Making Everything Easier!™

Sophos Special Edition

Securing Smartphones & Tablets

FOR DUMMIES®

Learn to:

- Protect your organization's smartphones and tablets
- Prevent mobile data loss and deploy secure apps
- Raise mobile device security awareness in your organization

Brought to you by

SOPHOS

Lawrence C. Miller, CISSP

Securing Smartphones & Tablets

FOR

DUMMIES®

SOPHOS SPECIAL EDITION

by Lawrence C. Miller, CISSP

John Wiley & Sons, Inc.

Securing Smartphones & Tablets For Dummies®, Sophos Special Edition
Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

ISBN: 978-1-118-17673-3 (pbk); ISBN 978-1-118-17737-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Table of Contents

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact `info@dummies.biz`. For details on licensing the *For Dummies* brand for products or services, contact `BrandedRights&Licenses@Wiley.com`.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Vertical Websites

Senior Project Editor: Zoë Wykes

Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Senior Project Coordinator: Kristie Rees

Layout and Graphics: Claudia Bell

Proofreader: Jessica Kramer

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Kathleen Nebenhaus, Vice President and Executive Publisher

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

Introduction

A new dawn of technology innovation is driving unprecedented changes in the way we live and work. Trends such as mobility and consumerization are defining some of the most significant changes in computing since the shift from mainframe computers more than two decades ago.

Smartphones and tablets feature ubiquitous connectivity with instant access to the biggest repository of humankind's knowledge (the Internet) and more processing power than NASA's control room during the first moon landing more than 40 years ago — literally in the palm of your hand!

Mobile devices enable busy professionals and home users to conduct business and manage their lives on the move. Furthermore, these devices are defining a whole host of new business models and services that will be a key catalyst to future economic growth for many organizations.

About This Book

But what are the key technologies driving the evolution of mobile devices, what's coming next, and what are the security implications of these trends and technologies? This book explores the mobility phenomenon and answers these important questions so that your organization can effectively secure your users' smartphones, tablets, and sensitive or confidential mobile data.

Foolish Assumptions

First and foremost, despite the title of this book, we assume that you know a little something about smartphones and tablets! We know, it's a bit of an oxymoron, but "Securing Smartphones & Tablets For Geniuses" just isn't that catchy! This book is written for executives, IT managers, and other

technical readers who need to know how to keep their organization's mobile workforce — with all their little gadgets, doohickeys, and assorted what-not's that go bump in the night (or on the sidewalk) — safe and secure. If this sounds like you, keep reading!

How This Book Is Organized

This book consists of five short chapters. Why five? Well, great things come in fives: fingers (so good you get five on each hand), oceans, senses, and the Spice Girls! Here's a brief look at the five great chapters that await you in this book!

Chapter 1: Mobility 101

We begin with an overview of mobile working and mobile devices. Here, we take a look at some mobility trends and their implications for individual users and organizations alike.

Chapter 2: Mobile Working — the Good, the Bad, and the Not So Good

In this chapter, we describe the many benefits of mobile working for organizations, as well as some of the risks and issues of mobile working.

Chapter 3: Keeping Your Mobile Devices, Data, and Applications Safe and Secure

In this chapter, you find out how to enable mobile working for your users while protecting your organization's sensitive data, network, applications, mobile devices, and employees.

Chapter 4: You Can Lead a (Mobile) Horse to Water

In this chapter, we discuss the importance of educating your users about the security risks associated with their smartphones and tablets — and how to stay safe. We tell you what your users need to know and suggest some ways to get the message to them!

Chapter 5: Ten (Okay, Seven) Tips for Securing Your Mobile Devices

Finally, in that classic *For Dummies* format, we end with an abbreviated Part of Tens chapter — this is, after all, a short book and destined to be a short classic!

Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important information. No smiley faces winking at you or any other cute little emoticons, but you'll definitely want to take note! Here's what you can expect:

This icon points out information that may well be worth committing to your nonvolatile memory, your gray matter, or your noggin' — along with anniversaries and birthdays!

You won't find a map of the human genome or the blueprints for the next iPhone here (or maybe you will, hmm), but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff legends — well, nerds — are made of!

Thank you for reading, hope you enjoy the book, please take care of your writers! Seriously, this icon points out helpful suggestions and useful nuggets of information.

Proceed at your own risk . . . well, okay — it's actually nothing *that* hazardous. These helpful alerts offer practical advice to help you avoid making potentially costly mistakes.

Where to Go from Here

With our apologies to Lewis Carroll, Alice, and the Cheshire Cat:

"Would you tell me, please, which way I ought to go from here?"

"That depends a good deal on where you want to get to," said the Cat — err, the Dummies Man.

"I don't much care where . . .," said Alice.

"Then it doesn't matter which way you go!"

That's certainly true of *Securing Smartphones & Tablets For Dummies,* Sophos Special Edition, which, like *Alice in Wonderland,* is also destined to become a timeless classic!

If you don't know where you're going, any chapter will get you there — but Chapter 1 might be a good place to start! However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is individually wrapped (but not packaged for individual sale) and written to stand on its own, so feel free to start reading anywhere and skip around! Read this book in any order that suits you (though we don't recommend upside down or backwards). We promise, you won't get lost falling down the rabbit hole!

Chapter 1

Mobility 101

In This Chapter

- Recognizing the explosive growth of mobile devices worldwide
- Understanding privacy and security issues
- Looking ahead to the future of mobile device security

Air, water, food . . . smartphones. Mobile devices are now an integral part of our lives, and it's hard to imagine life without them! We take it for granted that we can make calls from anywhere, send SMS (short message service) text messages to anyone, and work and access information from everywhere!

Mobile device technology is moving forward at an exponential rate and enabling us to do more and more every day, both at home and at work. From accessing our e-mails on planes, trains, and automobiles, to working from home and calling friends, customers, and colleagues at a coffee shop, distinguishing between our personal and work lives has become increasingly difficult in today's fast-paced, mobile world.

In this chapter, we explore the explosive growth in the use and development of smartphones and tablets, go into how we got here from there, and look at what all this means for your organization and the security of your mobile devices and data.

Mobility Is on the Move

Mobile device usage is growing like never seen before! Consider that:

- According to the International Telecommunications Union (ITU), by the end of 2010 there were 5.3 billion mobile subscribers worldwide, or approximately 77 percent of the world population — 90 percent of the world now lives in a place with access to a mobile network!
- Recent Gartner, Inc. research revealed a massive 72 percent increase in 2010 smartphone sales, which totalled 1.6 billion devices worldwide. Neilson data shows that 31 percent of all cellphone users in the U.S. have a smartphone.
- A study by Tecmark showed a 400-fold increase in web traffic being accessed by mobile devices in the U.K. between September 2009 and January 2011. The ITU predicts that mobile Internet access will surpass desktop access within the next five years.

As mobile devices offer greater connectivity and functionality, they are taking over personal computers as the primary device for work and Internet access.

In a March 2011 Betanews survey, 28 percent of respondents said that they use tablets as their primary PC. And a study by Tecmark revealed that iPhones are now responsible for 4.5 percent of all U.K. web traffic — not just mobile traffic!

How Did We Get Here?

Mobile devices have been around for quite a while. However, technology is now evolving far more quickly than ever before. Believe it or not, there was a full 20 years between the first cellphone call and the first SMS text message. Motorola and Bell Labs competed to produce the first portable mobile phone. In 1973, Martin Cooper of Motorola made the first mobile phone call to Dr. Joel Engel of Bell Labs (perhaps to claim bragging rights?!). But it was not until 1993 that the first person-to-person SMS text message was sent, and in that same year the IBM Simon ushered in the era of the smartphone — combining a mobile phone, a PDA, and a fax machine (yes, really!) into a convenient brick-sized form factor for a retail price of just $899. Only six years later, we had the first full Internet service on mobile phones, launched in Japan. Over the last decade, technology has moved forward significantly, so much that mobile devices like smartphones and tablets are

now everyday accessories in both our work and our personal lives (see Figure 1-1).

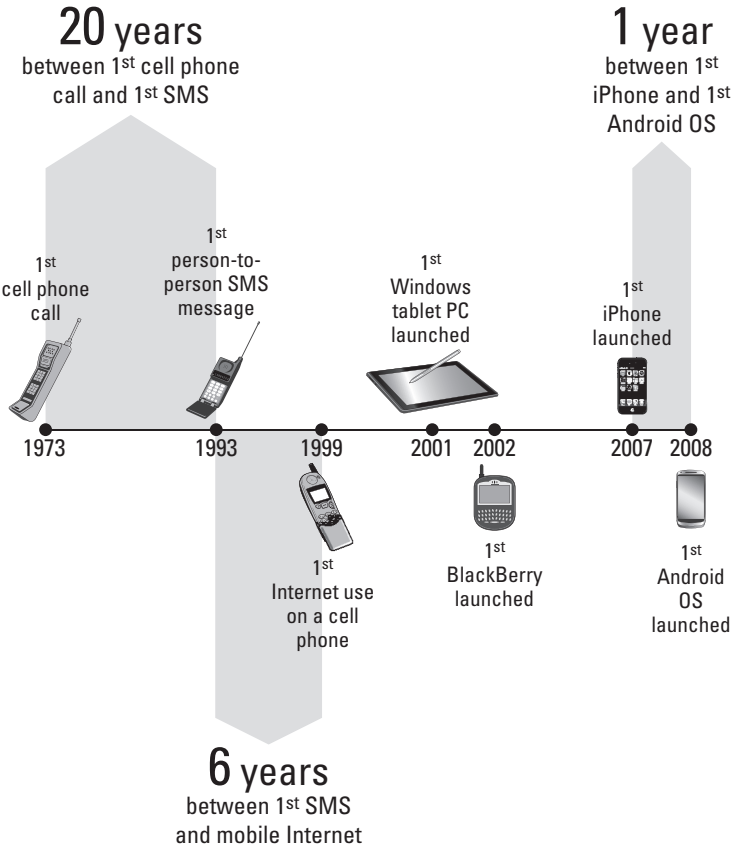

Figure 1-1: Mobile devices are developing quicker than ever before.

A Change of Attitude

Alongside radical technology changes, business expectations have also changed. Only a few years ago, enterprises wanted to block social media sites and nonstandard, unmanaged devices. Now we are all consciously trying to embrace these technologies; just look at the number of organizations with teams of people focused entirely on using social media as a channel to market.

Social media, such as Facebook and Twitter, is becoming increasingly common, and legitimate, for business uses. However, it can also introduce new security and privacy issues for your organization.

These changes in technology and business attitudes mean a new approach to security is needed. Organizations must embrace these business and technology trends with an inclusive strategy that recognizes and addresses their inherent security risks, rather than an exclusive strategy that attempts to block or deny their use in the organization. This change of attitude also impacts the future of mobile security and applications — the default answer to new technology is becoming yes rather than no.

An important first step in addressing security and privacy issues associated with mobile devices and applications (such as social media) is to decide whether your organization will allow, restrict, or prohibit their use, then develop an appropriate policy and implement the right security technologies to protect users, their devices, and your organization's sensitive and confidential data.

Many organizations have Acceptable Use Policies (AUPs) and provide security awareness training for their users, but mobile devices are often overlooked. Make sure that you've updated your policies and awareness training to get your users thinking about mobile device security before they become victims (we show you how in Chapter 4).

New Technology, New Privacy, and Security Issues

It is inevitable that mobile devices will grow more powerful and become ever more integrated into our personal and work lives. Greater computing power and increased portability will make these devices an increasingly viable replacement for the conventional PC, rather than just a supplemental tool. Many of you are already using mobile devices as such for a significant portion of the day. You can also expect further diversification of form factors; the tablet PC has already had immense success, but more challengers will follow. These new device form factors will further blur the boundary between the PC and the mobile device.

While many of you may naturally worry about traditional attacks like malware and phishing on these new devices — and without a doubt these issues do exist — new functionality breeds fresh opportunities for the bad guys. New features like augmented reality, facial recognition, and integrated social media could leave users open to new kinds of abuse.

Augmented reality, for example, connects location information with a user's social media "friends," enabling them to identify digital contacts nearby. This, in turn, opens up new prospects for social engineering, such as figuring out when you are away from your home for criminal purposes.

Go to PleaseRobMe.com to see just how dangerous "oversharing" on social media sites really is!

NFC (Near Field Contact) technology is an emerging trend that will enable users to make payments or pass on personal information with a simple swipe of their smartphones over a reader. This will further transform smartphones into the single device from which most aspects of your life are driven and make them an even more intriguing target for cybercriminals.

The more data and applications we make available and use on our mobile devices, the more tools we provide the bad guys to devise creative attacks to compromise our personal lives, businesses, and finances. Security is not the only victim; privacy will be challenged too. As we adopt more of these technologies for convenience, we can expect our private lives to come under greater public scrutiny.

A Different Architecture for a Different Time

Mobile devices are not just a smaller version of the traditional PC, even though they increasingly perform an identical set of tasks. The underlying operating systems (OS), from Android to iOS, are fundamentally different from those of PCs, and manufacturers have introduced many new concepts based on lessons learned from long experience with traditional operating systems.

Modern mobile platforms tend to include capabilities like "sandboxing" technology, which can isolate applications.

The access control and permission systems have also undergone drastic changes from the conventional OS. Rather than a permissions system based on access to arbitrary items like registry keys, they instead focus on more human-access permissions, such as whether an application needs to access your location data or SMS messages.

But many of these controls do not come with smart, secure defaults, instead relying on users to accept the permissions of an application being installed (a question they often may not know the answer to — we all recognize the tendency for users to just click OK).

Where Are We Going?

Recent events and changes in mobile technology innovation and use indicate that it is likely the threats to mobile devices, particularly smartphones and tablets, will both diversify and increase significantly. Organizations must take proactive steps to address these security and privacy issues now.

Regulators are getting smart (phones)

Regulatory standards have been through a series of changes at breakneck speed of late, increasing the power of regulators and further defining strict compliance requirements (for example, requiring specific controls like full-disk encryption for private data). These regulatory efforts have been primarily focused on desktop PCs, laptop computers, and enterprise networks, as the major vector of data loss and the traditional focus of security investment. However, these laws and regulations are written to address data protection and can be equally applied to mobile devices — the form factor of the technology or device is no excuse for data loss.

Indeed, as more data breaches occur via smartphones and tablets and more cybercriminals focus their criminal efforts on these devices, regulators will inevitably pay more attention and additional regulatory requirements will no doubt follow.

Similarly, the increasing use of these devices for business purposes will also increase the likelihood of new regulations that

specifically address the data on these devices. For example, iPhones are now being used to process credit card transactions and iPads are finding their way into the hands of doctors and nurses. Say hello to PCI DSS (the Payment Card Industry's Data Security Standard), HIPAA (the U.S. Health Insurance and Portability Accountability Act), and DPA (the U.K. Data Protection Act)!

Keeping up with innovation and development

Perhaps the most significant challenge to mobile device security is the pace of innovation and development on mobile platforms. Where traditional computers at best might evolve on an 18- to 24-month cycle, mobile platforms are undergoing significant changes on a quarter-to-quarter basis.

Born from this velocity is the challenge that new applications and ways of sharing data will often be adopted by large numbers of users before the security community has a chance to vet it and understand the privacy and security implications. *Consumerization* occurs as end-users increasingly find inexpensive and simple personal technology and applications that help them do their jobs quicker and better than the traditional corporate solutions they are provided. Regular visits to the "App Store" or "Marketplace" are a daily activity for many mobile device users. Organizations that attempt to buck the consumerization trend by altogether banning such applications will find themselves struggling to change their users' behavior and enforce untenable policies. Instead, organizations should consider accepting the consumerization trend and focusing on creating policies that promote safe and productive use of these applications. According to Gartner, Inc., consumerization will be the most significant trend affecting IT through 2015.

While applications and services on mobile devices are often updated automatically, OS updates for mobile devices can require cumbersome cable connections and user interaction. Missing OS updates can leave mobile devices with open vulnerabilities and pose significant security risks. The infrastructure for updating and patching security vulnerabilities in mobile devices is far from mature and has many lessons to learn from the traditional computer industry.

"Jailbreaking" iPhones is one example of "user-desired malware," which exploits security holes. Jailbreaking allows users to bypass Apple's security controls to customize their iPhones and run pirated applications, as well as use their iPhones on other carrier networks. These same security holes can be used for user-undesired malware too!

Getting back to the basics

It may be tempting to start with a comprehensive security solution for mobile devices that mimics desktop PC solutions with antivirus (A/V) software, data loss protection (DLP), host-based intrusion prevention systems (HIPS), full-disk encryption (FDE), and application control. But in reality, these capabilities are not yet broadly available or, in many cases, are currently not feasible to deliver.

Future mobile security solutions will need to feature a blend of device, OS, and vendor capabilities in an integrated solution. Some capabilities will be provided by the device in hardware (such as encryption) or the OS (for example, sandboxing) but will be managed and reported on by security vendors. Anti-malware capabilities will be increasingly required, although as previously noted, they will not be the same as their PC counterpart. Perhaps the most interesting areas will be DLP and continuous encryption of data as it flows between different devices: mobile, PC, or otherwise. The protection stack for mobile devices will expand over time, much as it did with the PC, but with the data rather than the network being the new enforced perimeter.

Priority one is to get the basics under control. Despite all the hype, most data breaches occur due to poor or missing configuration of basic security features and practices: weak passwords, lack of encryption, missing patches, and social engineering.

Chapter 2

Mobile Working — the Good, the Bad, and the Not So Good

In This Chapter

- Recognizing the benefits of mobile working
- Understanding the risks and threats to mobile devices
- Striking a healthy balance between your personal life and your work life

Mobile devices like Android phones and iPad tablets can do wonders for mobile workers and drive productivity and innovation in a business. However, doing so can also come with a greatly increased cost of administration and significant risk of data loss and reputation damage if these devices are not properly managed.

In this chapter, we explore the mobile working trend — its advantages, its disadvantages, and what it all means for your organization.

Mobile Working and Mobile Living — It's Here to Stay

With more than 5 billion cellphone subscribers worldwide, people today are more mobile than ever. Mobile working and mobile living are two terms that are often used interchangeably

to describe the mobility trend, and it is not without irony that the boundaries between our work lives and our personal lives have likewise become less distinct and interchangeable.

Regardless of whether smartphones and tablets are personal or company-issued, the boundaries between personal and work use have increasingly merged. Examples include

- Accessing personal websites from work devices
- Reading work e-mails on personal devices
- Accessing corporate systems outside the office

Most people are undoubtedly aware that mobile devices offer both organizations and users a lot of advantages, including

- **The ability to work from anywhere.** No longer constrained by the need to be in the office, employees can escape the cubicle and use their smartphones and tablets to work regardless of whether they're at home, on the road, or even . . . in the office!
- **The ability to work at any time.** This can be both a blessing and a curse! Your customers and counterparts have grown accustomed to sending e-mails from their smartphones and tablets whether they're at the dinner table (how rude!), driving a car (how dangerous and illegal!), or at 3 o'clock in the morning (how crazy!), and expecting a nearly instant response!

E-mailing and texting from your smartphone while driving a car is dangerous and even illegal (in many places). Your company's mobile device Acceptable Use Policy (AUP) needs to address this practice and strictly forbid it (to mitigate any potential liability issues for your organization).

These advantages, in turn, result in tangible benefits for both the organization and its users, including

- **Reduced operating costs.** It's often easier and less expensive to maintain a smartphone or tablet than a desktop PC.
- **Increased productivity.** Being able to work from anywhere and at any time enables higher productivity for your employees.

- **Improved responsiveness.** The earlier examples (at the dinner table, while driving, or at 3 a.m.) notwithstanding, smartphones and tablets provide the ability for your employees to respond more quickly to others to ensure that there are relatively fewer communications bottlenecks and to keep your customers happy!
- **Greater flexibility.** Smartphones and tablets provide the ability for people not only to work from anywhere and at any time but also with anyone, anywhere in the world, and at any time (for example, with someone halfway around the world in a different time zone).
- **Preferential satisfaction.** Ask people to choose between their smartphones and their desktop or laptop computer and quite a few would happily just use the former. Major benefits over laptop computers include lower device weight and longer battery life. In fact, by 2015 industry analysts expect mobile Internet traffic to surpass desktop Internet traffic!
- **Happier staff.** Despite the blur between their personal and work lives, people are generally happier with their smartphones and tablets. To paraphrase the British actor and comedian (see his blogs at `www.stephenfry.com`), "[we] have an emotional relationship with [our smartphone] because it's there all the time, it's our window on the world, it's our mouthpiece, it's everything we are and have."

As more and more companies worldwide recognize the benefits of mobile working, it will become increasingly commonplace. According to In-Stat, more than 25 percent of workers report being mobile from 11 to 20 hours each week and more than 15 percent are mobile 21 to 30 hours weekly.

It's Not All Good News

Like all technologies, while there are many benefits to mobile working, there are also many risks, such as data loss due to lost or stolen mobile devices and mobile malware.

Lost or stolen devices

The biggest risk with mobile devices — a lost or stolen device — comes not from the technology, but from the user.

A mobile device carrying personal and/or business data that is left unsecured and falls into the wrong hands is a major source of data loss and financial theft. Data loss is by far the biggest threat facing smartphone and tablet users today.

Most devices have a screen lock, which requires you to swipe the device and then enter a password, PIN, or unique sequence to unlock it. But if this feature is disabled or if the user has opted not to turn it on, the device is unlocked and unsecure.

In addition to locking your device, some screen lock features (such as in iOS) will also encrypt the data (such as e-mail) on your device. However, MS Exchange will only recognize a password or PIN for encryption.

If the device has access to different enterprise applications and they are pre-configured to automatically log-in, every company e-mail server, network, data resource, and application is potentially open to attack.

Financial theft is also a concern — if a criminal has access to an unsecured smartphone or tablet, it can be used to fraudulently purchase items on the owner's account. Examples include what Apple calls "in-app purchasing," where people buy things using mobile apps.

According to the 2010 annual U.S. Cost of a Data Breach study, 35 percent of U.S. organizations reported that a lost or stolen mobile device caused a data security breach. Increasingly, employees use their Androids, iPhones, iPads, and other personal mobile devices for work and blend their unprotected devices with business data. This introduces even greater risk to an organization's data, network, and reputation.

Malware goes mobile

Mobile malware and cybercrime are also major threats. Mobile malware (such as malicious applications, spyware, and Trojan horses) is still in its infancy, but it does exist and is on the rise. This trend is likely to continue and will become a major threat in the near future. The vast majority of cyber criminals are financially motivated and their focus is on data theft. Data equals dollars, pounds, euros, yen — and it is big money for cyber criminals. Now more than ever, data is the ultimate business asset. Criminals can convert data to money in many different ways, including

News flash: iPads are targets for thieves

A physician assistant (PA) at one of the largest healthcare facilities in the metro New York area used an iPad containing detailed and sensitive information about her patients. Because she was on call around the clock, she carried the iPad with her at all times. One afternoon she stopped to have lunch and left the iPad in her car. A thief broke into her car and stole the iPad containing patient data. Unfortunately, the security settings were not turned on and the thief was able to access medical information on more than 200 patients.

- **Bank details:** Steal money, make fraudulent purchases, and sell to other criminals
- **E-mail addresses:** Sell to spammers
- **Personal identities:** Steal identity, make fraudulent purchases, and sell to other criminals
- **Company data:** Blackmail organizations, corporate espionage, theft of intellectual property (IP) and trade secrets

Most mobile device users mistakenly assume that their smartphones and tablets are inherently secure because they've never experienced malware. The reality is that until recently, most people were not placing data on these devices that was worth stealing. Now that these devices contain valuable information (as we increasingly use them as a replacement for the PC) the bad guys are paying attention. We can expect a significant increase in the volume of malware targeting these devices over the coming years. Anti-virus capabilities will be important, although the defense technologies will work differently from PCs — focusing more on reputation and behavior than on traditional content security.

Fortunately, the current mobile market may help limit the spread of malware. Since there's a wide variety of platforms from which to choose — iPhone, Android, BlackBerry, and Windows Phone 7, to name a few — there's no "Windows PC-sized" target out there for malware writers.

Hacking comes full circle

You may not realize that hacking, or more correctly *cracking* (hacking originally referred to the relatively benign activity of technology enthusiasts to identify flaws in systems and software to improve their operation), has its origins in the phone system. In 1971, John Draper learned that the toy whistle packaged in Cap'n Crunch cereal boxes emitted a 2600 hertz tone that would allow hackers to make free long-distance toll calls. More recent high-profile phone hacking (or *phreaking*) cases include Anthony Pellicano ("the P.I. to the stars" or "Hollywood Phone Hacker"), and the *News of the World* voicemail hacking scandal that has embroiled the Murdoch media empire, British Prime Minister David Cameron, and Scotland Yard.

Today, cybercriminals hack into global networks and computer systems for many sinister purposes such as identity theft, fraud, espionage, and terrorism. The proliferation of convenient, easy-to-use mobile devices, particularly smartphones, packed with powerful applications and an abundance of potentially sensitive, private data makes these devices a logical — and lucrative — target for cybercriminals.

And because major vendors like Apple and Google maintain application markets, it's harder to spread infected programs.

However, given the potential rewards (for example, using smartphones as payment systems for purchases), malware writers are bound to figure out ways around these obstacles. Some already have:

- In February 2011, a new Trojan horse for Google's Android OS was found in Chinese applications stores, where it posed as legitimate programs.
- In early 2010, Google found and removed banking malware from its site after discovering a wallpaper application had gathered information on more than 1 million Android users.
- Researchers at the BBC put together their own smartphone spyware with ease and demonstrated how simple it was to crack the encryption on mobile phone conversations, providing the ability to listen in on private calls.

Smartphone apps and malware

An employee of a retail company had a smartphone and used it for a variety of purposes. The employee downloaded a financial application to help manage his bills and make purchases, but the app was infected with malware that stole credit card information. Three months later the employee received a credit card bill with thousands of dollars of fraudulent purchases. In addition, the smartphone had information about the company's customers that could now be potentially at risk for a data breach.

Most mobile malware today stems from third-party sites and markets. However, as open applications and web-based systems such as HTML 5 become more common — meaning that malware creators won't have to worry about application markets or other closed systems — the threat of mobile malware will increase.

The (Mobile) Work-Life Balance

There are, of course, gray areas in mobile working and mobile living as well — issues that are not necessarily good or bad, black or white, yin or yang.

For example, does your organization provide mobile devices for your employees (a company-liable policy), or do you allow your employees to use their personal smartphones and tablets for work purposes and reimburse them (an employee-liable policy)? Key differences between the two types of policies include

- A *company-liable policy* provides greater control over the devices and applications used in your business. You may also be able to leverage business plans or promotions from wireless providers to reduce costs and take advantage of features such as pooled minutes across the entire company.
- An *employee-liable policy* provides more flexibility and may be less costly for very small businesses or businesses that don't have a largely mobile workforce but generally provides less control over the types of devices

> and applications used in your business. The gray area becomes even murkier when an employee leaves the organization — what happens to company data on the device?

Company-liable and *employee-liable* only refer to who is liable for the phone bill. If a smartphone or tablet containing company/customer sensitive or private data is lost or stolen, the company is still potentially liable for the data compromise, regardless of who owns the device.

As more and more companies look to reduce costs and support flexible working, businesses are increasingly encouraging employees to use personal devices for work. Although mobile technology means that workers can be productive more of the time, it also means that employees are taking sensitive, business-critical data with them wherever they go, making it harder for IT security teams to manage and protect these devices. Prevalent use of mobile devices can also create challenges for human resources (HR) departments when dealing with certain classes of employees (for example, hourly versus salaried staff) and overtime rules.

Finally, while smartphones and tablets can be great productivity boosters, they can also be productivity killers — a double-edged sword.

Games, videos, music, and other personal apps are a few examples of some potential productivity killers. Enforcing restrictions or limitations on these types of apps can be a real challenge for personally-owned mobile devices.

And ultimately, if your employees are connected "24/7" and the boundaries between their personal and work lives become non-existent, then their morale and productivity will eventually suffer terribly.

Be sure to address the mobile work-life balance if your organization promotes the use of mobile devices and encourages the "always-on" employee!

Chapter 3

Keeping Your Mobile Devices, Data, and Applications Safe and Secure

In This Chapter

- Devising a protection strategy for mobile devices
- Preventing mobile data loss
- Developing secure mobile apps

Quick! Where's your smartphone? For many, that question sets off a brief panic attack as they grab at their hip or pocket, or glance at the table or desk in front of them. And if it's not there . . . ?

Just imagine. If your smartphone or tablet were lost or stolen, what information could people access through your device? What could they learn about your

- Work (contacts, customers, patients, e-mails, projects, proposals, private data and records)?
- Family and friends (phone numbers, pictures, text messages, social plans)?
- Life (banking and financial accounts, online store accounts, other personal information)?

In this chapter, we discuss the steps you need to take to protect your organizations' smartphones and tablets, any sensitive and confidential data on them, and the applications they run.

Protecting Mobile Devices from the Devious

Protecting your organizations' smartphones and tablets requires a comprehensive approach, including developing a strategy, educating users (which we cover in Chapter 4), understanding new and evolving technologies and threats, and deploying mobile security solutions.

Develop a mobile security strategy

Perhaps the most critical aspect of your strategy is how you will keep it current and up-to-date. Mobile devices and technology are evolving at an incredible rate and the evolution of this breadth of technologies is largely unpredictable. Your mobile device security strategy should look something like this:

- Project teams dealing with adopting mobile devices should define a six-month strategy using an agile methodology and then constantly reevaluate how the devices are changing and what new risks are being introduced. Developing a conventional three- to five-year IT strategy is unwise.
- Plan for mobile devices to be more explicitly included in your organization's regulatory compliance requirements. Although regulations typically lag behind technology and for the most part do not specifically address requirements for smartphones and tablets (yet), they are written with the intent of protecting sensitive data, irrespective of the technology being used.
- Ensure that any technology solutions you adopt (such as device management) provide as much abstraction as possible to device type and OS. Popular devices will change quickly, and you need to future-proof your security controls as much as possible. There is a risk

that as you adopt five times the number of device types you currently have, you increase the cost and complexity of managing them by the same order of magnitude. Challenge your security vendors to solve this issue for you with broad platform support.

- Carefully look at the combination of work and personal data on mobile devices. These devices are often the extreme scenario, blending your contacts, e-mail, and data into one user interface. Consider your strategy for this on an ongoing basis since it is a trend that is likely to continue. Deploy processes, policies, and practices to help users avoid making silly mistakes that lead to compromising themselves and your business.
- Invest in building mindshare with your users on mobile security (see Chapter 4). They need to understand the value of the information (both personal and business) they are placing on their devices and that these devices are not inherently secure.
- Don't be overly clinical with your definition of mobile devices — different format factors are evolving every day and your strategy needs to encompass smartphones, tablets, and potentially other popular embedded devices as well. That said, it would be wise to specifically authorize a list of devices; many enterprises, for example, will allow specific versions of an OS that include minimum required security capabilities. As devices mature, your list will grow longer.
- Finally, resisting these new devices and technologies entirely is not a tenable position for most organizations. Most businesses are in the position of having to adopt them. Enabling certain devices like the iPad at an appropriate level of security in your organization will earn you points to help prevent adoption of more risky technologies.

Understand new and evolving technologies and threats

The rapidly increasing number and speed of mobile devices introduces new challenges for security — high-speed, ubiquitous connectivity makes mobile devices an attractive target for malware, bot networks, and command-and-control, where previously they would have been less than ideal.

Sophos Mobile Control

Sophos helps you enforce a consistent security policy for iPhone, iPad, Android, and Windows smartphones used in your business, letting you control their security features and even remotely locking and wiping them if they get lost. SMC provides organizations with a hierarchical tool to manage and protect their mobile devices, which includes mobile device management, malicious apps protection, malicious website protection, device encryption, and data loss prevention (DLP).

Keep corporate data safe by applying security policies.

- Lets you turn on the built-in security features of iOS (iPhone/iPad), Android, Windows Mobile 6.x devices, including any OS encryption or password protection.
- Provides remote over-the-air lock. It can even wipe lost or stolen devices, all from the central web console.
- Tamper detection means Mobile Control knows if it's removed from a device and can block company e-mail access. It can also identify rooted Android devices.
- Ensures that only registered devices that meet your policies (like minimum required password length) can access corporate e-mail by using Exchange Active Sync Proxy.
- Lets you control application use. For example, you can block a time-wasting game or inappropriate application.

Easily install and maintain controls with over-the-air setup and a web console.

- Monitors and controls security features on mobile devices from a centralized, web-based console.
- Deploys security updates and policies over the air through the web portal, letting you maintain mobile devices anytime, anywhere — so that users don't have to visit the Help Desk.
- Lets you prove your corporate compliance with easy inventory and reporting tools.
- Tracks and reports on all registered devices, letting you drill down to their individual configuration settings, serial numbers, model numbers, hardware details, and more.

Reduce IT burden with a self-service portal for your users.

- Allows users to register their own devices, meaning that they can use their own personal phone — and that you can keep an eye on their security and make sure they're compliant.
- Lets users choose to remote lock or wipe their devices without having to contact the Help Desk.
- Now available for download in the Android Market.

Mobile devices have undergone a series of significant connectivity upgrades from first generation (or 1G) networks based on analog cellular technology, to second generation (2G) GSM (Global System for Mobile Communications) digital cellular networks, and much faster 3G (UMTS, or Universal Mobile Telecommunications System) and 4G (LTE, or Long Term Evolution) networks. Mobile networks around the world are currently undergoing significant upgrades enabling broadband speed (or faster) connectivity to mobile devices — an excellent enhancement for the roaming user and increasingly the default for many businesses.

IPv6 is one solution that provides enhanced performance features and new functionality designed specifically for mobile device security. Mobile IP (or IP mobility) in IPv6 is designed to make it easier for mobile devices to switch between different networks (for example, between WiFi and cellular) while providing a consistent, "mobile" IP address. Mobile IP delivers consistent connectivity and coverage, and enables efficient routing of traffic for the truly mobile road warrior. There are numerous security enhancements for mobile devices in IPv6 as well.

Prior to the widespread adoption of residential, high-speed broadband and cable Internet connectivity, malware was largely limited to relatively benign viruses that were primarily spread via floppy diskettes (remember those?) and e-mail attachments.

Deploy mobile security solutions

As new devices and security threats evolve, new mobile security solutions and controls are being developed. Organizations running mobile security solutions are linking in to a journey as the issues evolve, rather than a final mobile security solution. According to Juniper Research, only 4 percent of smartphones and tablets are protected with security software, such as Sophos' Mobile Control (SMC) solution (refer to the sidebar earlier in this chapter).

Protecting Data "On-the-Go"

After years of battling intrusions, viruses, spam, and more recently, data leakage, organizations are now wrestling with another growing security issue: mobile data leakage.

Download your free copy of *Data Leakage For Dummies,* Sophos Special Edition at `www.sophos.com/en-us/security-news-trends/security-trends/data-leakage-for-dummies-register.aspx` to learn more about data leakage.

Identifying data at risk

Information protection and control (IPC) begins with identifying what data is at risk within your organization. Broadly defined, this includes data at rest, data in motion, and data in use.

Data at rest refers to stored data. Most commonly, this refers to files and databases on laptops, desktop PCs, and servers, but increasingly it now includes data on smartphones and tablets.

Data at rest is perhaps the biggest data leakage challenge for organizations, because data is literally everywhere — now more than ever! Nevertheless, knowing where your data is stored, *everywhere* that it is stored, is an important first step — you have to know what you are protecting.

Data in motion refers to data that is being transmitted across a network, such as a corporate network, a cellular provider network, or a WiFi network. Data in motion is typically protected with VPNs (virtual private networks) using IPsec or SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption.

In this book, data in motion is defined as data that is being transmitted across a mobile or WiFi network, not data that happens to be on your mobile smartphone or tablet!

Data in use refers to data that is being accessed or modified on a device, such as a smartphone or tablet. Protecting data in use involves protecting the confidentiality and integrity of data while it is being viewed or changed.

Mobile malware protection helps to ensure that viruses, Trojans, and other malware don't compromise your data. Equally important to protecting data in use is security awareness and training. Social engineering is the easiest method for gaining access to confidential data. End users must be kept aware of current and evolving threats, as well as "common sense" steps — such as not working on confidential data in plain sight of others in a hotel lobby or airport terminal. See Chapter 4 to learn more about security awareness and training.

Classifying data at risk

Next, you need to know why you are protecting the data. This involves more than "because it's confidential" or "because it's the right thing to do." This is best accomplished with a data classification scheme that helps you place an implicit, or explicit, value on your data. This is necessary because it is simply not possible, or effective, to protect all data equally.

A data classification scheme also makes it easier to define (in an acceptable use policy, or AUP) what data is and is not permitted on smartphones and tablets. For example, "No data marked *Company Confidential* or *Internal Use Only* will be stored or processed on smartphones and tablets."

Examples of sensitive data that needs to be classified, addressed in policies, and appropriately protected include

- **Credit card information** (credit card numbers, billing information, PINs and security codes)
- **Financial data** (banking accounts, tax data)
- **Personally Identifiable Information or PII** (combinations of full names, birth dates, addresses, and Social Security or National Identification numbers)
- **Confidential business data** (intellectual property, trade secrets, proprietary information)

Storing or processing certain data (such as credit card numbers or patient information) on smartphones and tablets can greatly increase the cost and complexity of your organizations' regulatory compliance efforts. Be sure that you clearly define the business need and benefits before allowing such data to be stored and processed on these devices.

Securing data at risk

Finally, you need to identify appropriate solutions and controls to protect the confidentiality, integrity, and availability of your data for your organization. These solutions may include antivirus, encryption, and network access control (NAC).

Enabling basic security mechanisms in your smartphones and tablets is equally important for securing your organizations' sensitive and confidential data. A recent Sophos remote and mobile user study found that an alarmingly small percentage of organizations require use of these mechanisms on employee-owned devices used for business purposes (see Figure 3-1). These include

- **Require passcodes and define complexity requirements.** Passcodes or passwords should be required on mobile devices. Organizations should ensure that complexity requirements (such as a minimum number of characters) are consistent with other corporate security policies.
- **Enable Auto-Lock and Passcode Lock.** Think of it as a screensaver for your smartphone. Auto-Lock itself doesn't do much to protect your data (except perhaps from prying eyes), but when combined with a passcode, it will at least slow a thief down.
- **Enable Erase Data on iPhones and iPads.** The Erase Data function completely wipes all of the data on your iPhone or iPad after ten failed attempts.
- **Disable Bluetooth when not in use.** Only enable Bluetooth while you are using your Bluetooth device. You'll not only reduce your risk of Bluetooth attacks such as bluesnarfing, bluebugging, and bluejacking, but you'll also extend your device's battery life!
- **Use WiFi Protected Access (WPA).** Just like any other WiFi connected device, you should only connect to known and trusted WiFi networks that are secured with WPA or (preferably) WPA2 encryption. On the iPhone and iPad, use the "Ask to Join Networks" function to ensure that you don't automatically and unwittingly join any unsafe WiFi networks. Oh, and you'll extend your device's battery life too!
- **Use SSL to access e-mail.** SSL encrypts e-mails as they are being sent and received on your mobile device.
- **Enable browser security.** Just like the browser on your desktop PC, the browser on your mobile device has security settings that should be enabled, including Fraud Warning on the iPhone (to warn you when visiting fraudulent websites), turning off JavaScript, blocking Pop-ups, and handling cookies.

Tips for creating a safe passcode for your smartphones and tablets

Work, friends, family . . . smartphones and tablets open the door to your whole life. Keep them secure with a safe passcode.

- **ALWAYS** use a passcode. Otherwise if some gets hold of your device, that person can easily access your apps and data.
- Make your passcode **DIFFICULT TO GUESS**. Codes such as 1234 or 2580 can be cracked in seconds without any hacking software or tools. Go for something that's unique but easy for you to remember.
- **LONGER IS BETTER**. The longer the passcode, the harder it is to crack. Make yours a minimum of 6 digits.
- **MIX NUMBERS AND LETTERS**. If your device allows, use a passcode that combines numbers, letters, and punctuation. Avoid dictionary words and choose a personal memorable combination.
- **MAKE IT UNIQUE**. Don't use the same passcode for anything else, including other devices, bank cards, or online accounts. That way, if one gets hacked, the rest stay secure.
- **HIDE YOUR PASSCODE**. Look around and make sure no one is watching you type in your passcode, just like you protect your PIN at the ATM machine.

For more help securing specific devices, visit `sophos.com/loveyourphone`.

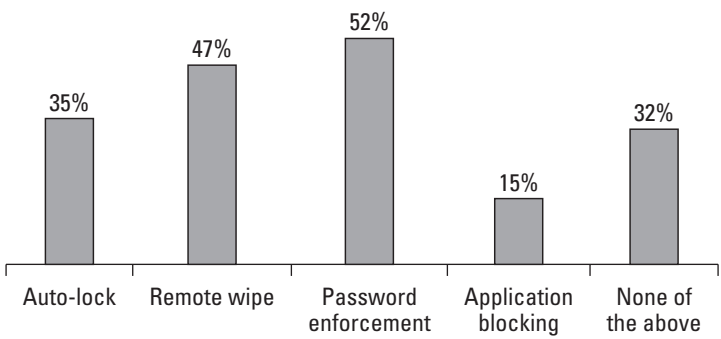

Figure 3-1: The percentage of organizations that require security mechanisms on employee-owned smartphones and tablets.

- **Limit e-mail retention.** Organizations can reduce their risk exposure by limiting the number of days that e-mail messages are retained on a mobile device (for example, three or ten days).
- **Set Device Usage Restriction.** You can enable restrictions to block certain content that may be prone to malware, disable the ability to install or remove apps, control changes (for example, location services and account information), and prevent certain productivity killers (such as games and YouTube).
- **Enable remote wipe or remote lock capabilities.** Using a mobile device management application, organizations can remotely wipe or lock a mobile device that has been lost or stolen.

Applying Security to Mobile Apps

There are literally hundreds of thousands of applications (or "apps") for smartphones and tablets available in the marketplace or app stores. Whether you're downloading apps or developing and deploying apps for your employees' mobile devices, it's important to understand what security exists to protect those apps and the devices they're installed on.

Playing together in a sandbox

Mobile operating systems like Apple iOS and Google Android have built-in security infrastructure to help protect apps from each other. Protecting or shielding one app from another is known as *sandboxing.* In effect, the app has its own little sandbox to play in and has no access to data or information stored in another app's sandbox.

A *sandbox* is an environment in which each application on a mobile device is allowed to store its information, files, and data securely and protected from other applications. The sandbox forms and maintains a private environment of data and information for each app.

A sandbox does not keep the entire device safe. If a malicious app is downloaded to the device, it can still infect and steal information from the user directly, even if not from another app.

The main points to remember about sandboxing mobile apps are

- **Apps can be sandboxed.** Apps can be developed to protect their information and data from each other, preventing one app's data from being read by another app.
- **A sandbox does not equal mobile security.** Sandboxing one or more apps means only that those apps are shielded *from each other*. Malicious apps can still seek information from unprotected apps or directly from the user.
- **A sandbox does not protect the entire device.** To protect the entire device, you need a mobile security app that detects and prevents viruses, spam, Trojans, and other mobile threats from invading in the first place.

Blackberry app security

Organizations can control what apps can be deployed on employees' BlackBerry devices. The BlackBerry Enterprise Server (BES) is an example of a mobile device management solution for BlackBerry devices that allows the configuration and enforcement of application security policies for corporate use. Using BES policies, you can specify whether a user can install third-party apps or determine the privileges that third-party apps can have on the device.

Third-party apps can, in general, access two types of data on a BlackBerry device:

- User data, such as e-mail, calendar, and contacts
- App data — persistent storage that shares data with other apps

You can control or restrict access to both types of data by using BES policies. If you develop your own apps for corporate-owned BlackBerry devices, you can enable appropriate permissions for your apps.

The BlackBerry also includes a personal firewall feature that restricts the types of connections maintained by an app. When an app tries to establish an internal connection to a corporate server, the device prompts the user to allow or deny that connection. Organizations can choose to allow or deny such connections as a policy. This prevents suspicious apps from

breaking into your corporate network and stealing information from internal servers.

Third-party apps can be written to use BlackBerry device APIs (application programming interfaces) for sensitive packages, classes, or methods. Such apps need to be signed by Research in Motion (RIM) before they are allowed to use those APIs. The signing process ensures that the app is tested and verified for authenticity before being granted APIs to use sensitive information.

Apple iOS app security

Application developers use the sandboxing capability of Apple iOS to protect the integrity of user data and to ensure that their apps don't share data with other apps installed on the user's device. Each app has access to its own files, preferences, and network resources. Recent versions of iOS have also added the capability to encrypt app data so that sensitive data such as usernames, passwords, or credit card numbers can't be accessed easily from the file system.

A sandbox limits the damage that a potential hacker can do to an Apple iOS device, but it *cannot* prevent an attack from happening. Software defects in an application could allow a hacker to cause the app to crash. Although Apple has built robust sandboxing features into the Apple iOS, it's up to the app developers to ensure that their apps are written securely and to prevent hackers from exploiting user data.

On Apple iOS devices, certain files marked by the app developers can even be encrypted when the device is locked. Doing so requires the encryption capability of the device to be enabled and configured. Once that's done, certain types of content can be protected automatically when the device is locked. When the files are locked, not even the app can access their contents.

This feature also extends the protection that shields a particular app's data from another app. Note, however, that this is an optional feature; not all apps need to encrypt files on the file system. A file only gets encrypted if the app developer designates it for automatic protection. Even so, this is a useful feature for app developers, especially if they hold sensitive

information on the device (such as the user's username, password, or other credentials).

Android app security

Like the Apple iOS platform, Android has a number of security features built into its operating system. On Android, by default, no application has the permissions needed to perform operations that impact other apps, or, for that matter, the device in general. This arrangement prevents apps from reading information or data stored by other apps, and keeps them from reading the user's personal data (such as contacts and e-mails) stored on the device. This inherent security model forms the basis of the Android operating system.

Android is based on the Linux Operating System, which has elaborate security mechanisms built in. Each app runs with a distinct system identity (including its Linux User ID and Group name), which is unique for all apps. The Android OS assigns a unique User ID to an app when the app is installed. Linux uses this mechanism to separate apps from each other and protect the system in general.

Even with the security built into the Android OS, smartphones based on the Android OS are highly susceptible to malware and other security issues.

Windows Phone 7 app security

Similar to RIM and Apple, Microsoft centrally controls the distribution of updates for the Windows Phone platform. But unlike the Blackberry and the iPhone, Windows phones are manufactured by several device makers and have multiple carriers.

Although Microsoft doesn't control its phones as closely as RIM or Apple, the updating process is not dependent on device makers and carriers, as with Android devices. This places Windows Phones in a sort of security middle ground — squarely between RIM and Apple at one end of the spectrum (centralized control and distribution of updates and fixes and rigorous testing for quality assurance) and Google (Android) at the other end (a "reference design" for updates, but customizing and

testing are up to the individual device manufacturers and carriers). Microsoft's central control of updates means flaws can be patched as soon as fixes become available. But because device manufacturers and carriers have no control over which updates to install, this approach comes with some risk.

In early 2011, Microsoft tried to push an update to the Windows Phone 7 that accidentally "bricked" some Samsung Omnia handsets — rendering them unusable!

Sandboxing and on-device security

Running a sandboxing application on your mobile device can be an advantage if the application protects the user data and device from mobile threats. Some apps available in the market provide sandboxing capabilities for particular features such as e-mail. For example, Good Technology (`www.good.com`) provides application sandboxing for e-mail, which maintains e-mail securely within the application and protects it from access by other applications.

Sandboxing by itself is not a substitute for real mobile security. You need to complement sandboxing with appropriate mobile security to protect the entire device, and not just the sandbox. Malicious apps can still attack a device even if one or more apps have sandboxing implemented.

An ideal corporate solution includes such a sandboxing or application security solution combined with an on-device mobile security solution that provides protection from viruses, malware apps, and spam. The sandboxing solution provides application security to your corporate apps as well as to the user's data in private apps downloaded from an app store. The mobile security solution complements this application security by ensuring that files and data received or sent by the device are free of viruses or threats to data or applications.

Chapter 4

You Can Lead a (Mobile) Horse to Water

In This Chapter

- Gaining an awareness of the awareness problem
- Addressing security awareness
- Drafting an acceptable use policy

Security awareness is an often overlooked factor in an organization's training programs — information security in general, and mobile device security specifically — are often taken for granted. As a result, users can unwittingly become the weakest link in an organization's information security program.

In this chapter, we help you to understand the importance of security awareness training, implement an awareness program, and develop an Acceptable Use Policy (AUP) for smartphones and tablets in your organization.

Beware a Lack of Awareness

Awareness of the need for security on mobile devices is limited — most people know how to use their smartphones and tablets but are generally oblivious to the risks.

A recent independent survey by TNS Omnibus, commissioned by Sophos, confirmed that the majority of people do not consider that their smartphone is a risk to their personal or work data — 89 percent are unaware that smartphones can transmit confidential information without a user prompt, 67 percent don't have passwords set up on their mobile phones to

protect stored data, and 65 percent worry more about laptop or PC security than mobile device security (see Figure 4-1).

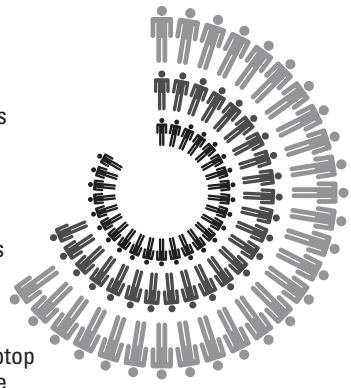

Figure 4-1: Widespread lack of awareness.

Source: TNS Omnibus

Raising Awareness

A security awareness program provides basic security information and ensures that everyone understands the importance of security. Several key factors are critical to the success of a security awareness program, including

- **Senior-level management support:** Under ideal circumstances, senior management is seen attending and actively participating in training efforts.
- **Clear demonstration of how security supports the organization's business objectives:** Employees need to understand why security is important to the organization and how it benefits the organization as a whole.
- **Clear demonstration of how security affects all individuals and their job functions:** The awareness program needs to be relevant for everyone, so that everyone understands that "security is everyone's responsibility."
- **Taking into account the audience's current level of training and understanding of security principles:** Training that's too basic will be ignored; training that's too technical will not be understood.

- **Action and follow-up:** A glitzy presentation that's forgotten as soon as the audience leaves the room is useless. Find ways to incorporate the security information you present with day-to-day activities and follow-up plans.

Awareness programs may include the following elements:

- **Orientation:** New employees and contractors should receive basic training and orientation. During the training, they may be required to read and sign a mobile device Acceptable Use Policy (AUP) — which we cover in the next section.
- **Presentations:** Short briefings, company meetings, and other informal presentations are excellent opportunities to get the word out about mobile device security.
- **Printed materials:** Security posters, corporate newsletters, and periodic bulletins are useful for disseminating basic information, such as security tips and promoting general security awareness.

You can download free security tips and brochures at `www.sophos.com/loveyourphone`.

Defining Acceptable Use

Developing clear guidance for users with regard to smartphones and tablets, to address what is and is not allowed, and what is required if personal devices are permitted for work purposes are critical elements of an organization's Acceptable Use Policy (AUP).

In a recent survey by TNS Omnibus, 30 percent of respondents stated that their company does not have a security policy in place to protect information on personal devices used for work purposes. Key findings of the survey include

- More than a quarter (28 percent) of those surveyed are actively encouraged by their employers to use personal devices at work.
- 47 percent of consumers believe that viruses are a major security threat to mobile devices.

- 25 percent of respondents have only one phone for work and personal use.
- Only 13 percent felt confident that information on their laptop or mobile device would be safe if they lost it.
- More than 85 percent of organizations have established an AUP, but only 36 percent have policies for employee-owned devices.
- AUPs for employee-owned devices are the least enforced amongst the different policies.

These findings reaffirm the results of a recent remote and mobile user study of Sophos' customer base, which showed that the vast majority of businesses do not approach the protection of personal devices in the same way that they protect company-owned technology.

Because security on personal mobile devices is typically limited, unprotected smartphones and tablets can accidentally disclose confidential or sensitive company data. In spite of this, 60 percent of respondents said that they've used their personal mobile device for work purposes, despite limited or no security policies being in place.

One of the challenges facing organizations today is securing both privately owned and corporate mobile devices, such as smartphones and tablets. Users do not recognize that mobile devices represent a threat to their organization and data security. As a result, they often do not apply the same security and data protection guidelines as they would on other devices, such as desktop computers.

Another challenge is that when users provide their own devices, they often give greater weight to their own rights on the device than to their employer's need to protect data.

The policy in the sidebar "Mobile Device Acceptable Use Policy: An example" can be used as a guideline for organizations looking to implement or update their mobile device security policy. Feel free to adapt this policy to suit your organization. Where appropriate, adjust, remove, or add information according to your needs. This is not a comprehensive policy, but rather a pragmatic template intended to serve as the basis for your own policy.

Mobile Device Acceptable Use Policy: An example

Introduction

Mobile devices, such as smartphones and tablets, are important tools for the organization and their use to achieve business goals is supported. However, mobile devices also represent a significant risk to information security and data security. If appropriate security applications and procedures are not applied, mobile devices can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

<Company X> has a requirement to protect its information assets in order to safeguard its customers, intellectual property, and reputation. This document outlines a set of practices and requirements for the safe and acceptable use of mobile devices.

Scope

All mobile devices: Whether owned by <Company X> or owned by employees that have access to corporate networks, data, and systems, not including corporate IT-managed laptops. This includes smartphones and tablets.

Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements), a risk assessment must be conducted before being authorized by security management.

Policy

Technical Requirements

Devices must use the following operating systems: Android 2.2 or later, IOS 4.x or later <add, remove, or update as necessary>.

Devices must store all user-saved passcodes in an encrypted passcode store.

Devices must be configured with a secure passcode that complies with <Company X>'s password policy. This passcode must not be the same as any other credentials used within the organization.

With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal wired or wireless corporate network.

User Requirements

Users must only load data essential to their role onto their mobile device(s).

Users must report any lost or stolen devices to <Company X> IT immediately.

If a user suspects that unauthorized access to company data has taken place via a mobile device, the user must report the incident in accordance

(continued)

(continued)

with <Company X>'s incident handling process.

Devices must not be "jailbroken" or "rooted" or have any software/firmware installed that is designed to gain access to functionality not intended to be exposed to the user.

Note: To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its security features and enabling the installation of unauthorized software.

Users must not load pirated software or illegal content onto their devices.

Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure whether an application is from an approved source, contact <Company X> IT.

Devices must be kept up to date with manufacturer or network provided patches. At a minimum, patches should be checked for weekly and applied at least once a month.

Devices must not be connected to a PC that does not have up-to-date and enabled anti-malware protection and that does not comply with corporate policy.

Devices must be encrypted in accordance with <Company X>'s encryption standards.

Users must be cautious about the merging of personal and work e-mail accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate e-mail system. If a user suspects that company data has been sent from a personal e-mail account, either in body text or as an attachment, they must notify <Company X> IT immediately.

(If applicable to your organization) Users must not use corporate PCs to back up or synchronize device content such as media files unless such content is required for legitimate business purposes.

Chapter 5

Ten (Okay, Seven) Tips for Securing Your Mobile Devices

In This Chapter

- Dealing with mobile device security

In this chapter, we identify seven ways to help you address mobile device security risks in your organization.

Develop an Enterprise Strategy for Mobile Device Security

Mobile devices, such as smartphones and tablets, can help an organization increase efficiency and productivity, improve responsiveness, and provide flexibility and speed. But mobile security challenges demand a holistic or strategic approach to managing risks, threats, and vulnerabilities.

Begin by conducting an audit to determine where mobile devices are used in your organization. An audit helps you to understand your organization's risk based on the numbers, types, and uses of mobile devices in your organization.

Next, conduct a risk assessment to determine possible theft and loss scenarios for your mobile devices and data.

Armed with the results of your audit and risk assessment, you can identify appropriate policies and controls to protect any sensitive or confidential data that may be processed, stored, or transmitted on your users' mobile devices.

Create a Comprehensive Policy for Mobile Device Use

Comprehensive security policies may be a challenge to create and enforce because of the variety and number of mobile devices in use. Still, organizations need to develop policies for mobile device use that address the risks associated with the various mobile devices being used and the security procedures that should be followed. Topics that should be addressed include

- Password requirements consistent with other corporate password policies, such as length and complexity
- What types of data should not be stored on mobile devices
- Guidelines for business and personal use of mobile devices
- How to determine if an application can be safely downloaded and installed
- How to report a lost or stolen device

One area that needs to be addressed in policies is the practice of turning off or bypassing security settings, or "jailbreaking." In a Ponemon Institute study of 116 companies, two-thirds of these companies reported that 10 percent or more of their users routinely turned-off or disengaged the security features on their mobile devices. This practice can be a pervasive problem within companies.

Establish Accountability

Organizations have a responsibility to provide their users with policies, procedures, and technologies to secure mobile devices used in the workplace. Users, in turn, must understand those policies and procedures, be accountable for the security of their devices and the data on those devices, and use their mobile devices responsibly.

Launch Awareness Training

Organizations should implement a training and awareness program to help mobile device users understand new and emerging security threats. This is particularly important as users are increasingly using mobile devices for both business and personal use. Some specific threats that mobile device users need to be aware of include

- **Phishing.** Employees should be trained to recognize a phish. Phishing e-mails usually appear to come from known organizations or individuals and ask for personal or confidential information.
- **Malware.** According to a 2011 study by the Ponemon Institute, 91 percent of companies say their employees downloaded web applications that contained malware, viruses, malicious code, or bots. Users need to be vigilant to prevent malicious software on their smartphones and other mobile devices.
- **Eavesdropping.** Users should never assume that voice calls are confidential (like fax or e-mail), especially when calling internationally where some countries' phone operators have no encryption security in place. An often overlooked risk is the disclosure of sensitive business information during phone conversations.

Use Application Control, Patching, and Other Safeguards

Implement appropriate application controls, patching procedures, and other security measures to protect both the data and the devices. Mobile device management solutions (such as Sophos Mobile Control, or SMC) can be used to:

- Restrict corporate e-mail delivery to only devices that conform to company policies.
- Change passwords on mobile devices over the air (OTA).
- Deliver apps to mobile devices in a controlled manner.

- Verify that mobile devices are in compliance with corporate policies.
- Ensure operating systems and applications are current and patched.
- Whitelist approved applications and blacklist banned applications.
- Discover jailbreaking and rooting on mobile devices.
- Manage and identify all mobile devices accessing your network (you can't protect your enterprise if you don't know all the doors into your network).

Use Remote Wipe, Encryption, and Anti-theft Capabilities

A lost or stolen mobile device that is encrypted is much less costly to an organization than a mobile device containing confidential or sensitive data that is not protected. In addition to encryption, you should implement anti-theft technologies that can be used to locate or prevent unauthorized parties from using a lost or stolen device. Most smartphones have remote wipe capabilities that you can use to erase any data on a lost or stolen device. You may also need to invest in software to manage all of your mobile devices, as well as to provide centralized logging and reporting.

Most data breach laws now include a safe harbor provision that exempts organizations from public disclosure requirements if they can produce evidence (such as log files) that any confidential or sensitive data on a lost or stolen device was sufficiently encrypted.

Understand Privacy Issues

Mobile devices have many inherent privacy risks. Unauthorized disclosure of customer or employee information can result in reputation damage and costly fines as a result of a security incident, data breach, or regulatory noncompliance.

Learn more and download the free Mobile Security Toolkit at `www.sophos.com/loveyourphone`.

About Sophos

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing security and data protection solutions that are simple to manage, deploy, and use, and that deliver the industry's lowest total cost of ownership. Sophos offers award-winning encryption, endpoint security, web, e-mail, and network access control solutions backed by SophosLabs — a global network of threat intelligence centers. With more than two decades of experience, Sophos is regarded as a leader in security and data protection by top analyst firms and has received many industry awards.

Sophos is headquartered in Boston, Massachusetts, U.S., and Oxford, U.K. More information is available at **www.sophos.com**.

What you need to know about mobile device security!

Mobile devices like iPads and Android phones can do wonders for mobile workers and drive productivity and innovation in a business. But this can come with a greatly increased cost of administration or significant risk of data loss and reputation if the devices are not managed correctly. With this book, you get clear, practical guidance on how to make sure that mobile devices are a benefit rather than a risk for your organization.

- ***Improve productivity* — by safely enabling mobile working in your organization**
- ***Develop secure apps* — use sandboxing to develop and deploy safe apps**
- ***Address employee-owned devices* — what they can and can't do on your corporate network**
- ***Create awareness* — so that your users don't become the weakest link in your mobile security strategy**

Open the book and find:

- **Why smartphones and tablets are a target for malware and cyber criminals**
- **What company data may be kept on your employee-owned smartphones and tablets**
- **How mobile working is affected by PCI, U.K. DPA, and HIPAA**
- **Tips on how to secure your smartphones and tablets**

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

Lawrence C. Miller has worked in information security for more than 20 years. He is the coauthor of *CISSP For Dummies* and more than 20 other titles.

For Dummies®
A Branded Imprint of
WILEY

ISBN: 978-1-118-17673-3
Book not for resale