strategy to your employees and get them onboard for the journey. Also, make sure to measure success and adjust the plan as necessary.

Setting Your Mobility Adoption Curve

Your workforce needs to know how this policy will affect their mobile devices, and you need to know exactly which devices to work with. Simply put, this process takes some time and planning, so you need to implement a plan.

Take inventory

Survey your workforce and find out which mobile devices they use (and which ones you can integrate into your plan). Decide how to work with unapproved devices and how to proceed from there.

Start with a small group

Software needs beta testing to ensure functionality, and this process is no different. Pick some representative samples from your workforce and find out how your implementation works. Then define what changes are needed.
Set your dates

Make sure your implementation works with any business events you may have coming up. Pushing a new software and methodology change in the middle of your big sales season may not help everybody out, so pick a quiet time for this.

Ease into it

Make the process as easy and painless as possible. Change will inevitably cause some stress, but a good schedule and implementation will help reduce that stress.

Communicating Your Mobile Strategy

Nothing makes a new policy more attractive than communicating exactly how that policy helps make life better. If you share your vision (and the advantages) with your workforce, you get much larger buy-in than just implementing the policy and asking for access to an employee’s mobile device. Involve your human resources department to ensure that the guidelines associated with the BYOD policy are clearly communicated to your employees.

Extending your functionality

Mobile devices probably won’t replace laptops and desktops for a little while, but they do help the employee remain productive away from the computer for longer periods of time. Make sure your employees know that this policy gives them more freedom to handle tasks from wherever they are.

Easier access

Your new policy helps employees get secure access to the latest version of any applicable information. No more using old or obsolete documents, and no more reconciling different
documents with different edits. A good BYOD policy lets employees access documents from their original locations with ease.

**Synced content**

A good BYOD policy and implementation makes sure the same version of your files appear wherever you need to access them, be it phone, tablet, or laptop. One edit applies to all locations, and everything stays up-to-date.

**Shared content**

Businesses cannot rely on emailed files and information for effective functionality. Good BYOD policies and implementations allow proper sharing with individuals both inside and outside the company. Simplifying and streamlining the sharing process makes life easier for everybody.

**Productivity**

Getting more done in and out of the office should appeal to your employees. Emphasize how this BYOD solution will help them better perform their jobs.

**Privacy and separation**

Because you will push your application, data, and configuration information to personal devices, you need to assure your employees that you won’t need to access their personal information in order to make your plan work. Assuring your employees that you use only the necessary and vital functionality while leaving everything else alone will go a long way toward assuring adoption.

Anything you can do to help the BYOD solution makes the process easier and more effective. Work with your employees to keep everybody happy and productive.
If you don’t have the in-house knowledge, figure out whom you can enlist to help. The most likely contenders include:

- IT channel partners — or mobility specialists
- The vendors themselves

Many offer trial downloads and assessments and host regular mobility workshops. Besides, it’s in their best interests to make your project successful because there’s nothing better than a happy customer who’s willing to give you a reference!

**Measuring the Effectiveness of Your Methodology**

Communication with your employees is key to finding out how effective your solution is in reality. Talk with the workers and find out how it’s working. You can also review audit trails from your BYOD solution to see who accesses what information and when. You can evaluate effectiveness based on employee feedback and usage data. You can also check with your customers to see how they enjoy working with shared data and how effective they find it. Basically, this step involves opening all possible communication channels and utilizing what information flows back:

- Employee surveys
- Customer surveys
- Usage statistics
- Audit reports
- Logged IT tickets
- Any other incident reports
Chapter 4

Setting the Bar for Your Mobile Content Management Strategy

In This Chapter

▶ Setting the selection criteria for a mobile content management solution
▶ Improving end-user productivity
▶ Implementing tools for IT to manage the mobile environment

The key to enabling productivity among the mobile workforce is a strong Mobile Content Management (MCM) solution. MDM and MCM provide useful enhancements to your solution, but MCM provides the foundation for your efforts. This solution lets employees get access to their files from any device, review and modify those files even when they’re offline, and share their work and collaborate with others inside and outside the organization. All the while, MCM helps you maintain the proper security, control, and compliance standards required by your business.

Driving End-User Productivity

To enhance the discussion of mobile user scenarios and requirements, this section reviews the three classes of devices the mobile workforce uses to get its job done.
Mobile devices

Smartphones and tablets provide access to the content your employees need. These devices allow editing and sharing, but they also keep control of information when mixing personal and business data on a device that may be lost or stolen as well. Users may lug along multiple devices, ideally allowing work started on one device to be accessible on the others.

For example, one company uses mobile devices to keep its workers at remote sites to update documents instead of requiring a trip back to a main construction office to reference or update documents. Another permits airline workers to update pilot documents and maintenance logs onsite instead of using paper and potentially losing data.

Web browsers

Browsers provide access to content when users only have a web browser or need the simplicity of web browser access to data instead of complicated VPN setups or additional software. Many people find relying on VPN connections to get into the corporate network can be complicated and introduces security threats by connecting the entire device to the network. Web browsers also allow partners to get access to shared content without the need to have additional software installed. This step can be especially useful when sharing content with a partner in an ad-hoc, one-off manner, when he only needs to get the occasional file from you. For example, a company can create a centralized document hub that its franchises can use to distribute important information and maintain a central store with folders for each franchise.

Laptops and desktops

Remote-user access to files to get work done can be done by using traditional laptops and desktops. But users can use simpler access than having to setup VPN tunnels and control access onto the network. For users who are traveling, an important use case is offline work, which enables users to work without constant connection to the corporate network or cloud, and sync their changes once they’ve regained network connectivity.
Laptops and desktops typically include their own controls on them, such as encrypted file systems. For example, a company can maintain a central store of documents that automatically updates information when connected to a network. A good mobile content management system ensures that all those documents sync to all applicable devices, giving everybody the latest information as soon as they connect to a network.

**Enabling Productivity for Your Users**

An effective BYOD MCM strategy enables the following use cases to enhance productivity.

**Accessing content**

MCM provides your workers with access to the data they use in their jobs, whether that’s on file servers, home directories, SharePoint sites, or in other document management systems. MCM allows them to have seamless access, including browsing, searching (by file name or content), file previewing, and bookmarking frequently used content. Ideally, the solution automatically configures available data sources on the BYOD devices, just like a network folder created on their desktops. The key to maximizing productivity involves recreating the desktop environment they’re familiar with on the mobile device.

**Editing and manipulating files**

MCM lets employees edit files and get their work done when they’re mobile. This includes full Office editing or PDF annotation capabilities on their mobile devices. MCM allows them to edit content in other applications or to take content from other applications and place them into the mobile content management system. For instance, an insurance adjuster may need to take photos from a remote location and upload them into the corporate SharePoint repository. A medical office may also use mobile devices to gather and share information to all involved staff, whether they work in the clinic or in the field. The security of MCM lets them maintain HIPAA compliance while performing their tasks.
Offline access and synchronization

Mobile users can’t always access the corporate network or the cloud. They may be on a plane, without cellular coverage, or otherwise prevented from getting a signal. But work must continue, even while they’re offline. Workers need to be able to synchronize the files they need onto their devices, work on them offline, and automatically place them back into the corporate repositories when they regain network connectivity.

For instance, the field sales force can know it always will have the latest product literature available on mobile devices before it goes into a meeting with a prospective customer. Any changes made by the marketing staff will automatically appear in folders after deboarding the plane.

Sharing and collaborating

Mobile workers don’t conduct business in a vacuum. They share information and collaborate with teammates and external partners. An MCM solution enables them to share and collaborate with each other while on the road, no matter where collaborators reside or who they work for.

MDM solutions only apply security policy to devices for a given company. The MCM covers not only those devices covered by MDM but also to anybody else accessing your information. Almost every business interacts with other businesses to get work done!

Securing Data, Users, and Devices

You need to look at several different methods to make sure that all aspects of your operations remain safe and secure. This section highlights the key components of your security plan.

Controlling access to data

The use cases enabled by your BYOD strategy sure sound exciting, but before you run off and start sharing data, make
sure the data is secured and access is controlled according to corporate IT policies.

**Active Directory permissions**

MCM lets you provide access to the existing content while honoring the security and permission structures already established. You don’t need to copy data into a new storage repository or implement new permissions that contradict measures defined by the corporate policy. Instead, take this opportunity to evaluate and enforce the directory and permission structure defined by Active Directory.

A properly implemented permissions structure provides the basis for a functional MCM policy.

**Providing additional security policies layered on top**

Even if the solution conforms to Active Directory security policies, you may need to define and enforce a mobile-specific permission on top of the current permissions. For example, while a user may have full access to a given folder when at their desktop, when they are on a mobile device you may want to limit them to read-only access. That way, they can display the material in the field without accidentally introducing errors into the file. This flexible permission based on usage scenarios represents an important component of the MCM solution.

**Securing data in motion and at rest**

Controlling access to the data is only the first step. Determining how you deliver the data to the mobile worker and how their device stores that data is critical in designing an effective protection strategy for your MCM BYOD policy.

**Mobile network access**

Mobile network access can be complicated and full of acronyms — 3G, LTE, GPRS, and other confusing jumbles of letters. You need to make the access seamless yet secure for the
mobile worker. Luckily, you have a few options when it comes to mobile network access:

- **Direct access via HTTPS**: The simplest approach provides the worker with direct access to resources via the standard HTTPS protocol — the same used for securing web-browser based financial transactions. This scenario usually includes a gateway that the mobile device authenticates with. This gateway handles communications with backend data sources like file servers or SharePoint to provide access. This process is similar to how workers access mail using the Microsoft Exchange Outlook Web Access feature.

- **Reverse proxy**: A reverse proxy introduces a proxy that forwards the incoming requests to other systems inside the corporate network. Reverse proxies can use their own security policies, authentication, and auditing.

- **VPNs and per-app VPN**: For deeper access to a corporate network, you can establish a virtual private network (VPN) connection. A VPN allows the mobile device or laptop to appear as an actual part of the corporate network and get access to all kinds of resources.

- **2-factor authentication**: For added security, some network access technologies use 2-factor authentication. This process requires another method of authentication besides a username and password to gain access to the network. This other method could include a PIN code, a separate device (RSA SecurID token or CAC card), a biometric signature (such as TouchID on the iPhone), or a separate code delivered via SMS to a mobile device.

- **Verifying mobile device is in conformance to policy before network access**: Some solutions provide the ability to ensure that a device is in conformance with a specific policy before network access is granted, for instance, that the device has been unlocked with a second factor passcode, that it hasn’t been jail broken, or that it isn’t located in a foreign unfriendly country.

The jailbreaking process involves using a software tool to bypass any operating system or network settings and take control of the phone at the root level of the device. This process can severely compromise the security and stability of a mobile device.
Encrypting data on mobile device

After content arrives on a mobile device, the effective MCM BYOD solution must ensure the content is secured. While some mobile devices provide an encrypted file system, not all do:

- **Not all devices are secure:** Rooted or jail broken phones may allow users to go beyond the intended functionality of the manufacturer, but they also present increased security challenges. Without the normal protections in place, rooted or jail broken phones may be easy prey to unwelcome attacks.

  Even with devices such as the iPhone, once the device itself is unlocked by passcode or password, the content can be accessed using third-party tools such as the iExplorer (http://www.macroplant.com/iexplorer/).

  Thus, the MCM solution must provide an additional layer of security on top of the native security of the device, such as an encrypted file system that keeps the content stored on the device secure at all times. This process should include encryption of file names of the content, since file names frequently can communicate information that must be protected as well.

- **Passcodes on top of passcodes:** Many mobile devices today lock by passcodes, so nobody but the intended user can access the phone. However, this level of security is not sufficient for the many companies deploying an MCM solution. Mobile device passcodes may be too simple, and anyone with children is familiar with the fact that kids may know the passcode to get to their parent’s phone and play Angry Birds better than their own phone number. So an MCM solution must provide an additional layer of passcode protection to the content, including optional complex passcode requirements, and control over when the passcode is requested.

- **Content expiration:** An effective MCM solution adds a layer of security for the content on the device by optionally supporting the automatic removal (expiration) of content under certain circumstances. For example, content downloaded to the device only remains present for a fixed period of time, or it automatically gets removed if the device hasn’t talked to the corporate network in a week. The device may also lose content when a user enters the incorrect passcode too many times.
Geofencing secures content using GPS technology, where content is only available while in specific physical locations. This method automatically wipes content even if the device leaves a country.

**Preventing data leakage**

Besides securing the content in transit and on the device, MCM must provide controls to ensure the content is not shared with the wrong parties, known as data leakage. This feature can be driven by the need to protect confidential information from competitors, or through regulatory compliance, such as HIPPA or personally identifiable information (PII).

**Printing, emailing, and copy and paste**

The most basic controls over data leakage required by an MCM solution prevent typical activities by the mobile worker, such as printing or emailing files or copying and pasting content from the device. These controls can apply to the type of content reviewed or the roles of the user (based on Active Directory security group memberships).

**Sharing content with third-party applications**

On a mobile device, workers may open content in files other than the built-in previewers you want them to use. Sharing information with third-party applications poses a potential window for data leakage.

Open In functionality in mobile applications allows content to be opened into a third-party tool. MCM solutions should provide the ability to block Open In completely, or allow restrictions so that Open In can only work with specific listed applications. For example, you can open content in your secure customer line of business application, but not in Dropbox (which can leak your data).

Recent enhancements to mobile device operating systems introduced the concept of Managed Open In. In this scenario, a device managed by an MDM solution allows you to mark an application as managed. In this case, you can allow Open In to other applications that are also managed. This control provides a more flexible way of controlling where your content flows on the mobile device.
Sharing content with others
Mobile workers rarely interact just with themselves. They collaborate with teammates and with partners in other companies. An MCM solution must provide the ability to share and collaborate while also enforcing corporate data leak prevention policies:

- **Providing controlled access to third parties:** Beyond preventing sharing at all (which is a viable option), MCM solutions should allow policies that specify a *whitelist* or *blacklist* of trusted parties for sharing. For example, a whitelist can include domains used for email that are allowed to receive content (bob@mylawfirm.com). A blacklist contains domains that should never allow sharing (sue@mycompetitor.com).

- **Providing links to content with expirations:** You can also protect the shared content by placing expirations or passcodes on the links that are shared. For example, if the MCM solution allows a worker to mail a link to a file for a third party to access this link could require a pre-negotiated password. It could also expire after a specific time or number of usages. You could also use a link that only works if the recipient uses the same MCM solution and conforms to the data sharing policies set by IT.

Audit trail
The past few steps helped you secure the data in transit and on the device and implement policies to protect data from leaking while also allowing collaboration. But a proper MCM solution requires one failsafe for proper compliance — an *audit trail*.

Track activity
The audit trail allows the system to track who accesses your content, where they put it, and with whom they share the content. Not only does this provide a record of what happens with your data through the mobile ecosystem, but also audit trails frequently provide required information for various regulatory and compliance reasons.
Provide logs for compliance

An effective MCM audit capability should provide the ability to filter and search for activity based on users or filenames. It should also allow for the exporting of the audit logs to third-party compliance systems.

Managing the Mobile Environment

This section defines mobile environment management requirements from the IT administrator perspective. This key functionality allows your admins to manage the users and devices they include in their mobile ecosystem, from a small handful of workers to a large number of users.

Managing users and devices

Mobile workers in an organization don’t just work with each other. If a company only worked with itself, it would never make any money. So an effective MCM solution will allow for the management not just of users from a corporate directory service like Active Directory, but also for ad-hoc users. These people share and collaborate with the company but may not be part of the company’s directory.

This key group typically won’t place their mobile devices under the control of an MDM solution. So the MCM solution needs to accommodate their access to corporate data while maintaining proper security controls for regulatory or compliance reasons.

Managing users with multiple mobile devices

How many mobile devices do you use? In addition to your laptop, you may own a phone and a tablet, and perhaps even a home computer. The MCM solution needs to track not only which users access corporate content, but also which devices they use for different activities. To support their users, your IT manager will want to gain visibility into the devices themselves, such as what platform they use, what version of the OS they loaded on their device, and what version of the MCM software is installed.
User expiration

External users may only interact with the MCM solution once, maybe over a short-term project. In this case, the MCM solution needs to allow for the definition of policies for when users expire. Not expire in the real world, of course, but when IT managers remove users from the MCM system so they can no longer gain access and consume resources, such as storage.

Quotas

Speaking of storage, if you’re sharing content with each other, what’s to prevent you from filling up all your corporate storage with personal content? A good MCM solution needs to provide quota policies, allowing IT managers to define how much storage each user can use. The policies should be driven by Active Directory or other directory security group definitions so that say regular users can’t have too many cat videos, but executives can have as many as they want.

Dealing with lost devices and passcodes

Your IT help desk will field calls from end users who lost their mobile devices or have forgotten their passcodes to gain access. The MCM solution provides a convenient way for administrators to issue remote wipe or lock requests to the devices, effectively allowing you to lock the content on a device until it is located. You can even totally remove the data.

A remote wipe of a MCM solution only removes the corporate content from the device, where a remote wipe of an MDM-managed device can also remove an employee’s photos from her kid’s latest birthday party. In the age of BYOD, you need to be very careful about what you remotely wipe!

Directory-driven security policy

From IT’s perspective, the MCM solution needs to provide tools to apply existing security group hierarchies to these policies. These tools restrict sharing of content to third parties if a worker is part of the finance department, but allow sharing of data sheets and proposals if they are in the sales group.
One-stop configuration

Security and ease of administration is only part of the equation. Your IT admins need a way to make sure that their mobile workers can access the information they need in the easiest way possible, with minimal confusing configuration for the mobile work.

Group policy for content

Anyone who has worked in IT is familiar with group policy or the ability to define a collection of settings applied to a user’s computer when they log in based on their role within an organization (typically dictated by their position in the Active Directory hierarchy).

*Group policy for content* helps IT managers define what content sources appear on a user’s mobile device or web browser automatically when they interact with the MCM system. For example, a person in the medical device sales group can use a sync folder that automatically appears on their phone, always containing the latest product data sheets available. Or someone in finance can access the SharePoint financial reporting documents placed on their iPad when they log in.

An effective MCM solution allows IT administrators to leverage existing directory structures to define what content becomes available to their users at any time. MCM offers minimally intrusive tools with a high security value, especially when paired with MDM. As user roles in the organization change, what appears on their devices does too. Workers always gain access to what they need to get their jobs done, which is the key benefit and requirement of the MCM solution in your BYOD strategy!
In This Chapter

▶ Making sure your information systems comply with laws and regulations
▶ Ensuring your policies stick
▶ Keeping your employees and customers happy

In this chapter, you take a look at the peripheral issues that surround your implementation. These issues may not take center stage in your BYOD policy, but you do need to consider them as you make your move into the enterprise mobility field.

Ensuring Compliance

Depending on the industry you work in, your business may need to comply with applicable laws and regulations. For example, the U.S. health care industry requires compliance with HIPAA laws that restrict access to personal health care information. Legal policies may require storage (or destruction) of certain documentation to comply with Sarbanes-Oxley or other regulations.
Managing information systems with these kinds of regulations can cause a lot of issues, but BYOD policies can help you comply with regulations. By implementing these policies, you can ensure that you only allow access to approved devices and users. In addition to the Mobile Content Management (MCM) functionality detailed in Chapter 4, implementing features like Mobile Device Management (MDM), Mobile App Management (MAM), and Mobile Email Management (MEM) makes sure that you keep control of your data at all times.

Do your research ahead of time to make sure you know every law and regulation you must comply with.

**Setting Acceptable Use Policies**

A good Acceptable Use Policy defines the actions that need to occur if something happens to the device (and the data that resides on it). You don’t have to break down specific scenarios (“You dropped your phone in the toilet? Take these steps now!”), but you should outline what your employees should do in the following circumstances:

- **Lost or stolen device**
- **Compromised device** (somebody can access the device using a password or code)

You also need to make clear what happens to whatever resides on the device:

- **Corporate data** (including apps, email, contact information, and any files or documents belonging to the business)
- **Personal data** (anything the employee puts on the phone not directly related to corporate activities, such as music, apps, embarrassing photos, and the like)

Essentially, you must balance the security needs of your business and the confidence of the employee. And you need to make sure the employees don’t feel burdened with your information and apps on their personal property.

Above all, good communication between you and your employees makes your BYOD policy work.
Enforcing BYOD Policies

Following the communication of your plans to your employees, you can roll out your BYOD plan and get your apps, data, and configuration settings on the mobile devices. Before you make the big step, check out your plan with the trusted beta group you assembled for testing.

After you implement your solution on approved mobile devices, keep the lines of communication open. You can follow device actions based on the audit trail functionality provided by a good BYOD solution, but you also need to let your employees know how they can reach you outside of that audit trail to let you know what’s happening with the mobile device. Provide phone and electronic communication methods that employees can contact when they’re outside of the office to get you prompt information if something bad happens to a mobile device.

Put this information on a separate card or make it easy to remember — if your employee loses or breaks a mobile device, they certainly can’t use the device to contact you, can they?

Make sure you also provide clear and precise documents that outline your BYOD polices and make sure your employees see and understand the information.

Honoring Service Delivery Policies

When you implement a BYOD policy, you enter into an agreement with your employees regarding the use of corporate data and functionality on personal mobile devices. But you also must honor any agreements you made with customers and clients as well.

Your BYOD policy cannot adversely affect any previous agreements you have with your customers regarding how you provide your service and products to them. Service Level Agreements (SLAs) ensure that you deliver an agreed-upon, consistent level of service at specified times.

Your BYOD policy can enhance the accessibility and productivity of your employees, helping you meet your SLAs. At the same time, though, you may need to disclose how
employees work with customer data and that they can access the information.

When developing a new enterprise mobility and BYOD strategy, do your research and make sure that everything you implement lines up with existing agreements.

**Staying Healthy and Safe**

After you make personal mobile devices a part of your workflow, you need to make sure that these devices remain up and functional. While they remain personal devices, you still need to provide some IT support to make sure that your device configuration needs can be met, and that your staff can get the assistance they need to keep everything working. Consider using implementation guides to keep your BYOD policy humming along. Implementation guides are simple, effective documents that users can access from mobile devices or computers that save a lot of help desk time and effort. Let your employees know the following information:

- Frequently asked questions (FAQs)
- What steps will occur, and when
- How those steps move the BYOD policy along
- What employees should do to ready themselves for these changes

**Keeping Everything Secure**

After everything is in place and to ensure that your data stays secure, follow these steps:

- Watch your audit trails and make sure nothing suspicious occurs.
- Train your employees to look for odd occurrences and keep in contact with your IT team if something goes wrong.
- Utilize your MCM, MDM, MAM, and MEM capabilities as soon as you need to. Let no unnecessary time elapse. Remember that you’re not erasing data, you’re just cutting off access.
In This Chapter
▶ Understanding the benefits of BYOD
▶ Enhancing employee productivity through real-time collaboration
▶ Protecting your data in a BYOD policy

This book contains the information you need to plan your BYOD solution (or pitch it to those who need to sign the checks). This chapter takes that information and boils it down to a handy reference list you can use to remind yourself or others of the advantages of a BYOD policy. Emphasize the points you need to make, or use the list as a whole.

BYOD Makes Employees More Productive

With a solid BYOD solution in place, employees can transcend the limitations of the office or other stationary workplaces. They can take advantage of access to files and documents from any location they may find themselves in, and they can work with other employees no matter the distance that separates them.

Good BYOD solutions also let employees share documents and work on single instances of projects without creating multiple copies. You get backed up data with easy access from anywhere. Productivity thrives in a BYOD environment.
For example, Bedford Industries uses Acronis Access Advanced to deliver the latest information and real-time video to sales professionals in the field. All information remains accurate, accessible, and highly available.

**BYOD Enhances Security**

No matter where employees access your data, you can count on a solid BYOD solution to make sure that data remains secure. Tools that allow you to wall off corporate data from personal accounts mean that you don’t have rogue points of access storing your data. Advanced solutions let you control security configurations, data, and even apps and devices themselves.

Without a good BYOD solution in place, employees can move and transfer data from corporate to business accounts without regulation. With an effective MCM solution in place, you actually gain more control over your data and apps, even on personal mobile devices.

**You Can Install BYOD Solutions Easily**

The right BYOD solution installs quickly and requires little training to access or manage. That solution should also integrate easily with your infrastructure. BYOD solutions should enhance productivity, not slow it down, and that philosophy applies to all aspects of the solution.

**Small- and Medium-Sized Businesses Benefit Greatly from BYOD**

Not only does BYOD enhance productivity, but it can alleviate strain on limited IT resources and budgets by allowing
employees to use existing hardware. Add cost savings and time savings to the benefits you realize from a BYOD solution.

**BYOD Solutions Require (and Enhance) Communication**

The actions of your employees matter as much as the security settings on a mobile device. Involve your employees with every step and make sure they know the expectations of the BYOD policy. Also, make sure they feel comfortable with how the policy affects their personal device and data. Both your company and your employees need to work together to make BYOD work.

Above all, your employees should understand that they also benefit from personal time savings.

**BYOD Allows Easy Access, File Edit, Sync, Share, and Control**

You can use BYOD solutions to specify how employees can interact with documents and files. For example, you can let mobile devices show files without editing, or you can enable full access to a document, including PDF annotation. Identify your needs and use BYOD to fulfill those needs.

**BYOD Enforces Active Directory Policies**

You can easily work existing Active Directory policies into your BYOD workflow so employees can seamlessly move from desktop to mobile devices. You already have the technology in place — make it work for you!
**BYOD Helps Maintain Compliance**

You can configure your BYOD solution to ensure compliance with any applicable laws and regulations. Whether you work in the health, banking, legal, or other industries, BYOD can meet your needs.

**BYOD Helps You Track Access**

A good BYOD solution provides an audit log to show where, when and which mobile devices accessed your network data. Use this information to track the effectiveness of your BYOD solution and make any necessary changes.

**BYOD Policies Standardize the Devices on Your Network**

Not every device meets the requirements of a solid and sound BYOD policy. Obviously, that old flip-phone from the '90s won't be a good option, but even more up-to-date devices may not be able to handle the technology necessary to keep your data accessible and secure. Make sure that you communicate to your employees which devices that work with a BYOD policy, and try to standardize your deployment as much as possible. Not everybody uses the latest and greatest mobile device, but you should be able to make a sound policy work with enough variety to make all your employees happy.
Empower your employees and make their jobs easier

The concepts of mobility and mobile technology offer organizations the ability to take advantage of existing mobile devices to extend the reach of your workforce. Through real-time collaboration, employees become more productive and can respond faster to customers, which improves customer retention, acquisition, and revenue.

- **Put a competitive mobile infrastructure in place** — set your company up for success
- **Get useful use cases** — discover tips on planning, implementing, and using a sound BYOD policy
- **Set your mobile content management strategy** — choose the selection criteria. Improve end-user productivity, and implement tools for IT
- **Make sure your information systems are up to date** — comply with laws and regulations

Open the book and find:

- The benefits of BYOD and mobility
- Ways to enhance employee productivity through real-time collaboration
- How to protect your data in a BYOD policy
- How to evaluate the success of your BYOD policy

Go to Dummies.com for videos, step-by-step examples, how-to articles, or to shop!
WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.