Commissioned Study

SURVEY:

Mobile Threats are Real and Costly

WEBROOT®

Introduction

A lack of integrated mobile security is costing companies in terms of everything from lost productivity to lost data. Cyber criminals are also increasingly targeting mobile workers as easy access portals to a company's backend IT infrastructure. As the popularity of employee-owned devices in the workplace continues to grow, an integrated mobile defense needs to be supplemented with a coherent yet simple BYOD (bring your own device) management strategy.

Webroot recently conducted research to assess the state of mobile security in organizations throughout the United States, the United Kingdom and Australia. The study—which focused on companies that provide smartphones and tablets or allow employees to use their personal mobile devices—found that mobile security is a high priority for almost half of the companies and mobile threats increased help desk support and consumption of valuable IT resources.

83% of respondents believe that mobile devices create a high security risk within the corporate environment.

The proliferation of mobile devices introduces new security risks for organizations of all sizes. Mobile devices are not only increasingly subject to the same threats as PCs, but they are also easily lost or stolen. In fact, an overwhelming 83% of respondents believe that mobile devices create a high security risk within the corporate environment.

Key Findings

- 62% of companies with company-owned or employee-owned mobile devices reported significant increases in demand for help desk support to repair, replace or manage the security of smartphones and tablets in the company, consuming as much as 36% of one help desk technician's time resolving these issues each month.
- 60% required additional IT resources to manage mobile security, resulting in higher costs.
- More than half reported mobile threats reduced employee productivity and disrupted business activities.
- 66% agree that the management of mobile device security is a great burden on IT resources.
- 47% of BYOD companies have implemented mobile security, but only 40% of BYOD companies with fewer than 100 employees have mobile security.

Study Overview

IT professionals are seeing more mobile devices in their environments every day. The study also confirmed what is obvious to most IT professionals—BYOD has become pervasive. The results show that 73% of companies have a mix of company and employee-owned smartphones and tablets.

73% of companies have a mix of company and employee-owned devices.

As workers increasingly want to use personal devices at work and need to use their company-issued devices during personal time, IT faces new challenges. For example, it is hard to know where to draw the line on enforcing security and usage policies when the organization does not actually own the device. In heavily regulated sectors (Healthcare, Financial Services, Pharmaceutical, Education, Government, etc.) this blurry boundary between company and personal also makes it more difficult to ensure compliance with government and industry regulations.

Managing BYOD is challenging

While users of employee-owned mobile devices might not want corporate IT to manage their data, they expect and need IT to protect it. Mobile malware threats—often the same sophisticated threats designed to steal data from PCs—are proliferating rapidly. Whether it is company data stored on an employee's device or the employee's personal private data, IT has a responsibility to protect this information against theft.

83% say managing BYOD is challenging

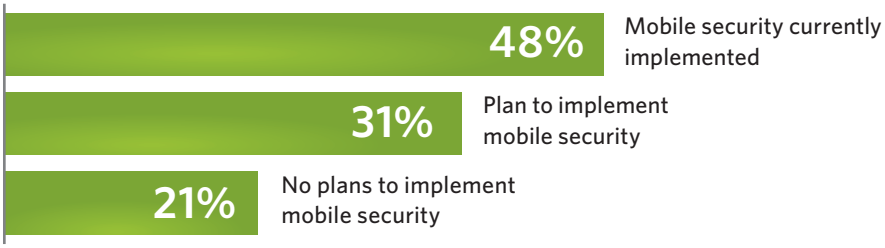
	Total Number of Employees				
Agree (Strongly, Somewhat, Slightly)	**10–19**	**20–99**	**100–499**	**500+**	**Total**
Managing the security of Bring Your Own Devices is challenging.**	75%	**83%**	**87%**	**84%**	**83%**
The cost savings of allowing employees to use their personal mobile devices at work outweighs the security risks.	63%	70%	62%	59%	64%

Business Mobile Security. August 2012. N=517 mobile security decision-makers in companies with 10 or more employees. ±4.3 pts. **p<.01

Actual implementation of mobile security lags the need to reduce risks

Despite the obvious awareness of the risks, less than half of participants said they had implemented protection for mobile devices. More surprisingly, 21% said they had no plans to implement mobile security.

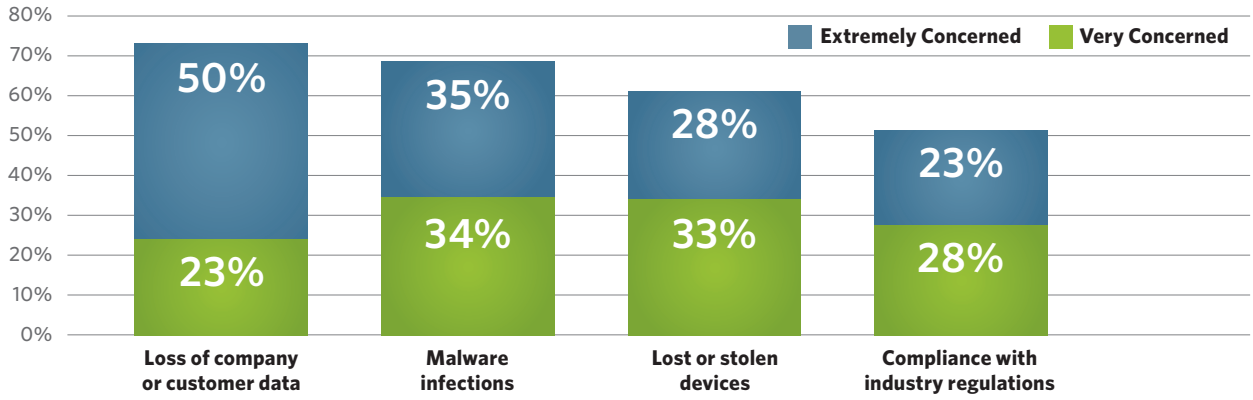
Less than half of companies have put mobile protection in place



Concerns about mobile threats and actual impacts

Specifically, what mobile security issues keep IT professionals awake at night? By far the biggest worry is loss of company or customer data, with 73% of respondents saying they were 'extremely concerned' or 'very concerned.' Malware and lost or stolen devices also comprise major concerns for almost two-thirds of companies, with compliance issues trailing with only about half of respondents saying they are extremely concerned or very concerned. However, since today's more malicious malware is often designed to steal data, data loss represents a consistent thread running through all of these key concerns.

Mobile data loss is a major concern



Business Mobile Security. August 2012. N=724 endpoint and mobile security decision-makers in companies with 10 or more employees. ±3.6 pts. **p<.01 (choices: not at all concerned, slightly, somewhat, very, extremely concerned)

The bigger the user base the bigger the risk

Research also shows that the more mobile users you have the more at risk you are of breaches or incidents. Larger organizations, those with 500 or more employees, had the highest number of problems. Among the most common issues, 67% had dealt with lost or stolen mobile devices and 32% had experienced mobile malware infections, creating widespread concern about the business impact of employee-owned devices within the enterprise.

Mobile threats hit large companies harder

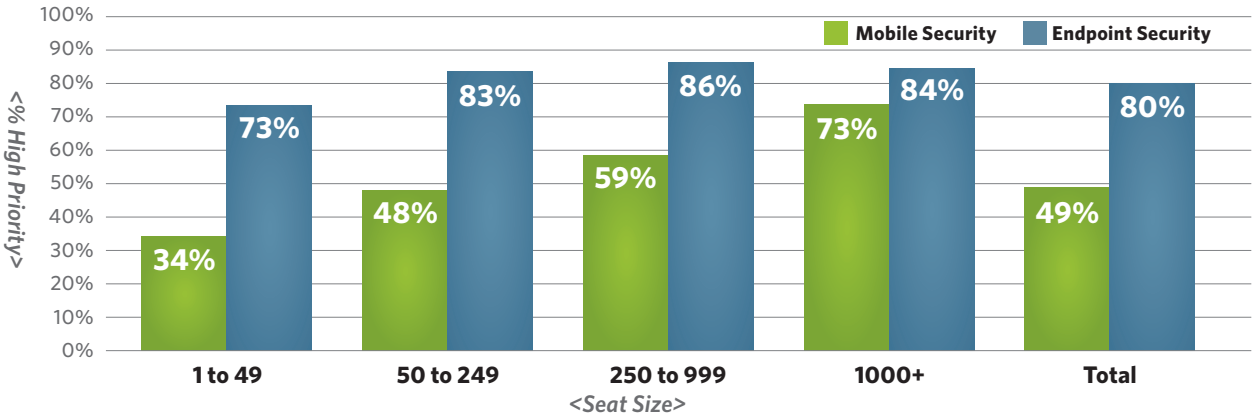
Experienced the following problems via smartphones or tablets in the past 12 months:	**Total Number of Seats** (desktops & laptops)				
	1–49	**50–249**	**250–999**	**1,000+**	**Total**
Lost or stolen devices**	24%	42%	**65%**	**67%**	44%
Malware infections (e.g., virus, spyware, Trojan, keylogger, system monitor, root kit)**	15%	23%	**32%**	**32%**	23%
Company or customer data compromised or stolen**	4%	6%	11%	**17%**	8%

Business Mobile Security. August 2012. N=660 endpoint and mobile security decision-makers in companies with 10 or more employees. ±3.8 pts. **p<.01

A top concern but a secondary priority

While mobile workforces are growing along with the prevalence of mobile devices, traditional endpoint security still receives more attention. However, larger organizations are quickly putting almost equal emphasis on protecting mobile devices as on protecting PCs. This data shows many segments are currently at risk because they have no protection in place for mobile devices.

High Priority vs. Seat Size



But overall, endpoint security is a higher priority

Business Mobile Security. August 2012. N=724 endpoint and mobile security decision-makers in companies with 10 or more employees. ±3.6 pts. **p<.01 (choices: not a priority, low, medium, high priority)

Companies are suffering the consequences

Data in chart below clearly shows the consequences of not having a mobile security solution in place. For example, companies with no mobile security are almost twice as likely to pay regulatory fines.

Impacts higher for companies with no mobile security

What impact did the mobile threats have on your company in the past 12 months?	**Experienced Mobile Malware, Lost/Stolen Devices, or Compromised/Stolen Data**		
Severe, Major, or Moderate Impact	**No Mobile Security**	**Mobile Security Implemented**	**Total**
Increased help desk time to repair damage	66%	57%	62%
Additional IT resources needed to manage mobile security	63%	58%	60%
Reduced employee productivity	58%	51%	55%
Disrupted business activities**	**56%**	44%	50%
Devices subscribed to premium pay-for-services**	**47%**	30%	38%
Company had to pay regulatory fines**	**27%**	14%	20%

Business Mobile Security. August 2012. N=360 companies in the US, UK, or Australia that experienced issues with mobile security. ±5.2 pts. **p<.01 (5-point scale: no impact, minor, moderate, major or severe)

One possible explanation for the lack of adoption is the amount of time required to implement mobile security. Without a solution in place that offers integrated protection for both traditional endpoints as well as mobile devices, device management becomes quite onerous at 57 hours per month.

Over 40 hours per month to manage mobile devices

22 hrs **Manage the security of the devices**

19 hrs **Provision devices**

16 hrs **Replace lost or stolen devices**

} 57 hrs

What can organizations do?

Webroot advises companies to implement a mobile security solution that includes three elements: device control policies, device-level security and mobile workforce security training. This includes taking the following steps to reduce the risks associated with BYOD.

Establish device control policies

Create a policy that governs how your corporate IT staff can gain control over a personal device while maintaining your network security. Include information about how to keep personal information private (e.g., via a mobile device backup strategy such as containerization that doesn't touch personal data) and define corporate ownership over data and applications.

Enforce device-level security

Both corporate-owned and personal devices should have secure passwords and screen locks; document this requirement in your mobile device policies. In addition, require that personal and corporate mobile devices maintain up-to-date, corporate-approved (and preferably corporate-managed) security software installed to guard against malware and other security risks.

Develop and deliver mobile workforce security training

Security training will keep your mobile workforce productive and prepared to be the first line of defense against malware and other security threats to their mobile devices. Spell out your corporate policies and include a participant sign-off stating that they understand and will abide by the policies.

Let your business drive mobile device security policies and training

Business requirements and culture drive the policies, training and other upfront work you do to support your mobile workforce security needs.

Survey Methodology

Between July 30 and August 1, 2012 Webroot commissioned a study of mobile and endpoint security decision-makers in companies with 10 or more employees in the US, UK, and Australia. The scope of the research included both BYOD and company-owned mobile devices. Research Now provided respondents from their online panel of IT and business executives. A total of 725 responded to an online survey hosted by Qualtrics. The margin of error for the study is +/- 3.6 percentage points at the 95 percent level of confidence. 609 of the respondents were from BYOD (Bring Your Own Device) companies, organizations that allow employee-owned smartphones or tablets to access the company network for work purposes. The margin of error for the BYOD subsegment is ±4.0 percentage points.

About Webroot

Webroot is committed to taking the misery out of Internet security with its suite of Webroot® SecureAnywhere™ offerings for consumers and businesses. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held security organization based in the United States. Webroot has operations across North America, Europe and the Asia Pacific region. For more information, visit http://www.webroot.com or call 800.772.9383. Read the Webroot Threat Blog: http://blog.webroot.com. Follow Webroot on Twitter: http://twitter.com/webroot.

Webroot Headquarters:
385 Interlocken Crescent, Suite 800, Broomfield, Colorado 80021 USA

©2012 Webroot Inc. All rights reserved. Webroot, SecureAnywhere, Webroot SecureAnywhere, and the globe design are trademarks or registered trademarks of Webroot Inc. in the United States and/or other countries. Microsoft, Windows, Internet Explorer, Applocker, Forefront, and SmartScreen are registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks are the properties of their respective owners. Webroot is not affiliated with, nor has it or Webroot SecureAnywhere Business—Endpoint Protection been authorized, sponsored, or otherwise approved by Microsoft Corporation.