Enterprise Mobile Security Survey

Fielded December, 2010

threatpost

The Kaspersky Lab Security News Service

Executive Summary

Paul Roberts, Editor, Threatpost

There's evidence of a protection gap emerging in the mobile space. Just 31% of those surveyed said their employer required them to install security software on their smart phone.

– *Paul Roberts*
Editor, Threatpost

Enterprises Facing Security Gap with Mobile Devices

A Threatpost.com survey of 120 enterprise users found that smartphone adoption is going full steam, but security for those devices is a back burner issue.

If you're like millions of other workers, you've made the leap to a smartphone sometime in the last couple years. And, like most workers, you don't check your phone at the office door. Indeed: with 3G and 4G wireless connectivity, full Web browsers and a blossoming application ecosystem, smart phones offer a huge productivity boost for wired workers.

But a new survey out from Threatpost indicates that, while enterprises are embracing smart phones, security for the devices is lagging. Employees are using the phones to check e-mail, browse the Web and connect to company VPNs. But increased access to corporate assets hasn't marched in step with increased security, our survey suggests. Just 31% of those polled said their employer required some kind of security software for their smartphone. Just as concerning: almost a third of respondents - 29% - reported encountering mobile malware within their organization.

At issue is the proper response to the rapid, consumer driven adoption of smart phones and other multi function mobile devices. As Threatpost has reported, (http://threatpost.com/en_us/blogs/enterprises-riding-tiger-consumer-devices-120210) enterprises find themselves in a bind with these new tools, which users often purchase on their own and bring to the office regardless of company policy.

Our survey reveals the depths to which smart phones are penetrating enterprise networks. Almost all of our respondents noted some level of smart phone use within their organization, with RIM's blackberry the clear leader among mobile phone platforms. Blackberry was the choice of 71% of our respondents, followed by Apple's iPhone (55%), Google's Android (46%) and Windows Mobile (32%).

Malware researchers note the rapid increase in malware targeting mobile devices, while recent reports on Threatpost and elsewhere have noted the dangers lurking among the hundreds of thousands of applications that populate Apple's AppStore, Google's Android Marketplace and other mobile hubs. The coming years will bring with them a host of new, complex mobile malware.

Check out Threatpost's Mobile Survey for a peek at what the mobile security looks like today, and what may be just around the corner.

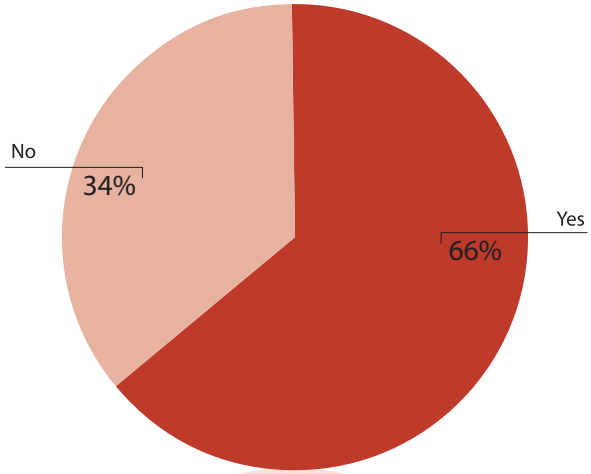
Threatpost readers tell us:

"Our network enterprise security is kept up to date and looks at data transfers through email closely. Only certain file types are allowed through from the phones. Most of them use laptops for serious file transfers or long email responses, and use their phones typically for quick email checks."

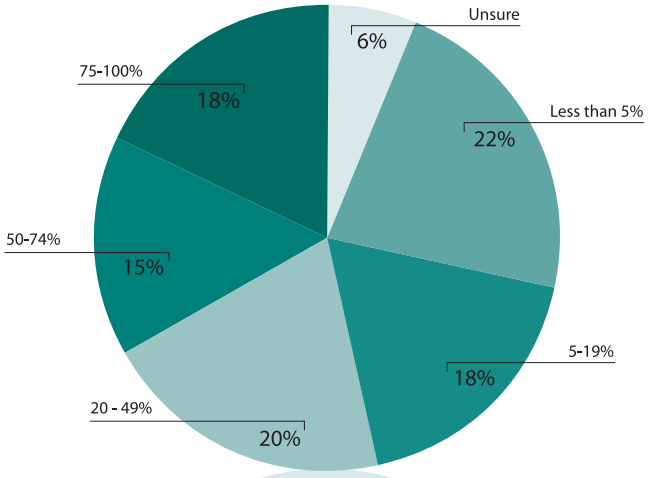
"My organization fits the medium business section and services other small and medium businesses. This threat is being completely ignored by my organization and we are not leading any of our clients to evaluate it. THANK YOU, for putting out this survey and I can't wait to see the results," one respondent wrote.

Enterprise Mobile Survey Results

Does your organization supply employees with smartphones?



What percentage of your employees have smartphones?

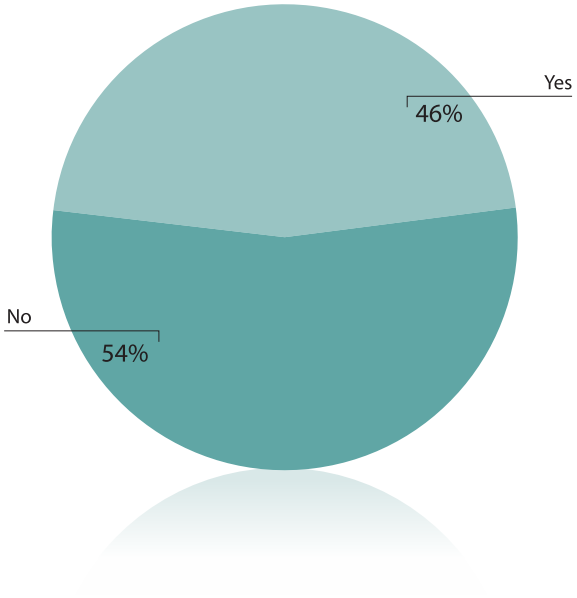


Threatpost readers tell us:

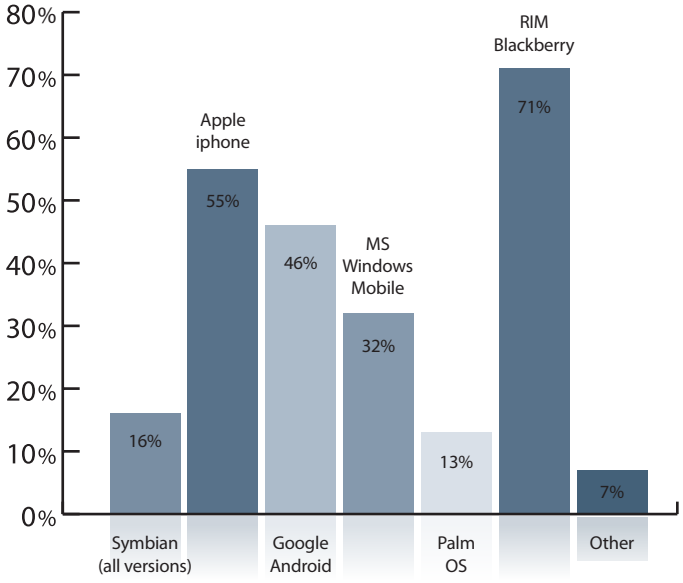
"We provide baseline assessments of devices, lockdown policies and constant brow beating of how insecure the devices are."

"There are still many employees who believe that smartphone security is not required or not an issue, which is difficult to explain on the possible dire consequences. They believe that because they are not using a "computer" as such that they are in a safe environment."

Does your organization support non-company issued employee smartphones?



The following mobile devices are used and supported within my organization.



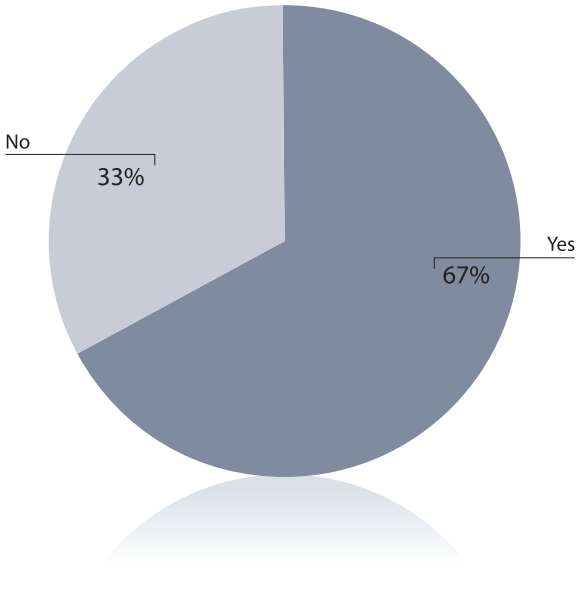
Editorial Review

What are employees using mobile devices for?

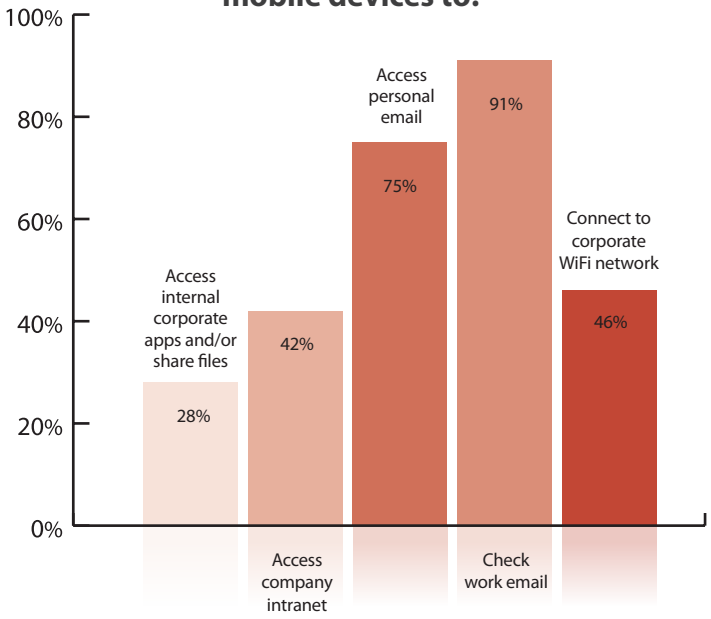
Fully 91% of those surveyed said they use their smart phone to check work e-mail with a strong majority, 75%, claiming to check personal e-mail with it. Smaller percentages of respondents said their smart phone was used to connect to the corporate wireless network (46%), company intranet (42%) or access internal file shares (28%).

But increased access to corporate assets hasn't marched in step with increased security, our survey suggests. Just 31% of those polled said their employer required some kind of security software for their smartphone. Sixty eight percent of those polled said their employer failed to provide security awareness training for mobile devices.

Does your organization provide any VPN or secure remote access tools for employees?



Employees in my organization use their mobile devices to:



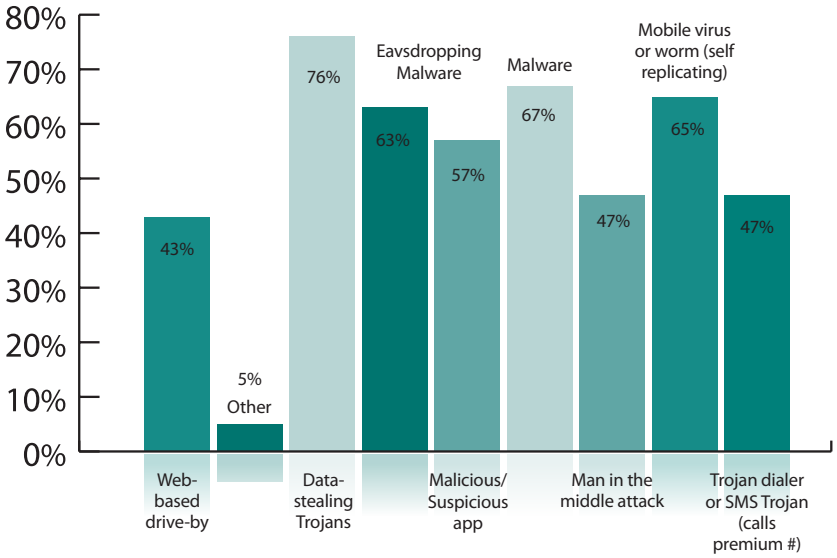
Threatpost readers tell us:

"If these things are built right with open code for all to see then the likelihood of getting malware and other unwanted software is immediately reduced."

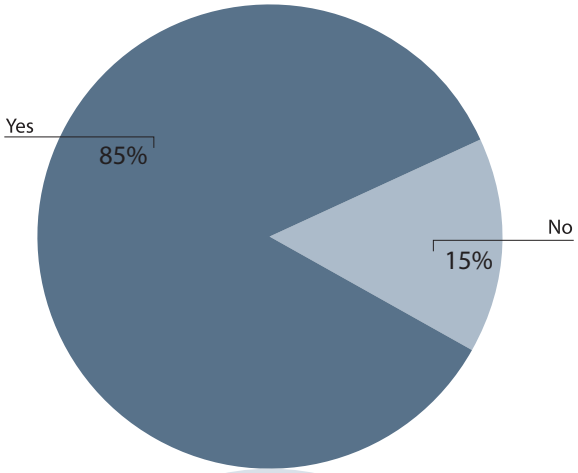
"Active mobile phones are not permitted in offices or meetings."

"I believe that it is a viable threat to mobile security. Soon computers will be left alone and mobile devices will be targeted since them now can do almost more than a computer."

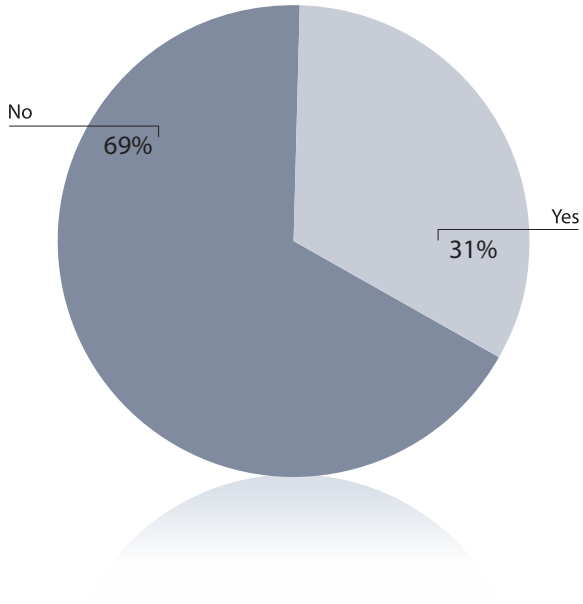
What mobile threats are you concerned with on employees smartphones?



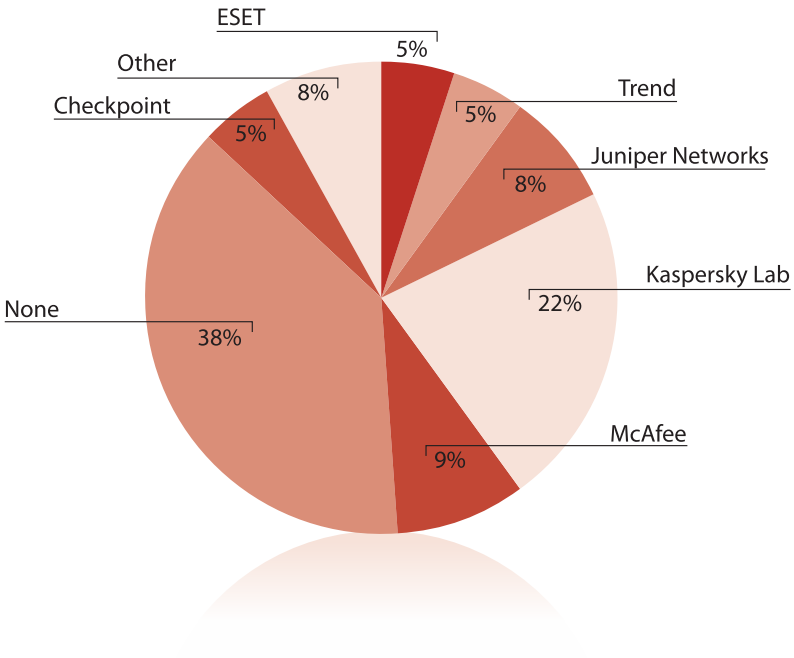
Does your organization allow employees to connect to public WiFi networks when traveling?



Does your organization require security software on smartphones?



What security software is installed on your employees smartphones?

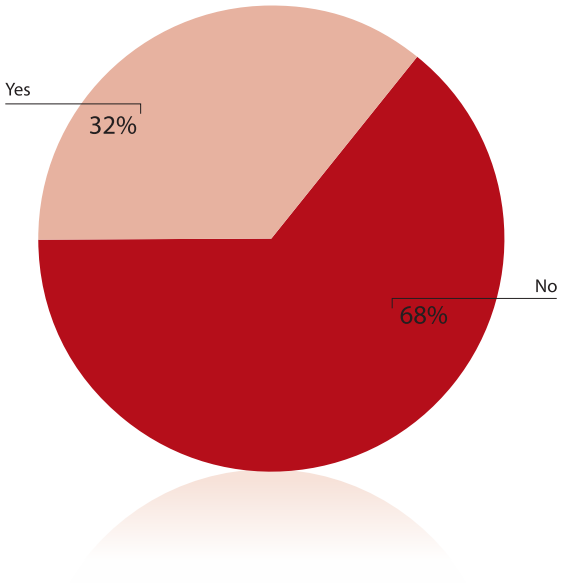


Editorial Review

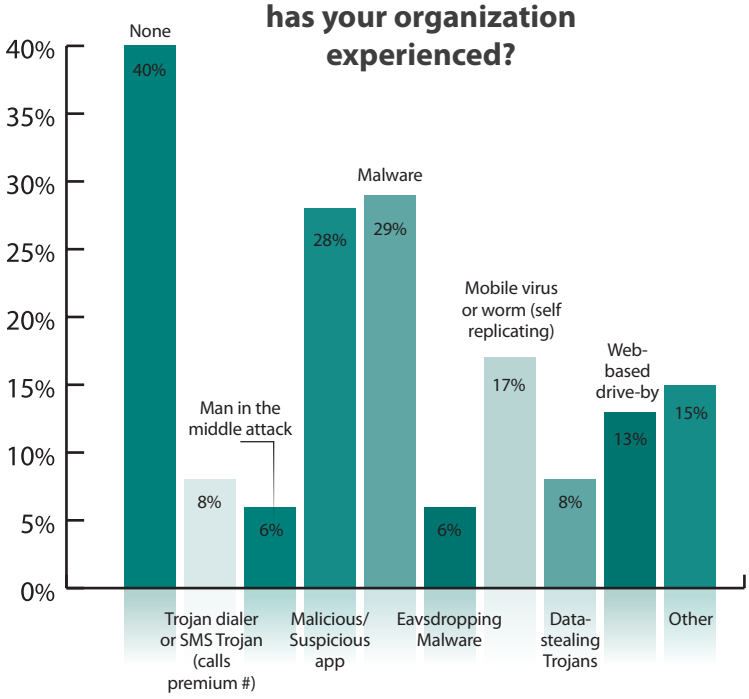
Despite those concerns, there's evidence of a protection gap emerging in the mobile space. Just 31% of those surveyed said their employer required them to install security software on their smart phone.

A startling small number of companies were taking steps to address those misperception. Just a third provided security awareness training to their users, while the vast majority - 85% - allowed employees to connect their mobile devices to public WiFi networks. Steps you mentioned to help secure devices ranges from a comprehensive lock down of devices and "lots of awareness training" to "hope and pray"

Does your organization provide any security awareness training for employees with smartphones?



Which of these attacks/threats has your organization experienced?



Respondents were clearly hungry for more information and more coverage of mobile threats.

Stay tuned to Threatpost for more coverage of Mobile Security as 2011 Progresses.