With business continuing its shift from the desktop to smartphones and tablets, more than half of all companies now have sensitive information stored on mobile devices. But despite a corresponding rise in malware, phishing and other mobile threats, an astounding number of firms are ignoring warnings to implement security safeguards. They’re about to learn that the dangers are very real.

BY JASON ANKENY • ILLUSTRATIONS BY HITANDRUN
Jose Quintero knows all too well how much havoc a lost smartphone can wreak on a business. Years before he became director of information services at law firm Bush Gottlieb, Quintero worked as an automated systems analyst at an international firm with more than 700 attorneys across 15 offices. Unknown to Quintero and others on staff, one of those attorneys transferred all his documents, photos and data from his laptop to his new iPhone, failing to back up the content onto a separate hard drive in the process.

“Not long after, his laptop got hit with a virus. All of its data was lost,” Quintero recalls. “Then he lost the iPhone, and all of that data was lost forever.” Quintero refused to let history repeat itself when he joined Glendale, Calif.-based Bush Gottlieb last year. He enlisted mobile security solutions firm Marble Security to implement a cloud-based, companywide program safeguarding phones and tablets against loss and theft, as well as malware, Trojans, phishing attacks and other cyber threats.

“Mobile devices are prac-
Quintero says, “We have people reviewing sensitive documents and sending documents to colleagues. Mobile security technology allows me to lock down a device that’s been stolen or gone missing, wipe it remotely (i.e., delete all the files) and change the password if necessary. The hardware is not the concern here. It’s the data.”

Mobile security isn’t a concern that’s exclusive to law firms, healthcare providers and other verticals dealing with hypersensitive client data. Fifty-three percent of companies surveyed by internet security provider Check Point Software Technologies store sensitive customer information on mobile devices, and that percentage is expected to skyrocket as business continues to migrate from the desktop to phones and tablets. This is especially true given how many organizations are embracing money-saving “bring your own device” (BYOD) policies that allow staffers to use their own Apple iOS and Google Android products for professional purposes.

Roughly 60 percent of small businesses have implemented BYOD initiatives, according to a recent survey conducted by Spiceworks, an online community for IT professionals. But more than half of small to midsize enterprises that support BYOD are either unaware of or defenseless against mobile security hazards like malicious apps, domain-name system poisoning (changing an IP address to divert visitors to a rogue website) and jailbroken devices (in which the user removes operating system limitations imposed by manufacturers and network operators), a Marble Security survey reveals.

SMALL BUSINESS AT RISK
While cyber criminals have historically targeted large enterprises, that dynamic is changing as corporations make heavy investments to apply more sophisticated security measures. The move has pushed digital predators’ focus to smaller, more vulnerable targets: In its most recent findings, cybersecurity firm Symantec reported that in 2012, 31 percent of targeted attacks were aimed at businesses with fewer than 250 employees, up from 18 percent the previous year.

Shockingly, many businesses don’t seem to care. Among 1,000-plus U.S. SMBs surveyed by Office Depot and digital-security giant McAfee, 66 percent expressed confidence that their data and devices are secure and safe from hackers, and 77 percent said they haven’t been hacked. Experts

---

VULNERABLE THINGS
As the internet expands, it’s not just your phone that will be hacked

The internet’s migration from desktop PCs to mobile devices is just the first stop on its journey to total hardware domination. Web connections are rapidly expanding beyond computing devices to everything from parking meters to refrigerators. Research firm BI Intelligence forecasts that the so-called Internet of Things will account for 9 billion device connections in 2018, roughly comparable to the number of smartphones, tablets, PCs, smart TVs and wearable computers combined.

As the internet bleeds into all corners of daily life, security concerns will follow. Researchers already have identified malware capable of hacking a car through its infotainment system and warn that something as seemingly innocuous as a Wi-Fi-enabled digital picture frame could allow intruders to access a home’s entire network of connected devices and private information.

“Old technologies were not built to be interconnected and slapped on the internet, so they’re not the most secure things,” says Adam Ely, co-founder of San Francisco-based mobile data security vendor Bluebox Security. “That means we’re going to see attacks by people looking to compromise these devices.”

Because hackers typically target devices that have achieved widespread adoption, it isn’t worth losing sleep over Internet of Things security—at least not yet. But as connected devices become commonplace, watch out.

“Just like we didn’t have PC viruses and then suddenly we did, we will have viruses for the Internet of Things,” Ely says. “Once any device becomes popular and powerful enough, it will be attacked.”
say the discrepancies between the Symantec and McAfee reports suggest that many small businesses are not even aware they’ve been attacked. “Small businesses feel that cyber threats are not relevant to them and that attackers are only going after larger companies. But they have many of the same valuable customer assets, like credit card numbers and e-mail addresses, just on a smaller scale,” says Adam Ely, co-founder and COO of San Francisco-based mobile data security vendor Bluebox Security. “SMBs typically run fast and loose to get things done in a cost-effective way, but they have to realize that security is part of running a business.”

The shift to mobile computing dramatically expands the risks facing small businesses. Security-software firm Trend Micro identified 1 million malicious and risky Android applications in the third quarter of 2013, surging from 425,000 at the beginning of the year. But Ely maintains that internal data leaks pose an even greater peril. “It’s a different world from 10 years ago, when only people with certain permissions were allowed access to data,” Ely says. “Now we’re in a situation where data is spread across Salesforce and Dropbox, and moving around everywhere it can possibly creep into. That’s why small businesses must reduce risk by managing data and applying basic controls like device security and data security.”

BYOD CONCERNS
The rise of BYOD further complicates the issue. It’s a strategy that makes obvious sense for businesses: Networking titan Cisco reports that U.S. companies can save as much as $3,150 per employee per year by implementing comprehensive BYOD programs that allow personal smartphones and tablets to access all the resources employees need to perform their duties. The savings derive from estimated productivity increases as well as from shifting mobile hardware and services costs to employees: The average BYOD staffer spends $965 on devices and an additional $734 per year on wireless network coverage, Cisco says.

But because employees own these devices outright, they feel free to use them however they wish—activities that may include downloading potentially nefarious applications from third-party storefronts or jailbreaking their phones. Some staffers also may balk at letting employers implement compre-
THREAT #3

Smishing

SMS-based phishing ("smishing") schemes send consumers text messages containing a link to a fraudulent website or phone number created to collect personal information such as bank-account data.

Protect yourself: Avoid clicking links within text messages, especially if the sender is someone you don’t know. Never respond to texts that request personal data, and beware of messages sent from “5000” or other numbers that are not conventional 10-digit phone numbers.

---

hensive security controls on their devices.

“Small businesses need to focus on the people-and-process side of mobile security,” says Sean Ginevan, director of business development for Mountain View, Calif.-based enterprise mobility management provider MobileIron. “It’s critical to ensure that the end-user is opting in and trusts their IT department. Recent studies say that end-users believe IT has more Big Brother tendencies than are actually possible, and that causes wariness to participate [in mobile security efforts].”

Ginevan says employers should clearly define the security protocols in place for BYOD employees, assuring them that the goal is to safeguard their mobile devices against hackers, theft and loss, while guaranteeing that IT staffers have no interest in probing any personal content stored alongside professional tools. That means implementing mobile security protocols that protect sensitive business data without monitoring personal usage, complete with tools to remotely wipe business information, documents and e-mail accounts in the event a device is lost or stolen, or if the employee moves on to another organization.

“Building a relationship with the end-user is essential,” Ginevan says. “You need to assure them that you’re not going to look at photos of their family or look at their music library, but you will make sure their device is properly secured.”

WHAT CAN BE DONE

So what kinds of mobile-device checks and balances should small businesses implement? Marble’s cloud-based security client application integrates real-time intelligence derived from machine data, as well as mobile user and device attributes like location, installed apps and network connection data, to apply dynamic risk scores to each device. The result is that IT administrators and users can detect threats and remedy them instantly. The solution costs $3 per user per month and spans all of each user’s devices.

“We have a security-threat lab constantly researching new threats, and our dynamic data feeds are updated in real time,” says David Jevans, Marble’s founder and CTO. “That’s the beauty of running security in the cloud—we can update our data feeds in real time.”

MobileIron’s Anyware solution touts enterprise-grade data privacy protection tools for company e-mail, apps and content. The cloud-based service offers easy configuration and personalized app and content catalogs, as well as app ratings and recommendations from co-workers. Firms running the Salesforce platform may use Anyware to block untrusted devices, wipe business apps when required, configure Wi-Fi and e-mail, and manage all mobile devices companywide via the Salesforce interface.

“We can tailor Anyware to tackle the SMB use case for about the price of a cup of coffee per month—$4 per device,” MobileIron’s Ginevan says. (At press time, Bluebox was in beta and unable to divulge specifics on its programs and pricing.)

While that price may feel steep to some SMBs, at the very least they can follow the advice to put into practice some kind of written security-enforcement policy, even if they opt against adopting premium-price protections. “Telling employees, ‘Don’t jailbreak your phones’ or ‘Don’t download these apps’ is better than nothing,” Jevans says.

Still, he estimates that 75 to 80 percent of companies have yet to put even bare-minimum security protocols in place.

Those laggards are likely going to be sorry. The issue is only going to grow more serious as mobile technology expands and more of our personal, financial and business lives flow through smartphones and tablets. With so much sensitive and meaningful data stored on each device, any kind of data breach has the potential to be catastrophic. ☎

THREAT #4

Unsecured Wi-Fi attacks

Shopping, banking or even accessing company documents over unsecured Wi-Fi connections can enable hackers to access your phone or tablet and steal its data.

Protect yourself: Limit all online banking and shopping to your secure home or office network. Eschew voice-over-IP apps and instant messaging services that automatically connect to nearby hotspots.