Why Should I Care?

MOBILE SECURITY FOR THE REST OF US

10 Simple Things You Can Do to Protect Yourself and Your Organization from Today's Mobile Computing Threats

by VERACODE

Share this:

Contents

FOREWORD

by Chris Wysopal
Co-founder, CTO & CISO of Veracode, Inc.

I've already accepted the fact that Bring-Your-Own-Device (BYOD) is a business trend that's here to stay. According to one report I recently read, just 23 percent of enterprise employees use company-sanctioned mobile devices only – meaning 77 percent of employees are using their own devices in some capacity to do their job.[1] As the Chief Information Security Officer (CISO) at Veracode I have experienced this trend firsthand and if it hasn't hit you yet, the BYOD tidal wave is coming your way!

We've created this mobile security book to help you successfully ride that wave. After reading this book you and your employees will learn, as we have at Veracode, it takes a coordinated effort between employees and IT/security personnel to truly secure mobile computing in the enterprise.

Formulating a BYOD policy is only one side of the equation – employee education is the other. Most business users simply aren't aware of the security threats facing them when they use their favorite mobile device at work. This book aims to increase that threat awareness level and ultimately convert your employees into willing participants in your organization's secure mobile computing or BYOD program.

This book lists 10 simple things that every business user can do to help protect their personal information as well as their company's data, IP and brand when they use their mobile devices at work. We've made every effort to make our mobile security story a fun one to read. Some of the details around the mobile security stack can be tedious, but it's hard to resist when the stack looks like a club sandwich!

We hope you and your employees find this book helpful, and we encourage you to share it with your colleagues. We'd also appreciate your feedback, so feel free to email us (info@veracode.com) or contact us on Twitter (@Veracode) with your comments.

Happy reading...

Chris Wysopal

PART ONE

It's Scary Out There

Share this:

Our mobile devices are wonderful things.

Not only are they highly portable, they are essentially small computers themselves – allowing us to stay productive with apps, email and Internet access at all times. We use them on our commute, we take them when we travel, and increasingly, we bring them to the office with us. They store vast amounts of information and provide a critical gateway to the rest of the organization.

Unfortunately, **your favorite mobile gadget is inherently insecure**. Small and compact, mobile devices are easy to lose or steal. Yet the looming threats to mobile security are larger than petty thieves alone. Hackers and criminals who don't even need physical access to your device can crack its sensitive and confidential data. Unless proper precautions are taken, intruders can "sniff" personally identifiable information over wireless networks or worse still, install mobile malware – malicious applications that hijack your mobile device to do all sorts of nefarious things.

Your employer or service provider has supplied this booklet to educate you about the potential dangers of mobile computing and to impart **10 simple things you can do to protect yourself and your organization**.

To do this, we'll need some help.

Joe IT here already knows a lot about mobile device security. It's his job to secure the corporate network and all of the hardware that runs on it, like laptops and servers. He's worried about all the smartphones, tablets and other mobile gadgets that are now accessing his precious network and the sensitive business data it protects.

May we also introduce Joe Worker, or "JW" for short. He's just like you. JW loves the portability and convenience of mobile computing, and carries his favorite gadget with him everywhere. He wants to use his personal device at work and can't understand why Joe IT shivers at the very idea.

Now that introductions are out of the way, let's look first at...

The Growth of Mobile Computing

42%

Growth of the smartphone market between 2010 and 2011. By mid-2013 smartphones could make up **50%** of overall mobile phone sales.[2]

40 MILLION

Number of tablets sold in less than 2 years, a feat which took the smartphone 7 years in the U.S.[3]

1 BILLION

Number of iOS and Android smartphones and tablets expected to be activated by the end of 2012. Since 2007 there have been more than **500 million** activated.[4]

3.1 BILLION

Estimated number of mobile broadband subscribers by 2015, compared to **848 million** The number today of mobile broadband subscribers worldwide surpassed that of fixed broadband subscribers at the end of 2010.[5]

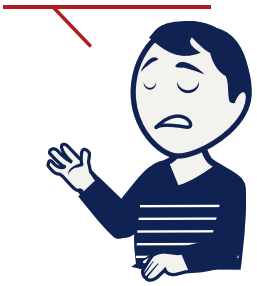
40 BILLION

Estimation of how many applications have already been downloaded from the Apple iTunes store and Android Marketplace. The average smartphone user is beginning to spend more time in mobile applications than they do browsing the web.

It's clear that consumers are going mobile in huge numbers. Now, they want that same great mobile experience they have at home to come with them to the workplace.

Joe IT, you can certainly understand why JW loves his iPad. But JW, you need to appreciate that IT organizations are struggling with how to advise employees about securing their smartphone or tablet before it's used as a business tool. Allowing staff to use any mobile device they choose is becoming a differentiator for companies seeking to hire great employees, but it can become a nightmare for the IT department who is responsible for protecting valuable customer data and company intellectual property (IP).

I certainly don't understand the danger here!
I mean, it's a smartphone.
Nobody attacks mobile phones.



Actually JW, they do.

Some hackers and criminals follow the crowd because they want to victimize the largest number of people possible. Other cyber criminals follow the money, sniffing out financial spoils from the unprotected. Your smartphone, if unprotected, makes you easy pickings and if it's connected to your organizations network it simply becomes a conduit to all the proprietary data stored there. With mobile usage reaching critical mass, ensuring the security of your mobile device has never been more important.

It is not inconceivable to predict a future where smartphone and mobile device usage becomes the de-facto standard for businesses and consumers alike, surpassing the use of desktop and laptop PCs.

We're not there yet, but we're heading in that direction.

Unfortunately, one could argue we're presently in a state of mobile insecurity.

Good point, Joe IT.
To understand the threat better, it's important to review some more stats on...

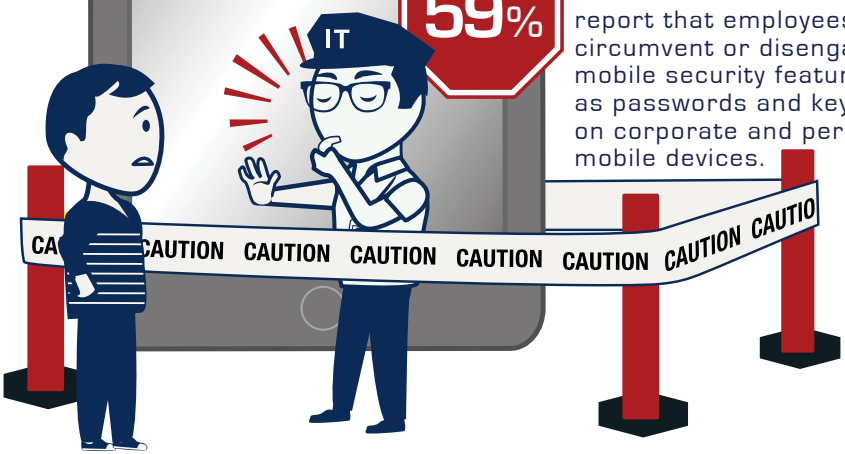
The State of Mobile Security

According to one recent study of IT professionals: [6]

51% of the organizations surveyed had experienced data loss from employee use of insecure mobile devices, within the past year.

59% reported that their organizations experienced an increase in malware infections as a result of insecure mobile devices in the workplace.

59% report that employees circumvent or disengage mobile security features, such as passwords and key locks, on corporate and personal mobile devices.



In fact, a single successful mobile attack can cripple your favorite device, result in the loss of personal or business data, open the door to possible identity theft or worse, result in financial loss to either you or your organization.

Consider the potential damage:

One study examined 855 data breaches in 2011 alone that were responsible for 174 million records stolen.[7]

174 million stolen!

The costs of a single data breach are daunting: now up to $194 per compromised record, or an average $5.5M per incident.[8]

$5.5 million per incident!

You certainly don't want your mobile device to contribute to those statistics.

Besides the threats of data loss, financial robbery and ID theft, victimized enterprises risk potential lawsuits from disgruntled users, regulatory action from government bodies, and severe damage to their brand and reputation. For public companies, data breaches can hammer their valuation. After its widely reported breach incident in March 2012, **Global Payments** stock dropped 13 percent before trading was halted.[9]

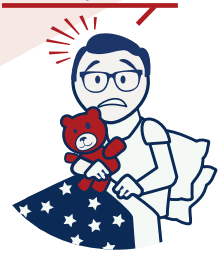
Among all organizations that reported the source of breach incidents in 2011, **40 percent** were traced back to application security issues such as cross-site scripting and SQL injection.[10]

But I download all my apps from the official marketplace. What do you mean they aren't secure?

Unfortunately JW, the security controls that the app marketplaces have in place to vet the safety of their offerings are woefully inadequate. Apple strictly controls its app store and inspects which apps are approved for listing, but it's not clear exactly what security measures they are checking for. Android is more open with more distribution channels including third-party marketplaces. While choice is good for Android users, app security is an afterthought – it's up to the community of users to "report suspicious apps". That approach has been a boon to malware authors. Even security researchers were startled to find that Android malware (malicious apps) grew **3,325 percent** in 2011 alone.[11]

No need to worry. I'd never buy a malware from my app store.

This is the kind of stuff that keeps me up at night…



App stores have been very quick to remove malware once discovered, but that's typically after the damage is done. They need to get serious about vetting code before it is made available for download. Users can't rely on the "halo effect" of a reputable app store or trust fellow user reviews to rate the reputation of app vendors when it comes to mobile code security. In some app stores, legitimate apps have been pulled down by hackers, corrupted with malware, and then reposted without the original publisher's knowledge.

You may think you are installing a harmless game or utility, then… Gotcha!

That's right. Malicious apps behave in insidious ways.

That innocent looking app might in reality be:

Hidden spyware that tracks your activities like texting, emails, calls, location, contacts, or browsing history – and sends it all to the crook.

Malware that actually generates unauthorized premium rate calls, texts or purchases – all charged to your wireless bill.

Phishing screens that look like legitimate logins to a known service like online banking or social networks but are instead clever methods to steal your credentials.

Processes that run completely in the background, conceal themselves, or lie in wait for certain behaviors like an online banking session to strike.

Wow, nasty stuff.
You mean while I'm playing sudoku,
my smartphone might be playing
fast and loose with my privacy?

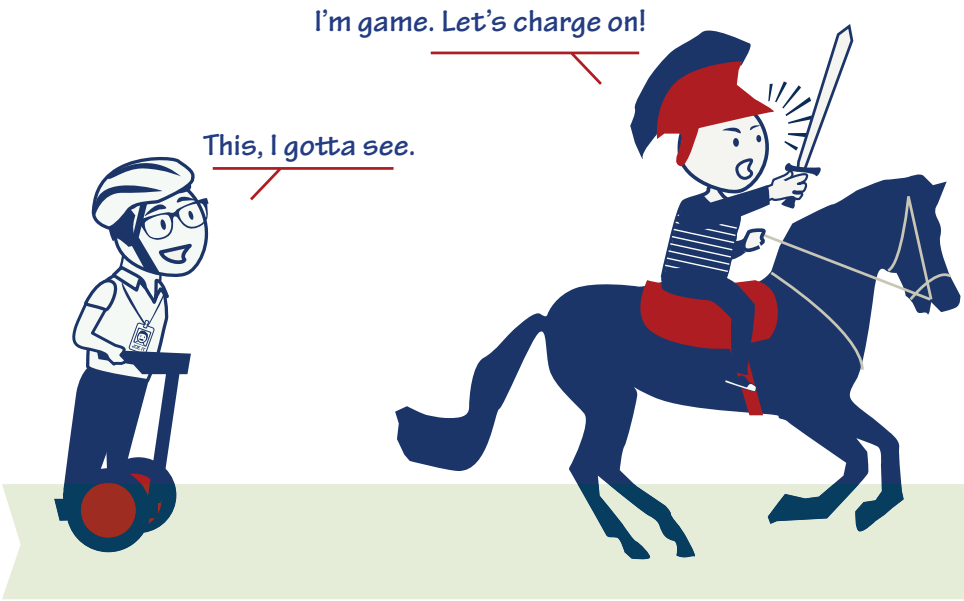
Not only your personal information, but maybe your organization's as well. If you're bringing your iPad and smartphone on the road with you, connecting remotely to the office network or email server, sending confidential files and other sensitive information back and forth, carrying the customer list with you, or any number of other normal workplace behaviors – you're putting the whole organization at risk.

Guilty as charged… I guess.
But I don't know how to secure my smartphone.
That's what I have Joe for, isn't it?

I can help…
but I can't follow you around all day.
I need help from you too.

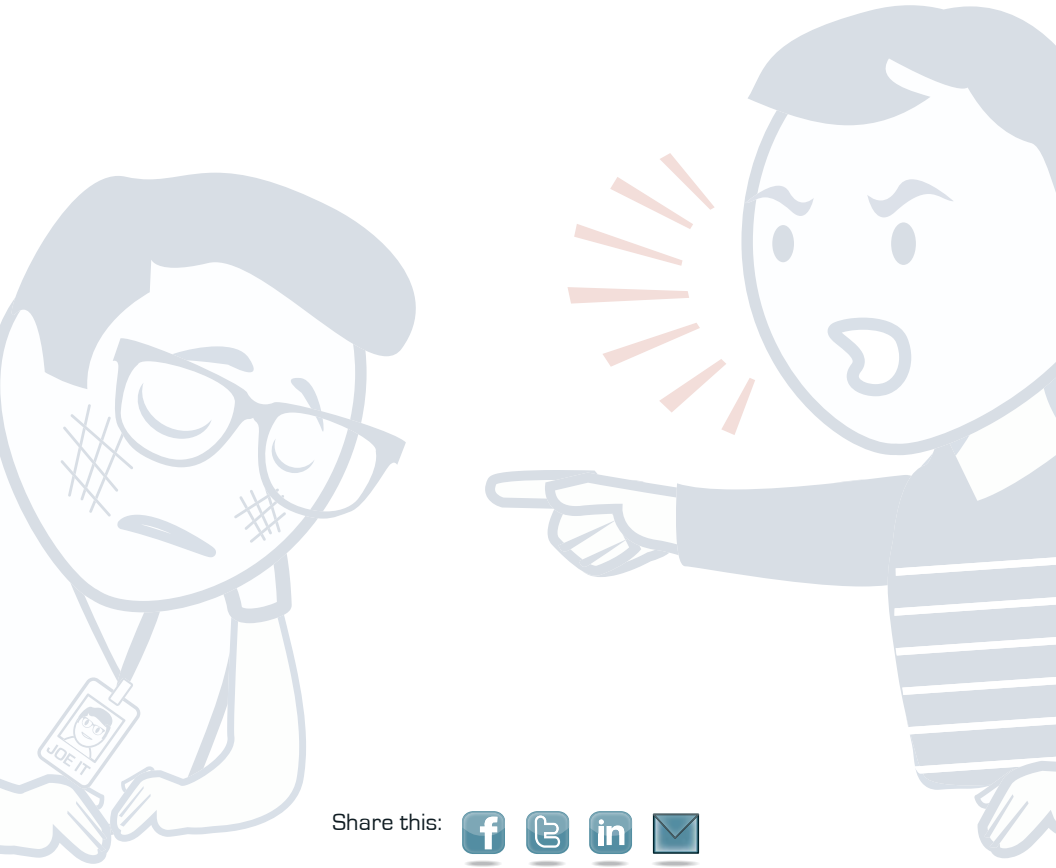
It doesn't matter if you work in sales, HR or accounting – **it's everybody's responsibility to protect the organization's sensitive data**. Neither of you would want confidential information about your customers falling into the wrong hands, would you? IT can lead the mobile security charge, but Joe can't be expected to take on complete and full responsibility – especially if it's your personal mobile device.

Maybe it would be helpful to review the roles each party plays in the mobile security problem? Then you'll see how each of us plays our part in securing the organization's data from those who would do us harm.



PART TWO

Whose Job is It, Anyway?



Share this:

Similar to the PC security market,

there are a number of players responsible for delivering mobile security. These include:

1. Mobile telecom service providers that own the infrastructure (e.g. AT&T, Verizon)

2. Hardware manufacturers that provide the devices (e.g. Apple, Samsung, LG)

3. Mobile operating system (OS) vendors that provide device software (e.g. iOS by Apple, Android by Google)

4. Mobile app developers (e.g. too many to count, but think Rovio, the creators of Angry Birds)