Small and Midsize Business Guide to Mobile Security

The increasing mobility of workers is a fact of life for small and midsize businesses. Employees are using their mobile devices for both personal and work activities – whether the company sanctions them or not – and are also expecting more flexibility and mobility when it comes to corporate-issued PCs and laptops. The idea of workers accessing business data from any location, at any time, on any device is now at hand.

SMBs must face the reality that all of this increased mobility is making their businesses far more vulnerable to security threats. Just how vulnerable are SMBs, and what do the threats look like? Here are some of the questions you may be asking.

How severe are the threats to mobile devices? What are the characteristics of these threats, and how rapidly are the risks growing?

Many SMBs believe they won’t be targeted by cybercriminals because of their size. This is a fallacy. Since the beginning of 2010, 40% of targeted attacks have been aimed at SMBs, versus 28% launched against large enterprises.¹ What’s more, cybercriminals are increasingly attacking mobile devices: The number of malware variants aimed at mobile devices rose from about 14,000 in 2011 to 40,000 in 2012, an increase of about 185% in less than a year, according to a congressional report by the U.S. Government Accountability Office.

There is no single characteristic that is common to all of these new threats, except that most of them seek to exploit user behaviors and security vulnerabilities that many SMBs haven’t yet addressed. They have also become far more highly coordinated and sophisticated. Malnets, for example, use search engines, social networks, e-mail and other popular platforms to direct users to sophisticated infrastructures that can launch a series of zero-day attacks across a long period of time. The average business faces 5,000 of these threats every single month, and a rapidly growing number are coming from mobile devices – nearly 15% of total malnet threats in 2011.²

What are the specific vulnerabilities of mobile devices versus traditional PCs?

What about BYOD?

Given all of these threats, why should I support BYOD? And why should I allow users in my organization to use social media sites?

How do I go about evaluating solutions for mobile devices?

Why should I consider a cloud-based solution for mobile security?

What are the advantages of Webroot’s approach to mobile security?

What’s my next step in addressing the challenges of mobile security?

---

¹ SMB Threat Awareness Poll, Symantec, November 2011
² “Ten common mobile security problems to attack,” PCWorld, September 21, 2012
³ Blue Coat Systems 2012 Web Security Report
FAQ

How severe are the threats to mobile devices? What are the characteristics of these threats, and how rapidly are the risks growing?

What are the specific vulnerabilities of mobile devices versus traditional PCs?

What about BYOD?

Given all of these threats, why should I support BYOD? And why should I allow users in my organization to use social media sites?

What are the basics I need to know about delivering proper security for mobile devices and mobile workers?

How do I go about evaluating solutions for mobile devices?

Why should I consider a cloud-based solution for mobile security?

What are the advantages of Webroot’s approach to mobile security?

What’s my next step in addressing the challenges of mobile security?

What are the specific vulnerabilities of mobile devices versus traditional PCs?

Mobile devices are a particular target of cybercriminals these days because many of these devices – smartphones and tablets, in particular – were initially aimed at the consumer market and thus don’t have the same types of embedded security features as PCs and laptops, which are often designed to meet more stringent business computing requirements. As noted in the GAO report, “Many mobile devices do not come pre-installed with security software to protect against malicious applications, spyware and malware-based attacks. . . Without it the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware and spam to lure users into revealing passwords or other confidential information.”

The security weaknesses of mobile devices make them particularly vulnerable (and attractive) as targets. If you look at Dark Reading’s Top 5 Deadliest Mobile Malware Threats of 2012, you’ll see that three of the top five threats on the list were aimed at devices using the Android operating system. For the record, the top five threats cited are the FakeInst SMS Trojan and its variants, SMSZombie, NotCompatible, Android.Bmaster and LuckyCat. How many of those are you aware of?

What about BYOD?

The growing acceptance of the bring-your-own-device (BYOD) trend means that many more users are utilizing the same device for both work and business activities. This exposes the organization to a wide range of risks, particularly if the organization hasn’t put in place any technologies or policies to manage and/or control the use of personally owned devices. Users are more likely to engage in dangerous behavior on their own devices – using social media, for example, or visiting vulnerable sites or downloading suspicious applications. Without corporate controls in place to protect users from themselves, they can put the entire company at risk. Other challenges inherent in mobile devices: They are smaller and, therefore, more vulnerable to theft or loss. In addition, they tend to be on all the time – unlike laptops or PCs, which generally go to sleep – so cybercriminals have access to them more frequently and at a wider variety of locations.

Given all of these threats, why should I support BYOD? And why should I allow users in my organization to use social media sites?

The basic answer is this: You have no choice. Employees will use their devices and social media anyway, so it’s much better for the business to control, manage and monitor usage than to just let it happen unencumbered. Besides, increased mobility can be a competitive advantage and a boon to employee productivity. It gives workers a lot more flexibility in terms of where and how they work, and done right, increased mobility can improve worker morale and lead to a better work environment.

What are the basics I need to know about delivering proper security for mobile devices and mobile workers?

Here’s a simple checklist of the steps IT organizations must take:

1. Ensure devices are secure
FAQ

How severe are the threats to mobile devices? What are the characteristics of these threats, and how rapidly are the risks growing?

What are the specific vulnerabilities of mobile devices versus traditional PCs?

What about BYOD?

Given all of these threats, why should I support BYOD? And why should I allow users in my organization to use social media sites?

What are the basics I need to know about delivering proper security for mobile devices and mobile workers?

How do I go about evaluating solutions for mobile devices?

Why should I consider a cloud-based solution for mobile security?

What are the advantages of Webroot’s approach to mobile security?

What’s my next step in addressing the challenges of mobile security?

What SMBs should be looking for are solutions that are focused strictly on mobile security needs, while delivering simple manageability, protection and performance at a cost-efficient price point. Most SMBs don’t have the resources to develop expertise in security, the changing threat landscape and all of the myriad business and technical issues involved in deploying mobile solutions. Therefore, it is critical that whatever solutions you choose are both easy to deploy and simple to manage. In this environment, there are significant benefits to working with an expert partner that will help you deploy the right solutions.

Why should I consider a cloud-based solution for mobile security?

A cloud-based solution will give you that expert partner to work with and provide the fastest, most cost-efficient and comprehensive approach for addressing mobile security. With a cloud solution, you won’t have to purchase any hardware or software, and you won’t have to hire additional staff to achieve the expertise you need to meet the challenges of today’s cyber threat landscape. Your cloud partner will provide that for you. The key is to recognize that not all cloud-based services are the same and to make sure the one you choose is focused on the specific challenges of mobile security. You will also want a mobile solution that seamlessly integrates with your existing endpoint solution and offers “true” cloud security by using the cloud to gather threat intelligence from endpoints all around the world.

What are the advantages of Webroot’s approach to mobile security?

Webroot Mobile Protection is an innovative cloud-based security solution focused specifically on the mobile security needs of small and midsize businesses. It
**FAQ**

How severe are the threats to mobile devices? What are the characteristics of these threats, and how rapidly are the risks growing?

What are the specific vulnerabilities of mobile devices versus traditional PCs?

What about BYOD?

Given all of these threats, why should I support BYOD? And why should I allow users in my organization to use social media sites?

What are the basics I need to know about delivering proper security for mobile devices and mobile workers?

How do I go about evaluating solutions for mobile devices?

Why should I consider a cloud-based solution for mobile security?

What are the advantages of Webroot's approach to mobile security?

What’s my next step in addressing the challenges of mobile security?

Includes a wide range of mobile protection features, including advanced antivirus, secure Web browsing, a lost device protection mechanism, device lock, device wipe, device scream, device locate and a SIM card lock, among others. The Mobile Protection solution is integrated as part of the Webroot SecureAnywhere Business portfolio, so it works seamlessly with Webroot's Endpoint Protection and taps into the Webroot Intelligence Network for cloud-based advanced threat detection and prevention. With Webroot Mobile Protection, SMBs can manage security for all mobile devices, as well as PCs, from a single console. The solution is infinitely scalable and uses a thin client that has virtually no impact on device performance.

What’s my next step in addressing the challenges of mobile security?

For many SMBs, the first step is to simply acknowledge that the threats of cybercrime are real and must be addressed, particularly as increased mobility and BYOD expose a whole new range of vulnerabilities. Once you’ve acknowledged that, yes, you may have a problem, you can start planning the steps you need to take to address it, including developing mobile policies and establishing a real plan for cyber security. That’s when it’s time to contact Webroot, an expert partner that can help you put the right plan in place and implement the most efficient, cost-effective and secure solution for your increasingly mobile business environment. When should you get started? The threats are out there now, and they are multiplying every moment. Today would probably be a pretty good time to begin.