With the compliments of Kaspersky Lab

Mobile Security & BYOD

FOR DUMMIES®

A Wiley Brand

Brought to you by

KASPERSKY lab

Georgina Gilmore
Peter Beardmore

About Kaspersky Lab

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users.* Throughout its 15-year-plus history, Kaspersky Lab has remained an innovator in IT security, and it provides effective digital security solutions for large enterprises, small and medium sized businesses, and consumers. Kaspersky Lab currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide.

Find out more at www.kaspersky.com/business.

* The company was rated fourth in the International Data Corporation's Worldwide Endpoint Security Revenue by Vendor, 2011. The rating was published in the IDC report 'Worldwide Endpoint Security 2012–2016 Forecast and 2011 Vendor Shares' (IDC #235930, July 2012). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2011.

Mobile Security & BYOD

FOR DUMMIES®

A Wiley Brand

Kaspersky Lab Limited Edition

Mobile Security & BYOD

FOR DUMMIES®

A Wiley Brand

Kaspersky Lab Limited Edition

By Georgina Gilmore and Peter Beardmore

FOR DUMMIES®

A Wiley Brand

Mobile Security & BYOD For Dummies,® Kaspersky Lab Limited Edition

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom For Dummies book for your business or organisation, contact CorporateDevelopment@wiley.com. For information about licensing the For Dummies brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Visit our Home Page on www.customdummies.com

Copyright © 2013 by John Wiley & Sons Ltd, Chichester, West Sussex, England

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London, W1T 4LP, UK, without the permission in writing of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, or emailed to permreq@wiley.com, or faxed to (44) 1243 770620.

Trademarks: Wiley, the Wiley logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER, THE AUTHOR, AND ANYONE ELSE INVOLVED IN PREPARING THIS WORK MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN 978-1-118-66242-7 (pbk); ISBN 978-1-118-66241-0 (ebk)

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Contents at a Glance

Introduction

Welcome to *Mobile Security & BYOD For Dummies* – your guide to some of the key points to consider when you're enabling mobile access to your business systems or extending your existing mobile policy. With the tips and pointers in this book, we aim to help you avoid compromising your security and incurring any regulatory or legal penalties.

As with any change in business process, it's wise to consider more than just the benefits. Potential challenges can arise when mobile devices are used to access corporate data and systems. Plus, if you decide to go down the BYOD (Bring Your Own Device) route, you have additional benefits and issues to deal with. So it pays to be prepared . . . and that's why we've written this book.

About This Book

This book may be small, but it's packed with information about the benefits and challenges that mobile and BYOD access can bring.

For mobile access initiatives, there's no 'one-size-fits-all' approach. The book provides valuable tips and pointers to help businesses consider their own unique requirements – before formulating their own strategy. *Mobile Security & BYOD For Dummies* can help you take account of:

- General business benefits and challenges.
- Legal considerations and potential liabilities.
- HR implications – contracts, policies and training.
- Security and IT challenges, and solutions.

Foolish Assumptions

To help ensure this book provides the information you need, we've made a few assumptions:

- The business you manage or own or work for is interested in providing – or extending – access to its business data and systems, via mobile devices.
- You're looking for some tips on mobile or BYOD strategy.
- You need a few pointers about potential legal issues – and how to avoid them.
- You're keen to ensure that confidential data remains confidential.
- You're seeking information on technologies that can help prevent mobile-enabled access becoming a source of attacks on your corporate systems.

How This Book Is Organised

Mobile Security & BYOD For Dummies is divided into six concise, information-packed chapters:

- **Chapter 1: Why Mobile and BYOD?** We explain the benefits and the challenges you face.
- **Chapter 2: Exploring the Scary Stuff: Malware, Loss and Other Risks.** This chapter fills you in on the main security risks, now and in the future.

- **Chapter 3: Knowing the Legalities.** Keep on the right side of the law with the info here.
- **Chapter 4: Finely Tuning Your BYOD Strategy, Policy and Guidelines.** Decide who to involve and how to roll out your mobile initiative.
- **Chapter 5: Selecting Security Software: The 'Must-Have' Features.** Get the lowdown on the technologies that help you protect your data and your systems.
- **Chapter 6: Ten Questions To Help You Refine Your Strategy.** Use these questions as a useful checklist.

Icons Used in This Book

To make finding the information you need even easier, these icons highlight key text:

The target draws your attention to top-notch advice.

The knotted string icon highlights important information to bear in mind.

Watch out for these potential pitfalls!

Where to Go from Here

You can dip in and out of this book as you wish, or read it from cover to cover. It's a quick and easy read! Whichever way you choose, we're sure you'll find it packed with useful advice on how to ensure your mobile access or BYOD project is a success.

4

Chapter 1

Why Mobile and BYOD?

In This Chapter

- Assessing the benefits
- Considering the challenges to address
- Deciding if BYOD is right for your business
- Catching up . . . when the decision's already made

In this chapter, we look at some of the benefits and challenges that businesses face when considering the introduction of mobile access to corporate systems and data. We also consider the implications of Bring Your Own Device (BYOD) initiatives.

What's Mobile Access All About?

In today's fast-moving business environment, companies that provide their employees with rapid, convenient access to more of their corporate data and systems – via mobile devices – can gain a significant advantage over their competitors. Giving remote or mobile workers access to up-to-the-minute data and providing employees with the ability to upload

information to corporate systems has the potential to boost efficiency and business agility.

However, even with significant benefits on offer, there are some issues to address if your business's mobile access initiative isn't going to affect the security of your corporate systems and data, or result in the business falling foul of legislation and compliance requirements. No one wants to see the business being sued by customers and business partners – or the CEO being held personally responsible for any legal penalties . . . especially if you happen to be the CEO!

Just for starters, here are a few of the challenges that businesses face when considering the introduction of access via mobile devices:

- What are the implications of corporate systems being accessed from outside the corporate firewall?
- Should any corporate data be stored on the mobile devices?
- Is there a risk that the business could lose control over exactly where its data is?
- Are there potential legal penalties for the company and its directors?
- What can you do to prevent malware and cybercriminals gaining access to your corporate systems?
- How do you motivate your workforce to take sensible precautions to avoid legal and security issues?
- Can you ensure ongoing security of corporate data if a device is lost or stolen?

- Are there compliance issues associated with mobile access to your corporate systems and data?

Why Bother with BYOD?

With the recent growing interest in *BYOD initiatives* – whereby employees are allowed to use their own mobile devices for business communications – there's a lot of focus on the additional benefits that BYOD can offer for both employers and employees. If there are potential benefits to be gained, we need to take a closer look.

Knowing the benefits

For employers, BYOD offers potential benefits:

- **Reduced costs:** The business doesn't have to buy and upgrade mobile devices. The upgrade cycle for mobiles can be very short – especially if some of your employees 'simply have to have' the latest and greatest device as soon as it becomes available. BYOD can successfully disentangle the business from this costly merry-go-round.
- **Improved productivity:** With many users experiencing something that's worryingly close to a 'personal relationship' with their mobile devices, it's not surprising that employees generally appreciate being able to choose their own make and model. If the employee is already familiar with a particular device, that can aid efficiency when they're using it for work-related tasks.

For employees, BYOD can also offer advantages:

- **Better protection:** With responsible employers taking steps to safeguard their systems and data, employees can find themselves benefitting from mobile security software that helps to protect their own personal data on the device, with their employer picking up the cost.
- **Ease of use:** Employees can choose the device that they're happiest using – and that, in turn, can help to improve productivity even further for the employer!

When a new employee joins the business, there's a lot to learn. If they're able to use their own device to perform work tasks – instead of having to learn how to operate an unfamiliar mobile – they can hit the ground running.

Okay . . . what's the catch?

Before getting a little too carried away with the potential benefits and starting to regard BYOD as standard practice, let's take a pause. Yes, there are benefits. It's also true that, as workers move from one company to another, the 'BYOD habit' is likely to spread. So this BYOD juggernaut seems to keep gaining momentum and businesses feel growing pressure to roll out their own BYOD programme.

However, that doesn't automatically mean that BYOD is right for *your* business. It could be, if you come up with a strategy that ensures you can capitalise on the potential benefits – without suffering any of the pitfalls.

On the other hand, some businesses may do well to steer away from BYOD – perhaps because of the industry sector they operate within, the type of data they handle, the regulatory codes that apply to them . . . or all these factors.

BYOD brings the following challenges:

- The business has little or no control over the range of device types and operating systems (OSs) being used, so the task of managing all those different devices could add to the management overhead.
- There's a greater risk of compromised security on the device (from infected data, attachments or apps), which can lead to infections or attacks on the rest of the corporate network.

If the business is going to support the use of absolutely any mobile device that the user chooses, that could absorb a lot of resource. Compared with a policy of corporate-owned devices – whereby a small selection of devices and operating systems are assessed and rolled out – BYOD brings a plethora of devices and OSs that all have to be enabled and secured. Some clever technologies can help you cope with this, but be aware of what you're getting into.

BYOD could mean the business has to support the use of iOS, Android, BlackBerry, Symbian, Windows Mobile and Windows Phone – including different releases for each of these OSs. Plus there's the potential for new OSs in the future, and they'll all have to be supported too.

Would You Say No to the CEO?

BYOD has set the cat among the pigeons in ways that no other technology roll-out has previously. When a company upgrades its fleet of laptops, desktops or servers, the IT department obviously plays a major role in the project – vetting potential suppliers, assessing the performance of competing technologies, setting up support and maintenance contracts, and managing the roll-out. Even though adopting a new mobile access strategy has many technical, support and security requirements, the initial impetus behind the introduction of new mobile technologies has often been a lot less formal.

Consider the situation where the CEO gets the latest 'whizz-bang device'. This is a device that's so cool, it's cryogenic! Now, wouldn't it be great to use that device to access business systems? 'This could revolutionise the way we do business,' they say – and in no time, the mobile access project is off and running.

Bowing to the inevitable

Now, is there anyone – and we mean anyone who values their career – who's going to say, 'No way, José'? Even if your CEO just happens to be called José, it could be a career killer (and if his name's Frank, he might wonder whether you've been working a few too many hours). Even a simple 'Whoa . . . hold on, there's important stuff we need to consider here' could be beneficial. But who's going to deny the CEO's wishes? After all, he does have a valid point: this device could do a lot to revolutionise key business processes and boost efficiency.

Getting it all back on track

So, in our scenario, the company and the IT team have to find a way of making it happen. But that can leave the IT team and the security guy playing catch up. The horse has bolted – now we've got to see about building a stable. The next chapter helps you consider what's at risk . . . and how you can get it all back on track.

Chapter 2

Exploring the Scary Stuff: Malware, Loss and Other Risks

In This Chapter

- Discovering the scale of the security risks
- Understanding the nature of different threats
- Keeping safe when using Wi-Fi
- Looking at what the future holds

Few businesses would contemplate running their IT infrastructure without adequate security technologies in place. However, in general, businesses and their employees are much less aware of the security risks and the issues associated with corporate use of mobile devices. After all, it's just a phone or a tablet – and everyone's lost one or two of them at some time . . . right?

Well, that may be so, but today's smartphones and devices are a million miles away from the old clam-shells or those brick-like phones that took two people to carry. If someone left a phone in a taxi cab in 2003,

they lost a bunch of contact details and that was an inconvenience . . . but that's all they lost. It wasn't as if the security of their employer was compromised in any way!

But fast-forward to today, and it's a very different story.

Is That a Computer in Your Pocket?

Your mobile device is really a powerful computer that's capable of storing a massive amount of data. If you use it for work tasks, some of the data on your phone or tablet could seriously compromise your company's security if that information fell into the wrong hands. With all your passwords stored on your device, criminals could get direct access to your personal information and direct access to the company's corporate systems.

The main security risks include:

- Data loss – as a result of a device being lost or stolen.
- ID theft – if a criminal steals your device and logs into your online accounts.
- Malware that steals information.
- Leakage of information, via bogus Wi-Fi connections.

Where did I put my phone?

Modern mobile devices are so small and slim that it's easier than ever to lose one. For some users, it's almost an inevitability. So all users should take some simple precautions. Is it wise to rely on just a simple PIN when a pass-phrase could be more secure?

Precautions and technologies can help in the event of a device being lost or stolen. It's possible to store data in a form that's totally unreadable if your phone is stolen. In addition, special mobile security technologies can give you remote access to your missing phone, so you can run a series of anti-theft and protection features on the device. There's more on that later in the book (but if you want to skip ahead to see how it's done, see Chapter 5).

Mobile Malware Madness

The recent rise in the use of smartphones has resulted in a corresponding rise in the activities of the bad guys who skulk around looking for opportunities to rip off innocent victims. Because we're all using our phones to do more – like shopping, banking and work tasks – cybercriminals are targeting smartphones.

Cybercriminals! They may sound like exciting beings from a sci-fi thriller, but in reality they're well-funded professional teams that are constantly developing ever more sophisticated ways to steal your money and your identity . . . and launch targeted attacks against businesses.

Even though the first mobile malware was found back in 2004, growth in malware attacks was fairly slow until 2010. But then . . . KABOOM! In 2011, the volume of new malware that was targeting mobiles exceeded the entire volume from the past six years. And 2012 saw another six-fold increase in mobile malware. Now it's obvious that mobile devices have become a prime target for criminals and malware.

Don't let your guard slip

Why the rapid increase in mobile malware? It's partly due to the rise in the number of smartphones that are in use, partly down to the things we use our smartphones for and partly because some of us are a bit guilty of letting our guard down. That last point is something we can help you to address.

Devices that are used for online banking, shopping and accessing employers' systems are bound to attract the attention of the bad guys. So the risks are growing. However, many businesses that wouldn't take security risks inside their IT network are regularly letting those innocent little handsets gain access to precious data . . . without sufficient thought about what happens to the information they access and the passwords they use.

Is any mobile safe?

Criminals are currently targeting some mobile platforms much more than others. Although there are definitely risks that affect Apple and BlackBerry devices, the largest recent increase in threats has been in those attacks that target Android devices. So, do Apple and BlackBerry users need to worry?

Put simply – yes!

Consider the world of laptops and desktops. A lot of people and businesses felt safer using Macs rather than PCs. However, that past complacency about the possibility of attacks against Macs was clearly a grave mistake. There have been many well-documented instances of malware attacks that have specifically targeted Macs – and the number of attacks is growing.

Similarly, for mobile devices it can be a mistake to rely on one particular platform being safer than another, and to keep on relying on that, and do nothing about security. As soon as cybercriminals spot an opportunity – and realise that the guard is down for a specific platform, as a result of some misplaced sense of security – that's the time the bad guys are likely to pick a new target.

It's happened in the past. Before the recent rise of Android threats, the main focus of attack was the mobile version of Java. Before that, the targets were Symbian-based and Windows CE-based devices. So it's a fast-moving, fluid situation – and businesses need to try to stay one step ahead of the bad guys.

Also, remember that the risk isn't just from malware. The data that's held on any lost or stolen device is vulnerable if the device isn't secured. Furthermore, a criminal can steal data on any device if a user connects to an untrusted Wi-Fi network.

When a user jailbreaks or roots their mobile device – in order to unlock the device for use on another carrier's network or to remove limitations on the range of applications that can be run – it's a little like removing the front door from a house. Jailbreaking or rooting a

device strips away the security. At that point, it doesn't matter which OS the device is running. The risk is real. Do you want jailbroken devices accessing the corporate network?

Major Mobile Malware

Currently, three main types of mobile malware exist:

- Trojans
- Adware programs
- Botnets and other hacker threats

SMS Trojans

Despite the name, there's nothing classical or mythological about this kind of malware. They're a particularly sneaky way of taking money from the person or business that pays the phone bill. After a device has been infected by an SMS Trojan, the criminal generates revenues by making the device automatically – and silently – send multiple text messages to premium rate telephone numbers. Okay, so that's not necessarily going to break the bank, or your business if it's the company that pays the bill. But it's still worth protecting your devices against these attacks, especially as they could potentially damage the reputation of the business.

Other Trojans

The two other common types of Trojan are backdoors and spy programs – and both are designed to siphon data from mobile devices. Backdoors provide an attacker with remote control over the device – allowing the attacker to do virtually anything with it.

Spy programs 'leak' data from the phone to the attacker – for example, personal messages or the serial number of the device.

That ad that drives you mad

Adware programs sound pretty harmless, but the problem with them is that they don't just display adverts . . . they also carry out additional, unauthorised functions. For example, they can do things like change the user's browser start page without the user's permission.

Botnets

We've saved the worst till last. This group of threats extends the backdoor concept to allow remote control of mobile devices en masse – sometimes tens of thousands at a time.

Botnets are networks of security compromised devices that are exploited by hackers to work as part of a network that spreads malware and attacks. This is one network you don't want your devices joining.

Sometimes mobile threats are hybrid attacks that combine the functionality of a backdoor, an SMS Trojan and a bot.

Because targeted attacks on companies often start with hackers gathering intelligence that can help the criminal to tailor and set up their assault against a specific company, hacker and botnet attacks are a source of grave concern. There are many well-documented instances of these types of attacks being launched via desktops and servers. Now, with a lot of businesses failing to ensure adequate security on their employees'

mobile devices, criminals are seeing mobiles as an easy – and increasingly productive – means to gather information and gain access to the corporate network.

Wi-Fi, Wi-Fi, Wherefore Art Thou, Wi-Fi?

When employees access public Wi-Fi networks – at airports and hotels, for example – there's a risk that data and passwords can be *sniffed* (that is, captured illicitly by criminals that are connected to the same Wi-Fi network). The user may only be logging in to Twitter or Facebook – but if their passwords are captured, there's a lot of information that could benefit the criminal.

More and more criminal gangs are happy to 'play the long game' and carefully exploit the personal information that they've captured. Often the capture of personal data is just a means to an end. With this information, the criminal can assume the employee's digital identity and then communicate with the employee's unsuspecting colleagues. When these colleagues receive communications that look as though they're from the victim, what are the chances of them being on their guard and not revealing corporate system passwords or other valuable information? These highly targeted phishing attacks are known as *spear phishing*.

Are they who they say they are?

Spear phishing attacks can be highly sophisticated. There's a lot of information that people willingly post

on social network sites – including details of business trips, holidays and family. So the attacker can slip a lot of personal knowledge into their communication with the victim's colleagues. A message that starts by asking the contact how their business trip to Vienna went last week – and then goes on to ask the contact to click on a link and input their corporate network login – can be very convincing. Yet all this has resulted from an employee accessing a legitimate public (and therefore insecure) Wi-Fi hotspot.

And criminals don't just sniff information that's sent using a legitimate Wi-Fi network. They also create fake Wi-Fi hotspots. These can be set up virtually anywhere. Criminals will even park up in a target company's car park, set up a hotspot – from the comfort of their car – and then set about sniffing passwords from any unsuspecting employee that uses the bogus hotspot.

Surfing the web using a public Wi-Fi connection may be fine, but it's best to avoid signing into specific services that need you to input your confidential passwords or other sensitive data.

A lot of people use the same password for multiple accounts. If a criminal manages to sniff a user's password for a social network, that could be all they need to gain entry to the corporate network (and any other online account belonging to the victim). Bingo . . . the criminal doesn't even need to use a spear phishing attack.

Looking to the Future: Could It Get Any Worse?

Plenty of security threats exist in the here and now – but what could the future hold? It's a safe bet that the nature, sophistication and range of threats that exploit mobile devices are likely to increase the danger even more. As the use of smartphones and tablets continues to increase . . . so will the cybercriminal's interest in exploiting any weaknesses in defences. If businesses routinely fail to devote sufficient effort to securing mobile access, criminals will continue to regard mobile as a path of least resistance for attacks.

Drive-by dangers

For laptops and desktops, there's been a marked rise in the number of attacks that exploit unpatched vulnerabilities that are present within commonly used applications. These often take the form of *drive-by attacks*. In this type of attack, the user unwittingly visits a web page that just happens to have been compromised and contains a malicious script. When the user views the web page, the script executes automatically and uses an unpatched vulnerability – within an application on the user's computer – in order to install itself on the computer. Such attacks are routine on desktops and laptops. So far, we haven't seen any of these browser-based drive-by attacks targeting mobile devices, but it's probably only a matter of time before we do.

Red October

The Red October attack was one of the first targeted attacks that not only gathered information from computer systems but also harvested data specifically from mobile devices. Mobile devices are going to feature in more targeted attacks that don't just access the business's network . . . the attackers will also take steps to escalate their rights, access confidential documents and gain access to databases and contact information. Mobile devices are likely to become a routine aspect of cyber-espionage attacks on businesses.

Chapter 3

Knowing the Legalities

In This Chapter

- Understanding your security obligations
- Working out what's 'reasonable' in the eyes of the law
- Defining the core elements of a mobile strategy
- Thinking about licence issues

No matter how large or small the organisation may be, every business stores data that it can't afford to see falling into the wrong hands. Some businesses make the mistake of thinking that because they don't sell to consumers, they don't have to comply with any regulations regarding the security of personally identifiable information. This is rarely the case. All businesses are likely to hold personal data on their employees. If the security of that data is compromised, an expensive lawsuit could follow.

Ask yourself, does your business store any of the following:

- Customer lists and contact information?
- Sales and marketing data?
- Intellectual property, know-how and designs?

- Business bank account details?
- Personally identifiable data on employees?

If a business is working on a joint project with another company, it's likely that each of the parties to the project will be holding confidential information that's owned by the other business. What would be the consequences if any of that data was lost or stolen as a result of negligence? At best, it would be the end of a beautiful relationship. At worst, it could result in a costly lawsuit, the end of that beautiful partnership and a loss of reputation throughout the industry!

So, Where Does the Buck Stop?

It's not something that anyone enjoys contemplating (except maybe a few ambitious young lawyers), but it's wise to give some thought to the legal risks and what could be at stake. If your mobile strategy goes badly wrong, there's a chance that the following could be subject to legal action:

- The business itself.
- Directors and other senior personnel.

Any person or entity that suffers damage as a result of negligence that leads to a loss or leakage of data could bring a legal action. This could include customers, employees or other companies that have partnered with you on specific projects.

Any shareholder or investor may have an opportunity to sue – the business or its directors – in the event of security breaches.

The full cost of legal action can go much further than the sum of any compensation, fines and legal expenses. Bad publicity can severely damage a company's business reputation.

Regulation and Compliance

Quite apart from the risk of civil actions, a whole raft of regulations and legislation might apply to your business. Obviously, the nature and scope of any regulations vary from territory to territory and according to the type of business you have. However, at the very least, they're likely to include a set of general rules about data protection. In addition, specific requirements and compliance issues will apply if you're in a tightly regulated industry – such as financial services or healthcare.

If your company operates in several territories, it's advisable to seek advice on the legal requirements that apply in each territory.

Some jurisdictions have specific rules on whether data is allowed to cross borders. Check whether it's okay to let an employee in one country access data that the business stores on systems that are in another country.

In some legal cases, senior personnel can be held to be personally liable – with the possibility of heavy fines or even custodial sentences.

Where's the legal precedent?

Normally, when companies try to get their heads around the legal requirements associated with introducing new technologies into the work environment, it's helpful to

be able to refer to existing laws and the results of specific court cases interpreting those laws. These can be a valuable source of guidance on what's acceptable. Sadly, when it comes to mobile access to corporate data – or the use of BYOD – there are no specific laws and virtually no relevant court cases that businesses can reference.

If the worst comes to the worst, and your company does find itself in the unfortunate position of being sued or prosecuted, what's your line of defence going to be? In the absence of specific laws, your best bet could be the ability to prove that the business took reasonable measures to avoid data loss or leakage.

Does 'reasonable' put unreasonable demands on business?

So, exactly how does the law define *reasonable*? That's a tricky question and the answer varies according to:

- Your industry sector.
- The value of the information you hold.
- The potential consequences of data loss.
- The level of investment required for preventative measures.
- What other businesses in the same situation are typically doing.

If your business holds vast quantities of valuable or sensitive information – and there's the potential to cause significant damage to other parties if the security of any of the data is compromised – that fact will

greatly influence the court's view. In this situation, most judges are likely to have a tough time deciding that the business acted reasonably if the business withheld a few thousand dollars of investment in some security measures that are typical within the specific industry sector. Similarly, if such a company has put little or no effort into training its staff on specific security considerations, the courts would be likely to take a dim view of this approach.

Ask yourself, given the type and value of the data your business holds – and the cost of suitable preventative measures – has the business acted reasonably in order to:

- Protect its employees?
- Protect its customers?
- Protect its business partners?
- Comply with general and specific regulations?

A word of caution: BYOD is a relatively new phenomenon. That means:

- There's little or no consensus on best practice within any one industry sector. So don't be surprised if the courts take a demanding view on what's 'normal security practice' within your industry.
- Security practices and normal expectations of reasonable security precautions are changing rapidly. *Reasonable* is a moving target – so make sure your business keeps the evolving nature of reasonable in its sights.

Taking the First Steps Towards Being Reasonable

We look at the details of mobile and BYOD strategy a little later in the book (or you can take a look now, in Chapter 4). For now, there are some basic strategy steps that help you keep ahead of the law, and we outline them in the next sections.

Getting started

First, you'll need a security policy. If you're one of the diligent businesses that has already generated a detailed, written security policy and communicated it to your employees, you need to do two things:

- Take a bow – because many companies, of all shapes and sizes, have yet to do what you have done.
- Devote some effort to thinking about how you need to adapt your security policy to cover mobile and BYOD.

On the other hand, if your business has yet to define a detailed security policy, now is the ideal time to make a start.

It's all in there – if you can find it

Crafting and finely honing your security policy pays dividends in the long run. Although it's debatable whether the perfect policy can ever be drafted, don't let that be an excuse for not giving it your best shot. A lack of the perfect policy isn't necessarily the area in which most companies fail.

Some companies put the hard yards in, devise a detailed security policy and then write it up in language that a Harvard lawyer would have a hard time deciphering. If an employee handbook runs to 1,000 pages of dense, impenetrable text that's full of jargon and flowery language – but the specifics of the BYOD security policy are hidden away on pages 836 to 849 – we can all make a guess at the court's views on whether the company has acted reasonably.

So, aim to write up your policy in terms that are easy for every employee to understand. Then clearly communicate the policy in a way that ensures employees are going to take notice of it.

Security is like housework: it's only meaningful if you repeat it at regular intervals. You need to update your security policy to reflect changes in the way you do business or any changes in the nature of the risk to your business.

Training and raising awareness

The value of training should never be underestimated. Businesses that recoil at the idea of spending money on training should pause and consider the potential costs that could result from a failure to provide adequate training. Okay . . . now those training costs don't look quite so onerous!

Again, how much training you need to conduct depends partly on the value and nature of the data that's at risk – so you need to provide a level of training that passes the legal *reasonable* test, given the nature of the data and the industry sector that the business operates within.

Simply developing a security policy and then not putting sufficient effort into communicating it to your employees – and raising awareness of the issues – is unlikely to pass the *reasonable* test.

Training needn't be prohibitively costly. In some cases, it's appropriate to hold formal training courses and also test employees' knowledge at the end of the course. However, for other businesses, maybe just providing access to a short training webinar is enough.

Whichever training method you use, think about how often you should remind employees about the policy. A simple email that's sent monthly or quarterly could be an ideal way to reinforce specific points. If you can make the email eye-catching, humorous or memorable, that can help to get key points across to employees.

Meet 'The Enforcer'!

Think about how you're going to enforce your security policy. Enforcement may sound a little dictatorial, but it's just a matter of approach. No one's advocating beating employees over the head when they fail – no matter how tempting that may seem when they've missed their sales targets or they're late getting you that monthly report! For one thing, you don't want to discourage anyone from sharing details about innocent mistakes they may have made or security problems they've encountered.

The most important aspect of enforcement is taking the necessary actions to ensure that security violations simply don't happen in the first place (that leads us back to making sure that the security policy is reasonably concise and easy to understand – plus all employees benefit from adequate levels of training). So, as with most things in life, when it comes to enforcing security policies, prevention is far better than cure.

What's the worst that could happen?

The good news is, in the vast majority of cases, when an employee violates part of your security policy it's likely to be as a result of ignorance, not malice. Wait a minute! This means the power to prevent the violation actually lies in the business's hands. Do we hear shouts of 'Was there adequate training and a clearly written policy'?

Extreme circumstances do arise. So the final element in an enforcement process sees the business defining the penalties that can apply when an employee deliberately or repeatedly violates the security policy. Is it a case of delivering escalating levels of warnings for each transgression – perhaps culminating with the withdrawal of mobile/BYOD access? If access has to be withdrawn, will the employee still be able to perform their work duties? If not, does the company's procedure set out what should happen next? All these considerations should be clearly set out and communicated, or they're less likely to be legally enforceable.

Have you paid for that?

Here's a legal issue that a lot of companies fail to take account of: software licences and the effects of BYOD access. The business may have diligently ensured that it has sufficient licences for every item of software within its network. However, do those licences allow the applications to be remotely accessed via BYOD devices? Some licences permit such access and some don't. Avoid making any dangerous assumptions. Check the fine print, or the business could face some severe penalties.

Stepping away from the world of mobiles for a moment, it's also worth considering the case whereby an employee uses their own laptop to complete work tasks when they're at home. If they're using their own 'Home and Student' version of the necessary application software, that licence probably excludes commercial use. If the business is deemed to be encouraging employees to work at home – but isn't providing the properly licenced tools to do the job – the company could be subject to penalties.

Chapter 4

Finely Tuning Your BYOD Strategy, Policy and Guidelines

In This Chapter

- Deciding between mobile access, BYOD and CYOD
- Involving the relevant stakeholders
- Managing employees' expectations
- Providing ongoing advice for users

In Chapter 3, we took a look at some of the first elements for a mobile access strategy, and how they relate to legal considerations. In this chapter, we drill down into the detail. But first, a pause . . .

Even though interest in BYOD may seem to be all-pervasive, each business really needs to consider whether BYOD is right for them – in their specific circumstances.

Starting with a Pilot

Rushing headlong into a hasty roll-out of any new technologies can often be a source of regret. Even if you decide that BYOD is absolutely right for your business, it's worth taking things at a measured pace. Whereas many early adopters rolled out BYOD in a 'big bang' project across their entire business, other companies are already learning from those mistakes. Controlled pilot schemes are becoming the order of the day because they give the business an opportunity to iron out any issues while the BYOD user group is relatively small.

If you choose to run a pilot scheme or test programme, it's a good idea to make sure you let it run for a suitable length of time. Then allow a period for defining further updates to your security policy and protection measures, after the pilot scheme has been completed and before the full roll-out begins.

The ABC of BYOD and CYOD

Some businesses are stepping back a little from BYOD and considering CYOD (Choose Your Own Device) instead. Under a CYOD scheme, the employee doesn't have a totally free choice over the device they use. Instead, the business issues a list of approved devices, and if the employee wants to gain access to corporate systems and data, they have to use one of the listed devices.

Many of the benefits of BYOD simply don't apply to CYOD. If a business implements CYOD, it's likely that a

high proportion of employees will choose to operate a different device for personal use – and if that device is still brought into the work environment, that can raise security issues, even if it's not given access to corporate data. Only your business can decide whether CYOD is a viable option that will meet your objectives.

For companies that are operating a CYOD initiative, it's still essential that policies and checks are in place that deal with the presence of personal devices within the work environment. Of course, it's easy to prevent employees from using their personal devices to gain access to the corporate network, but there are still issues to cover. For example, will personnel be permitted to access the corporate Wi-Fi using their personal mobile devices? If Wi-Fi access is allowed, should the business implement automatic controls that prevent visits to social networks during working hours?

Who's Involved in Your Mobile or BYOD Roll-out?

The short answer is . . . everyone. Well, perhaps not everyone, but probably at least one representative from every significant stakeholder group within the business. It's tempting to get the legal department to look at the legal aspects and draw up the policies, and then just get the IT guys to rubber-stamp the way ahead. Big mistake!

Every stakeholder group tends to look at the issues from a different perspective. That's a good thing. Aggregating the output from all those perspectives is likely to give you a much more workable strategy that takes a three-dimensional view of all the issues.

- Sales directors, marketing directors and field service directors can all play a valuable role – by defining which corporate applications and data their remote workers need to access when they're out in the field.
- The legal team will provide the expertise in helping to ensure no legal or compliance issues exist.
- The Human Resources (HR) team can assist with all aspects of employee relations – from helping to develop new policies to training and amending employment contracts. (See the next section for more info on the HR team's role in the roll-out.)
- The IT team will advise on technologies – including security. Their knowledge and skills will be vital during the roll-out, and they'll be the team that has to deal with any technology or data security issues that result from the wide range of mobile device types that employees could use to access corporate systems.

Take me to your leader

The HR team is probably very well placed to take a leading role in helping to refine key elements of your mobile and BYOD strategy. After all, they've got a wealth of experience in developing policies, documenting

them – in an employee-friendly manner – devising training courses and motivating employees to follow best practice.

HR personnel also have the most enlightened attitude to defining the objectives that lie behind the policies and guidelines you need – and the objectives behind the necessary training. They can take care of what's required to amend employment contracts and set up disciplinary rules for security breaches. For this latter task, they're the team that won't purely focus on punishing transgressors. Your HR personnel understand that the aim is to give your employees all the tools and information they need to make sure issues don't arise, so there's less need to apply penalties.

However, it's not a perfect world, so you'll still need their help in defining how transgressors will be dealt with. Again, the HR team is likely to be very well versed in how to draw up fair and equitable disciplinary procedures.

It's worth noting that if policy violations occur, that could be the perfect opportunity to reassess the company's policies. Perhaps it wasn't the employee's fault – perhaps the policy is inadequate or needs a few adjustments.

As we discuss in Chapter 3, training – and possibly ongoing refresher courses and reminders – are a vital element in ensuring your BYOD initiative is successful, secure and less likely to land the company in legal difficulties. When it comes to devising and running training programmes, who's better qualified than your HR team?

Making it clear that access isn't guaranteed

Whenever a business rolls out a new work method, it needs to take care to ensure that any changes to work processes can't be interpreted as a fundamental change in employment terms and conditions. Obviously, the HR team is your in-house source of expertise in avoiding such issues and ensuring that the introduction of new technologies doesn't create a sense of entitlement.

The BYOD programme should be regarded as something that the company can offer to specific job roles – but it doesn't have to offer the programme to everyone that operates within those roles. Similarly, the business needs to express the rules in terms that make it clear that the privilege of being part of the BYOD scheme can be withdrawn, and that participation in the BYOD initiative does nothing to bring about a fundamental change in the employment relationship.

Clarifying . . . not contradicting!

Having considered all the stakeholders to consult throughout the initial stages of defining policies and strategy, and then rolling out your mobile access or BYOD programme, let's also spare a thought for any confused employees who have legitimate queries even after they've completed all the necessary training.

Providing a single point of contact that's able to offer informed advice is a great move. What you really want to avoid is the situation whereby an employee raises a query with the marketing department and gets one answer . . . raises the same query with IT and gets a

slightly different answer . . . and consults the HR team and gets a third answer.

Your single point of contact may include representatives from different stakeholder groups, so each can focus on queries that fall within their specific remit. However, by providing a single email address for queries – and making sure your employees are aware of it – you provide one conduit for all questions.

Policies, guidelines and contracts that aren't clearly understood – or are subject to contradictory advice from different expert contacts within the company – can be totally unenforceable if legal issues arise.

Chapter 5

Selecting Security Software: The 'Must-Have' Features

In This Chapter

- Defending against the malware attacks
- Simplifying mobile security, including Mobile Device Management (MDM)
- Protecting data on lost or stolen devices
- Making it easier to manage security – across all your endpoints

When it comes to security, mobile access brings a need for a new mindset. In the past, it was easier to trust any device that was within the corporate network. Now, with mobile devices and BYOD subject to the security risks and attacks that are present in the outside world, how can we trust the behaviour of those devices when they're operating within the corporate network?

Mind the Gap!

Whereas previously all you had to do was protect your perimeter with a world-class firewall and then ensure you had suitable security provisions for every endpoint inside that perimeter, security is no longer that simple. Mobile access is the big game changer – and it can create a few security gaps.

In reality, part of your security perimeter is still around your business, but part of it is also around each user. There's an invisible boundary around every one of your mobile users, and it needs to be secured.

Here comes the cavalry

Adding any new type of endpoint to the corporate network has the potential to increase the burden on the IT department – especially when it comes to security. Mobile brings its own unique challenges. In Chapter 2 we look at the various threats . . . and there are a lot of threats and security risks for the unwary. Combine these threats with the dispersed nature of the business's security perimeter and it all gets a bit scary.

Well, it would be scary if there was nothing we could do to counter those risks and defend those perimeters. Luckily, the good guys – in the form of security software vendors – have more than a few clever tricks to help you defend your device, your data and your corporate systems.

There are some really great technologies that help to protect your corporate data and keep malware off your

network. Whereas some elements of mobile security have been around for a little while, new technologies have been unveiled only recently. So here's a brief introduction to the features and capabilities that you might like to ensure are included in the mobile security solution you choose for your business.

Anti-malware

The rapid rise of malware and other threats that are targeting mobile devices means that businesses need to install anti-malware software that's capable of protecting mobile devices against the very latest viruses, spyware, Trojans, worms, bots and other malicious code. Solutions that just use traditional, signature-based anti-malware technologies are no longer enough to guarantee adequate protection. So it's a good idea to look for a security solution that includes heuristic analysis – as well as signature-based protection – so that it's capable of defending against documented malware and also those new threats for which a signature doesn't yet exist.

Rigorous anti-malware solutions also include anti-spam technologies, in order to filter out unwanted calls and texts that try to reach the mobile device. So that means fewer distractions for your workforce.

Anti-phishing features are also vital in helping to prevent inadvertent visits to fake or fraudulent websites that try to steal information.

Benefiting from a hybrid solution

Hybrid anti-malware solutions – which combine anti-malware technologies that run on your devices, plus cloud-based services – can deliver an even higher level of protection. By sending up-to-the-minute data to your systems and devices about the very latest emerging threats, cloud-enabled services can work with the signature-based and heuristic anti-malware technologies that are running on your device . . . so you benefit from multi-layer security.

Here are a couple of additional things to look out for in your anti-malware solution:

- How often are the anti-malware databases updated? Frequent, small updates help to ensure you're protected against new threats, without placing an unnecessary load on your systems.
- Does the solution let you run on-demand scans, as well as scheduled scans?

Mobile Device Management (MDM)

An integrated MDM solution can help to make it easier to do a whole host of administration and security tasks across a range of different devices and operating systems (OSs), including:

- Deploying the security agent onto each device – with features that let you remotely provision security software Over the Air (OTA).
- Simplifying the implementation of security policies on the devices.
- Separating personal and corporate data on each device – and enabling 'selective wiping' of corporate data, without deleting the user's own personal data.
- Enabling the use of encryption technologies on the devices.
- Controlling how applications are launched and used.
- Managing access to the web.
- Detecting the presence of jailbroken devices.
- Protecting data when a device is lost or stolen.

Containerisation

Now, this is a very clever way of solving the issues that can arise from having both personal and corporate data stored on a BYOD mobile. Some security solutions let the business set up special containers on each device – with all corporate data being stored in the container. The administrator can then set specific policies for the data that's held within the corporate container on the phone. For example, all data within the container can be automatically encrypted.

When an employee leaves the company – or if a device is lost or stolen – containerisation helps to cover an

important issue. If the corporate data has been stored in a container on the mobile device – so that it's totally separate from the user's personal data – it's easy for the administrator to remove (selectively wipe) the corporate data without affecting the user's personal information.

Encryption

Encrypting sensitive data is a great way of ensuring that any information that's stored on a mobile device could be virtually useless to any thief. Many mobile devices include data encryption technologies – so it's just a matter of ensuring that your chosen mobile security solution has MDM features that make it easy for your administrators to manage those in-built encryption features.

Because jailbreaking a phone can seriously compromise protection, some mobile security solutions actively seek out jailbroken devices that employees may be using. The security software then prevents the jailbroken phone from gaining access to corporate systems and applications. There may also be a feature that lets you delete all corporate data from the jailbroken device.

Application Control

Application Control features are a powerful way of controlling the launch of applications. Your administrators can set up a blacklist of applications and ensure that none of these applications are allowed to run on the user's mobile device, but all other applications are able to launch.

Using Application Control to set up a Default Allow policy lets any application run on the user's device, unless that application is on the blacklist.

Setting up a Default Deny policy blocks all applications from running, with the exception of those apps that are on the whitelist.

Web Control

Web Control gives the business the ability to monitor and filter users' browser activity – often the control can be selected according to category, content or type of data. The company's systems administrators can permit, prohibit, limit or audit users' activities on specified websites or categories of sites.

Help, My Phone's Been Stolen!

We all know that feeling, deep in the pit of the stomach, when we've lost something precious. Well, just imagine how you'll feel if your mobile device is lost or stolen – and it's crammed full of confidential corporate information. How's that going to go down with the boss?

Fear not. If the business has had the foresight to invest in a security solution that includes anti-theft features, there's a lot that can be done to remedy the situation and prevent corporate data and systems being illegally accessed.

Blocking your missing phone . . . and wiping data from it

First there are remote lock capabilities. So you can send your phone a special text message that blocks the

use of the device so that the thief can't access data or applications on the mobile. Some security solutions even let you display a special message on the phone's screen, so you can appeal for the phone to be returned.

If you're convinced that this time your phone hasn't just slipped under the sofa cushions, some security solutions give you remote access to a data-wiping function that can totally delete selected data sets on the phone – or delete all data and reset the phone to its default factory settings. So you may have lost the handset, but you'll be able to prevent the bad guys from exploiting any data that was on your phone.

Finding your phone

What about actually trying to locate your phone? There are even solutions that give you details of the device's approximate location – using GPS or Wi-Fi connections in order to calculate the phone's whereabouts.

Of course, the thief may have wasted no time in changing the SIM card in your device. Again, technology has the solution: some security products send you a message with the device's new telephone number, so you can still remotely access any blocking, locating and data-wiping functions.

Putting It All Together

Security software is an essential element in helping to keep corporate information safe and secure. However, IT security – vital though it may be – isn't really part of most companies' core business activities. So the less time your IT team has to spend configuring, deploying and managing mobile security, the better for your business.

Try to find a security solution that offers:

- All the security features you require – so you're not faced with having to integrate or manage different products from different vendors.
- Tightly integrated mobile security and comprehensive MDM that simplifies management tasks – so you can devote more resource to your core business activities.
- High levels of integration and interoperability across security for all endpoints . . . not just mobile.
- The ability to set universal policies across all endpoints, instead of having to set up individual policies for individual endpoints.
- A single, unified control console for all protection technologies.

For any IT security solution, ease of use is vitally important. If your mobile security solution is time-consuming to use, will it be used to the fullest extent? Any software that adds a layer of complexity has the potential to detract from your security, and introduce security gaps.

Chapter 6

Ten Questions to Help You Refine Your Strategy

In This Chapter

- Making sure your strategy covers all the bases
- Assessing the risks and the rewards
- Checking everyone's on board

Here are ten questions that can help you to refine your mobile and BYOD strategy:

- Is mobile access necessary?
- What are the potential benefits of mobile access for your business?
  - Improved business processes?
  - Productivity gains?
- Which sections of your workforce need mobile access, and which data or systems will they need to access?
- What sensitivities are there around these systems and data?

- Could BYOD offer additional benefits for your organisation?
- Should you provide company-owned devices for some sections of the workforce and allow BYOD for other personnel (depending on types of data/systems being accessed)?
- Have you conducted a full risk assessment – including legal issues – and generated a security policy?
- Who are the various stakeholders, and how is each affected?
- What level of consultation is required for each group of stakeholders?
- Will the business need to establish new HR policies?
  - New contracts for new employees?
  - Annexes to existing contracts, for existing employees?
  - Awareness and training programmes?
  - Procedures regarding negligence in data security?

With so much at risk if sensitive corporate data falls into the wrong hands – or cybercriminals gain access to your corporate systems – make sure your mobile strategy includes selecting a rigorous mobile security solution. Turn the page for more details. . . .

Security Your Business Can Depend On

With Kaspersky Lab's award-winning security technologies protecting your systems, data and mobile devices, the world of mobile access and BYOD doesn't have to be scary.

Kaspersky Security for Mobile combines powerful protection technologies and extensive Mobile Device Management (MDM) functionality in one tightly integrated solution that delivers rigorous, multi-layer security and far-reaching control and management capabilities. So it's easy to configure, deploy and manage world-class mobile security.

- Anti-malware
- Anti-spam
- Anti-phishing
- Mobile Device Management
- Containerisation
- Encryption Management
- Application Control
- Web Control
- Anti-theft features including:
  - Remote Lock
  - Remote Find
  - Remote Wipe
  - Remote SIM Watch

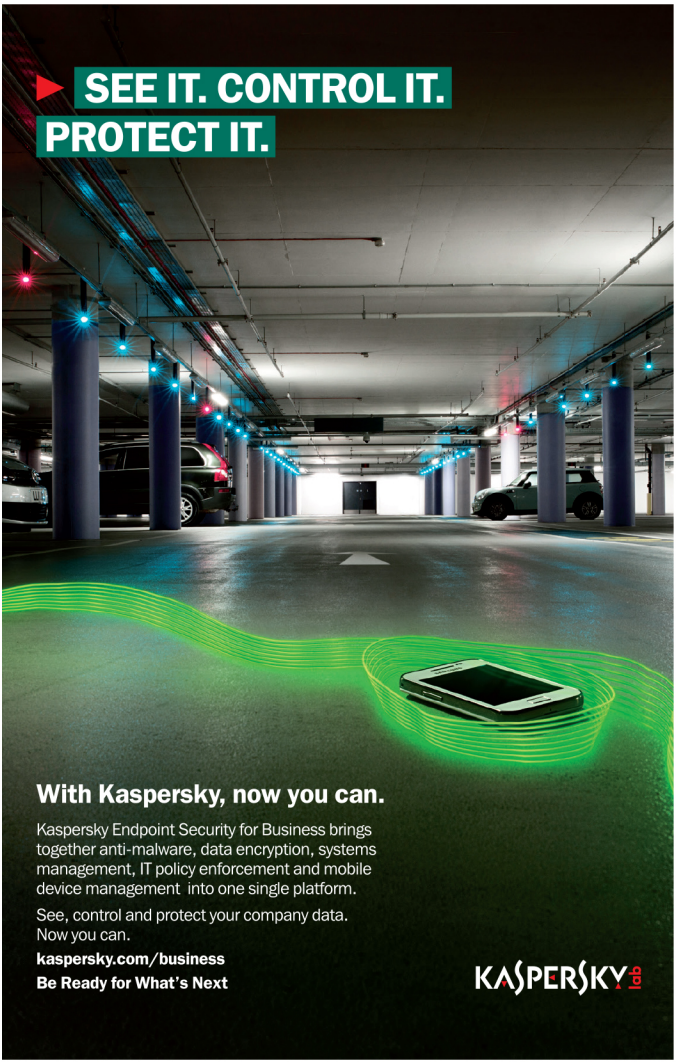
Kaspersky Security for Mobile is included in the following Kaspersky integrated security solutions for business:

KASPERSKY TOTAL SECURITY FOR BUSINESS

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT

To discover how Kaspersky can help protect every endpoint on your corporate network, please visit www.kaspersky.com/business-security.


SEE IT. CONTROL IT.
PROTECT IT.
With Kaspersky, now you can.
Kaspersky Endpoint Security for Business brings together anti-malware, data encryption, systems management, IT policy enforcement and mobile device management into one single platform.
See, control and protect your company data. Now you can.
kaspersky.com/business
Be Ready for What's Next
KASPERSKY lab

Essential tips on securing mobile and BYOD access for your business

Giving your workforce anytime, anywhere access to corporate systems and data can help everyone to do a better job. But there are security risks. Roll out a BYOD initiative and there can be additional benefits . . . and additional security issues. This easy-to-read book brings you tips on strategy, policies and legal considerations, plus guidance on vital security technologies that can protect your business and its reputation.

- ***Evaluate your options* – company mobiles: BYOD or CYOD?**
- ***Bespoke tailoring* – fit your mobile strategy to your specific business needs**
- ***Get 'buy in'* – so users do more to protect sensitive business data**
- ***Keep it all secure* – with easy-to-manage mobile security**

Open the book and find:

- **The business benefits mobile access and BYOD can deliver**
- **How to prevent costly legal and regulatory issues**
- **Guidelines on how to deliver and manage a secure BYOD programme**
- **How to select technologies that protect your business systems and data**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Georgina Gilmore has over 20 years' experience in the IT industry. Georgina is Director of Global B2B Customer Marketing at Kaspersky Lab. **Peter Beardmore** joined Kaspersky Lab in 2008 with extensive IT marketing and product management skills. He is Senior Director of Product Marketing.

FOR DUMMIES®
A Wiley Brand

FSC®
www.fsc.org
MIX
Paper from responsible sources
FSC® C013056

ISBN: 978-1-118-66242-7
Not for resale