THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY:

A SURVEY OF IT PROFESSIONALS

June 2013

dimensional research

Sponsored by Check Point SOFTWARE TECHNOLOGIES LTD.

THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY:
A SURVEY OF IT PROFESSIONALS

Dimensional Research | June 2013

Introduction

Mobile devices cause ongoing concern for IT teams responsible for information security. Sensitive corporate information can be easily transported and lost, while the Bring Your Own Device (BYOD) movement has dramatically increased the number of expensive security incidents.

The following report, sponsored by Check Point, is based on a global survey of 790 IT professionals conducted in the United States, Canada, United Kingdom, Germany, and Japan. This is the second survey on this topic, and this report evaluates differences in responses to similar questions asked one year ago. The goal of the survey was to gather data to quantify the impact of mobile devices on corporate information security.

Executive Summary

1. BYOD is growing dramatically and affecting enterprises of all sizes
2. Corporate information on a mobile device is a more important asset than the device itself
3. Mobile security incidents are costly, even for SMBs

Key Findings

- **Increasing numbers of mobile devices connect to corporate networks**
  - 93% have mobile devices connecting to their corporate networks
  - 67% allow personal devices to connect to corporate networks
- **BYOD grows quickly and creates problems for organizations**

  Among companies that allow personal devices to connect to corporate networks:
  - 96% say number of personal devices connecting to corporate networks is growing
  - 45% have more than five times as many personal mobile devices as they had two years ago, an increase from 36% last year
  - 63% do not manage corporate information on personal devices
  - 93% face challenges adopting BYOD policies
  - Securing corporate information cited as greatest BYOD challenge (67%)
- **Customer information on mobile devices causes security concerns**
  - 53% report there is sensitive customer information on mobile devices, up from 47% last year
  - 94% indicate lost or stolen customer information is grave concern in a mobile security incident
- **Mobile security incidents very expensive**
  - 79% report mobile security incidents in the past year
  - 52% of large companies say cost of mobile security incidents last year exceeded $500,000
  - 45% of businesses with less than 1000 employees reported mobile security incident costs exceeding $100,000
  - 49% cite Android as platform with greatest perceived security risk (up from 30% last year), compared to Apple, Windows Mobile, and Blackberry
  - 66% say careless employees greater security risk than cybercriminals

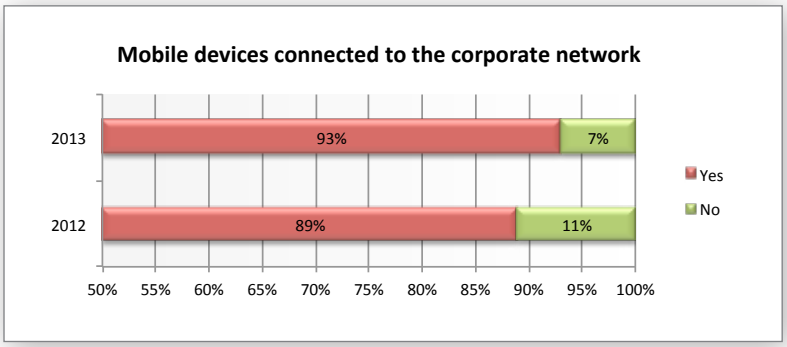
dimensional research

Sponsored by Check Point SOFTWARE TECHNOLOGIES LTD.

Detailed Findings

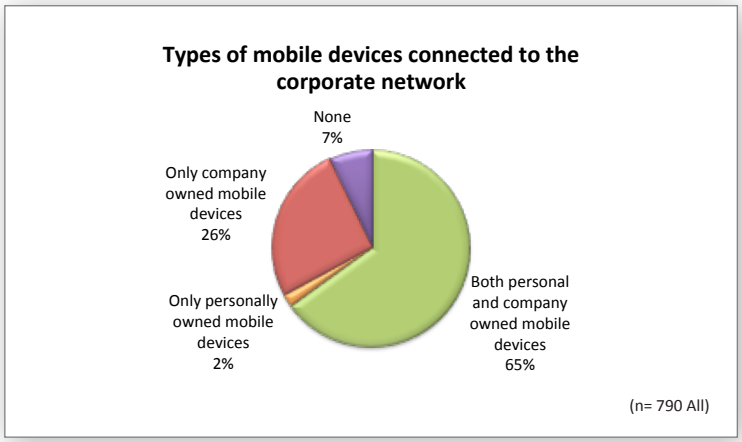
Extensive use of mobile devices on corporate networks

Participants were asked if mobile devices, such as smartphones or tablets, connected to their corporate networks. Broad use of mobile devices was reported, with 93% saying that they had mobile devices connecting to corporate networks. This is an increase compared to 89% in 2012.

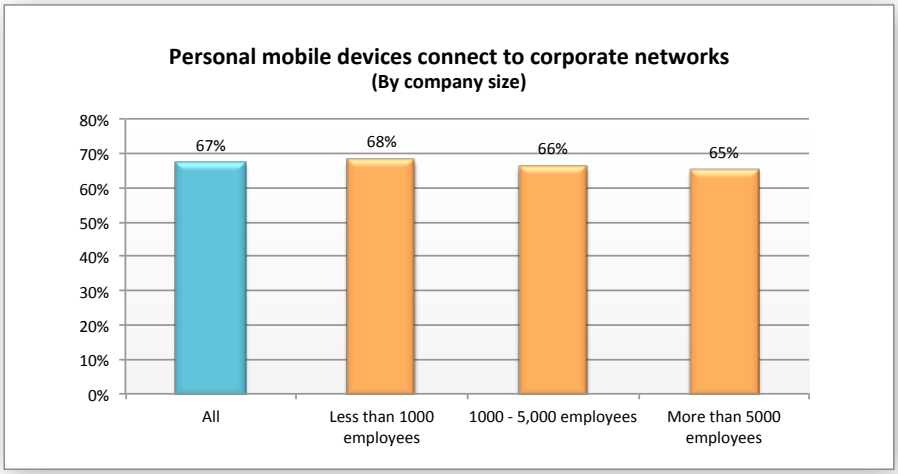


More corporate networks include personal devices

Just over two-thirds of organizations, 67%, have devices owned personally by employees, contractors, or others that connect to their corporate networks. This included 65% who allow both personal and company owned mobile devices, as well as 2% that had only personally owned mobile devices on their networks. This is an increase compared to 65% in 2012.

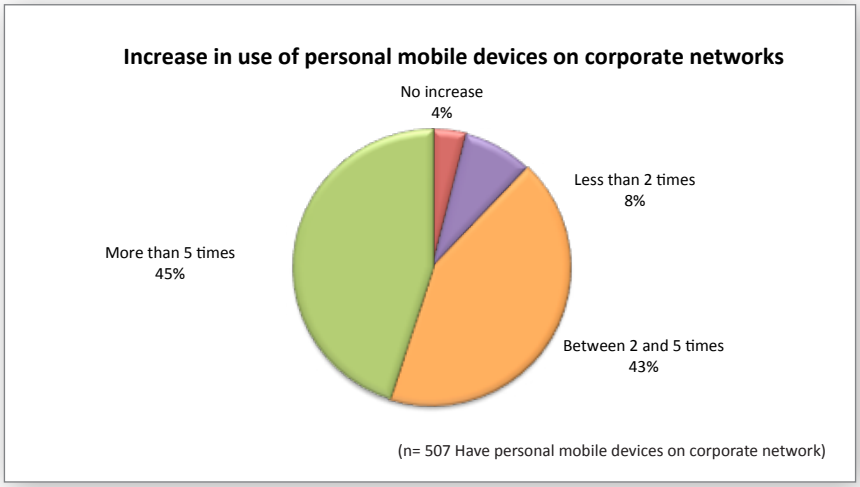


The use of personal mobile devices for work is very consistent across companies of all sizes. Little variation was seen in the number of businesses saying they have personal mobile devices on their corporate networks from the smallest businesses (68%) to the largest (65%).

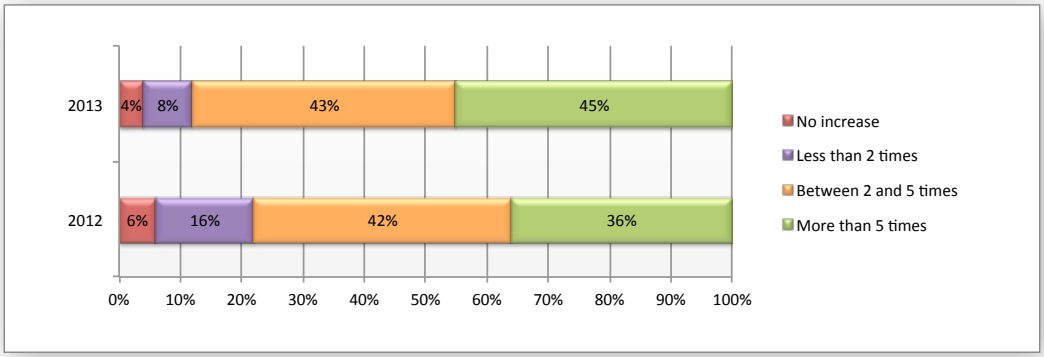


Personal mobile devices at work continue to expand

IT professionals whose companies do allow personally owned mobile devices to connect to corporate networks were asked how much growth there has been in the past two years. The vast majority, 96%, have seen an increase in the use of mobile devices connecting to corporate networks. For some companies, the increase was very dramatic with 45% saying they have more than five times as many personal mobile devices on their networks as they did two years ago.



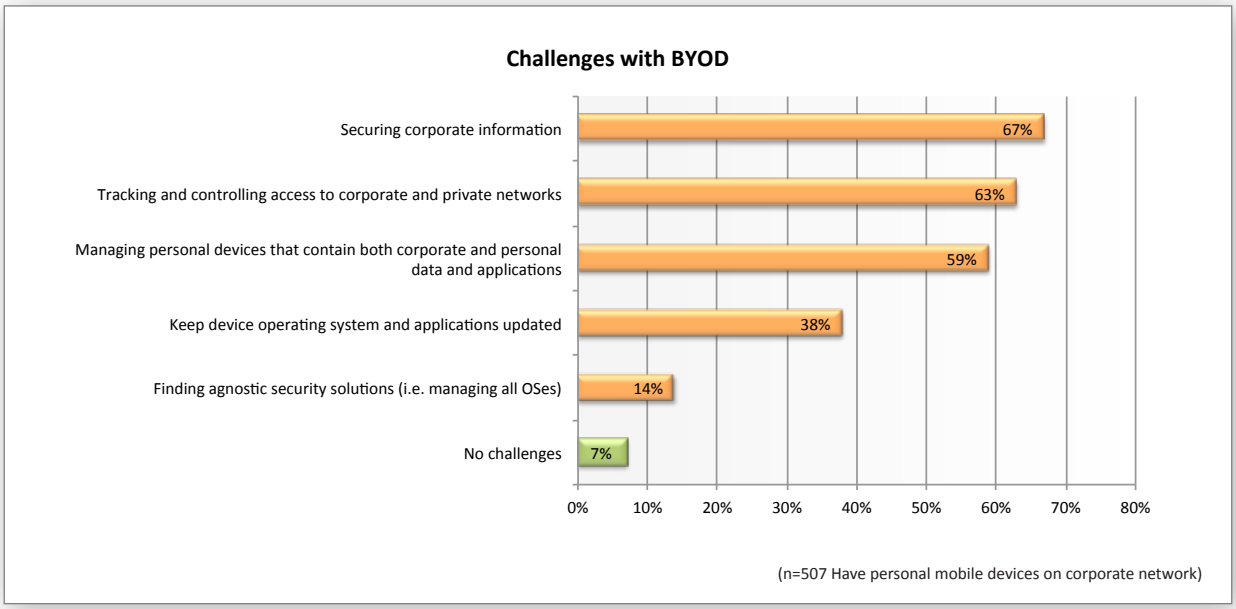
This growth is even more dramatic than last year. In 2012, the same question was asked. Only 36% of companies have more than five times as many personal devices connecting to corporate networks compared to 45% in this year's survey.



Securing corporate information greatest challenge in adopting BYOD

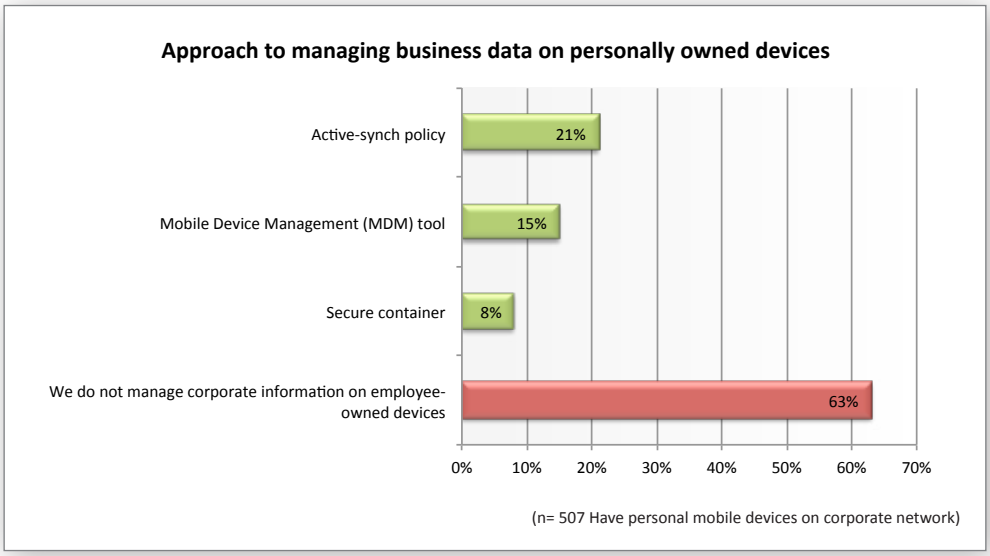
BYOD is causing challenges for corporate IT. Among companies that allow personal devices on their networks, the vast majority, 93%, reported that when employees use their own smartphones, tablets, or other devices to work with business information, it causes issues.

Participants reported that the most common challenge faced by IT organizations in adopting BYOD was securing corporate information (67%), closely followed by tracking and controlling access to networks (63%).

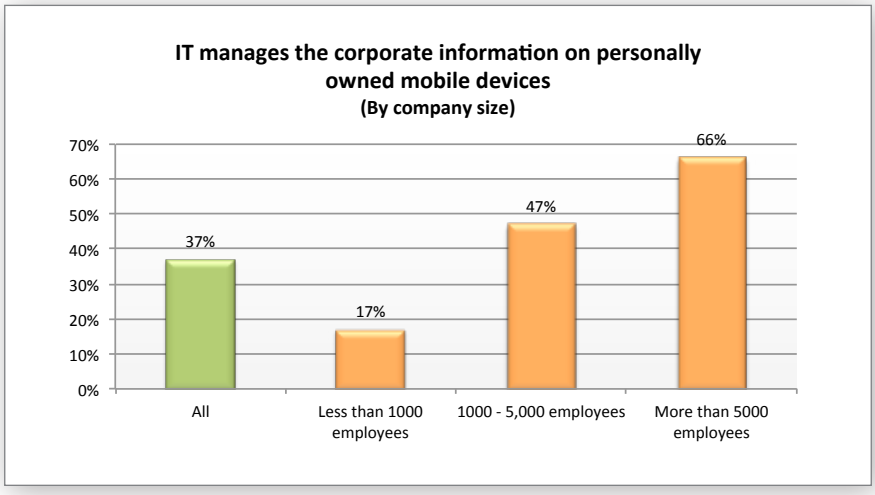


Corporate information on personal devices not managed by IT

Almost two-thirds, 63%, of companies who have personally owned mobile devices connecting to their corporate networks do not manage the corporate information that resides there. Among those who do manage the information, active-synch policies were the most common (21%), followed by Mobile Device Management (MDM) tools (15%), and secure container (8%).



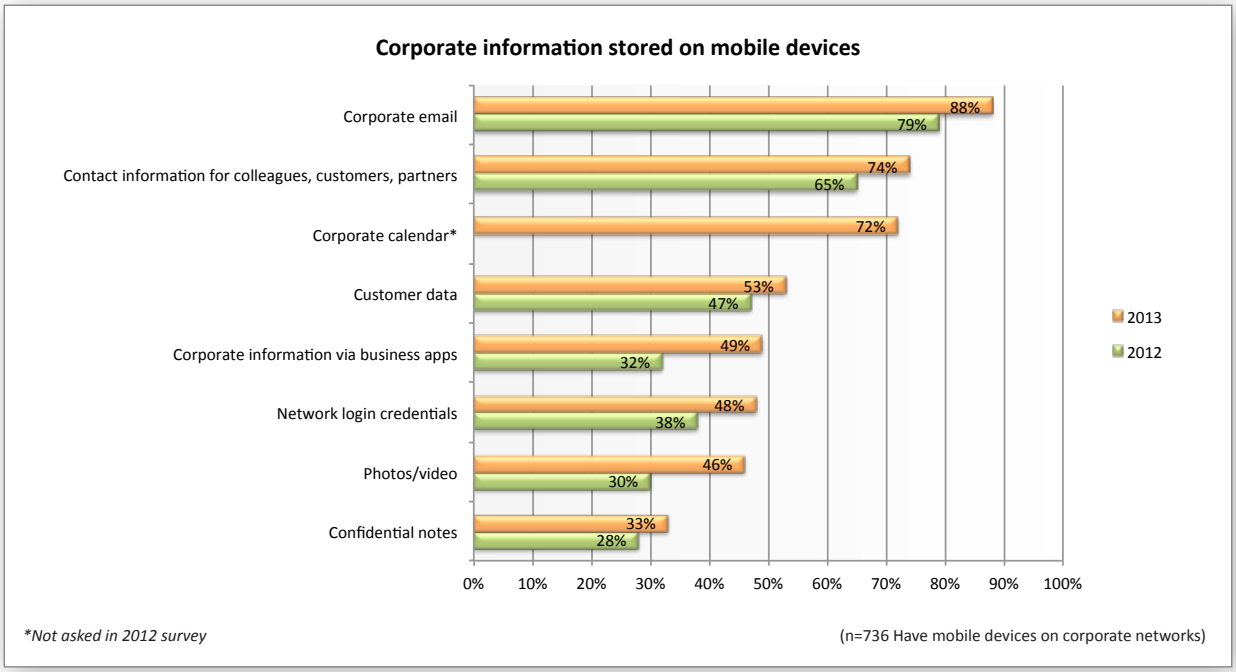
Larger companies were the most likely to manage corporate information on personally owned devices. Very few companies with less than 1000 employees, 17%, use a technical approach to information management on employee's mobile devices, significantly less than the comparable 66% of companies with more than 5000 employees.



More types of information on mobile devices today

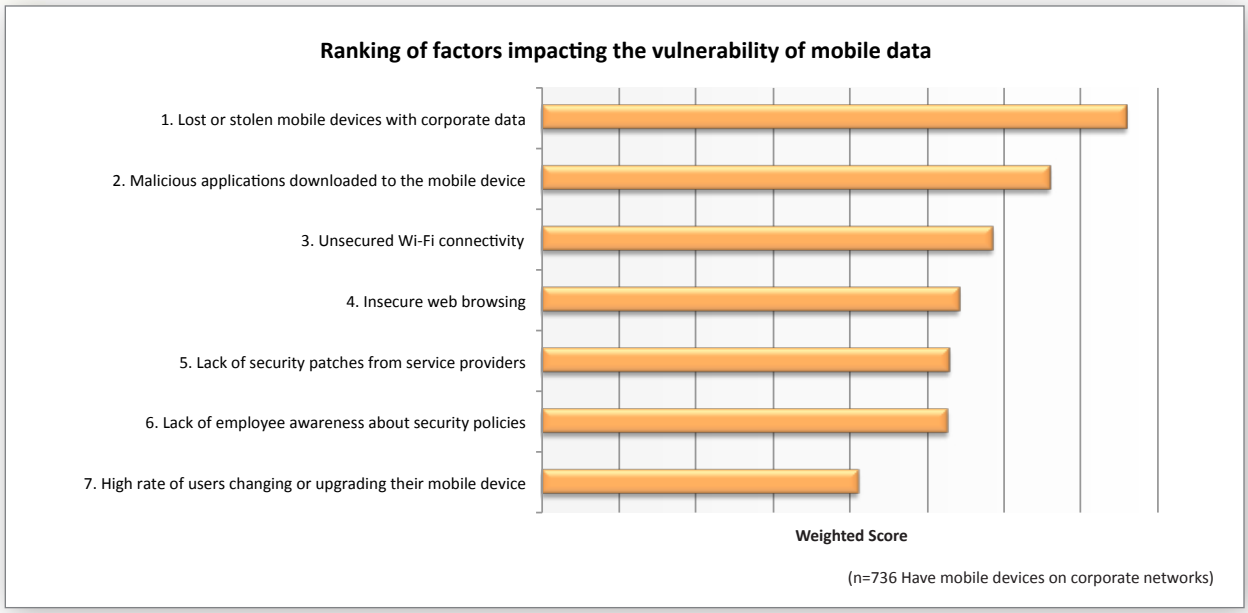
Participants reported an increase in all types of information stored on mobile devices compared to last year. Corporate email, the most common type of corporate information reported, increased from 79% of mobile devices last year to 88% this year.

More companies have their most sensitive business information stored on mobile devices. Customer data stored on mobile devices increased from 47% in 2012 to 53% in 2013. Corporate information on mobile devices through business apps installed on mobile devices saw the greatest increase with a 17% rise from 2012 to 2013.



Possible loss of corporate information from mobile devices ranked most concerning

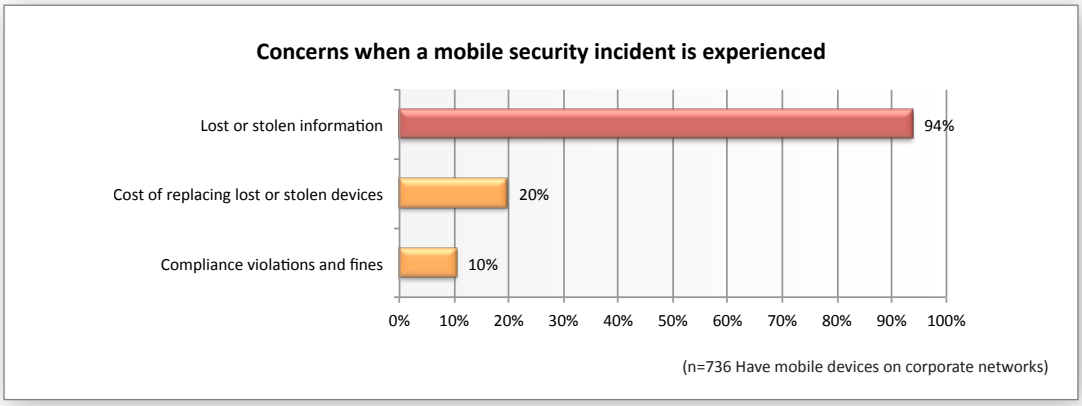
Mobile security incidents can have a wide range of impacts. Participants were presented with a list of possible impacts and asked to rank them from first to last with the first being the factor that was the most impactful and the last being the factor that was the least impactful. Lost or stolen devices was ranked number 1 as the factor that had the greatest impact on the vulnerability of mobile data, followed by malicious applications downloaded to the mobile device. The high rate of users changing or upgrading their mobile device was ranked last as a factor impacting mobile security.



Loss of corporate information greatest concern during a mobile security incident

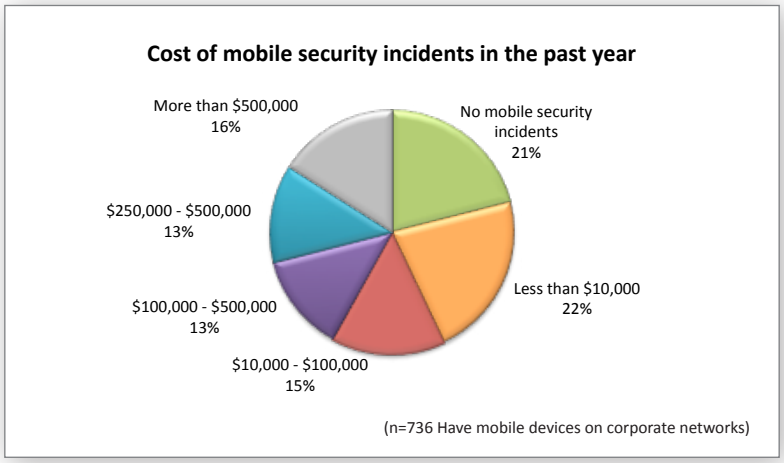
Mobile security incidents can have a wide range of impacts. Participants who had mobile devices on their corporate networks, including both personal and business, were presented with a list of possible issues that could occur as a result of a mobile security incident and asked which were most concerning.

Possible loss of corporate information was by far the most concerning (94%). The cost of replacing the lost device ranked a distant second (20%).

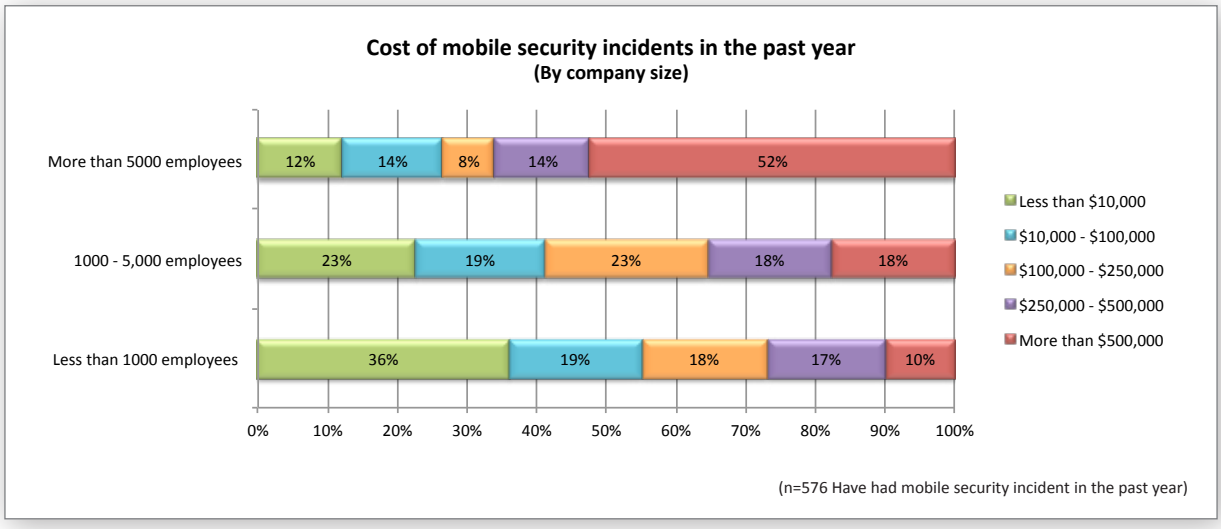


Mobile security incidents are expensive

Once companies have mobile devices, security incidents happen and the costs are substantial. Most companies, 79%, that have mobile devices on their networks have had a mobile security incident in the past year. The majority, 57%, reported that the total costs of their mobile security incidents cost them from $10,000 to more than $500,000 in the past year. These costs included staff time, legal fees, fines, resolution processes, and so on.



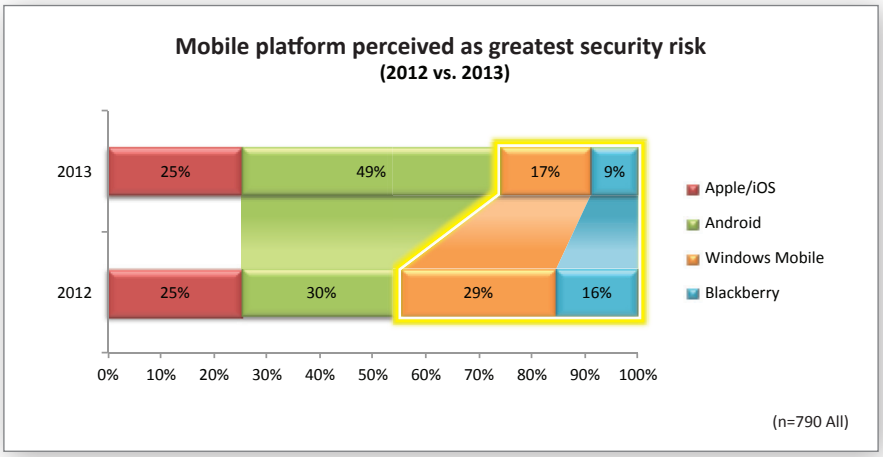
When security incidents did happen, the cost was most substantial at the largest companies. Among those who work at companies with over 5000 employees, more than half (52%) reported that last year the cost of mobile security incidents exceeded $500,000. However, even SMBs reported that mobile security incidents were very expensive. Almost half of companies with less than 1000 employees, 45%, reported security incidents that cost more than $100,000, a significant amount for a small firm.



Android trusted less; Windows Mobile and BlackBerry trusted more for security

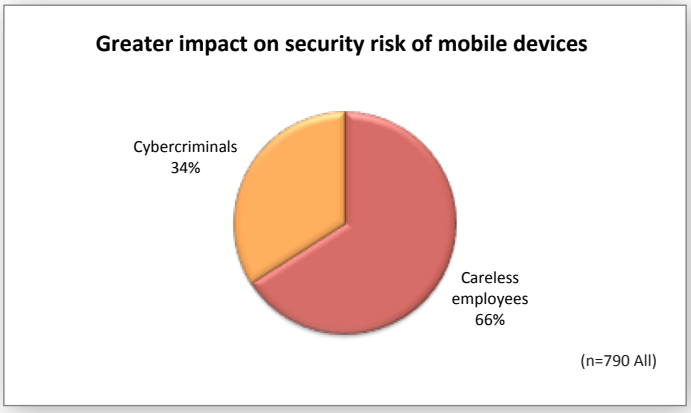
Participants were asked which of the most common mobile platforms they viewed as being the greatest risk to their corporate security. Android was by far the most frequent platform indicated (49%), followed by Apple/iOS (25%) and Windows Mobile (17%).

This question showed a dramatic change from the previous year. Android increased dramatically as the platform perceived to have the greatest security risk. Windows Mobile and BlackBerry both saw the number of IT professionals who viewed this as the most risky platform decrease by almost half.



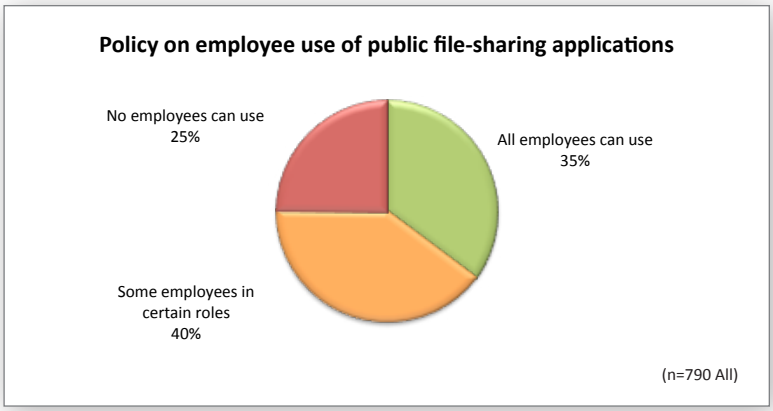
Careless employees seen as a greater security risk than cybercriminals

Participants were asked which group of individuals was considered the greatest security risk — careless employees or cybercriminals who intentionally try to steal corporate information. Significantly more said careless employees pose greater security risks (66%) than cybercriminals (34%), which reinforces the importance of implementing a strong combination of technology and security awareness throughout an organization.

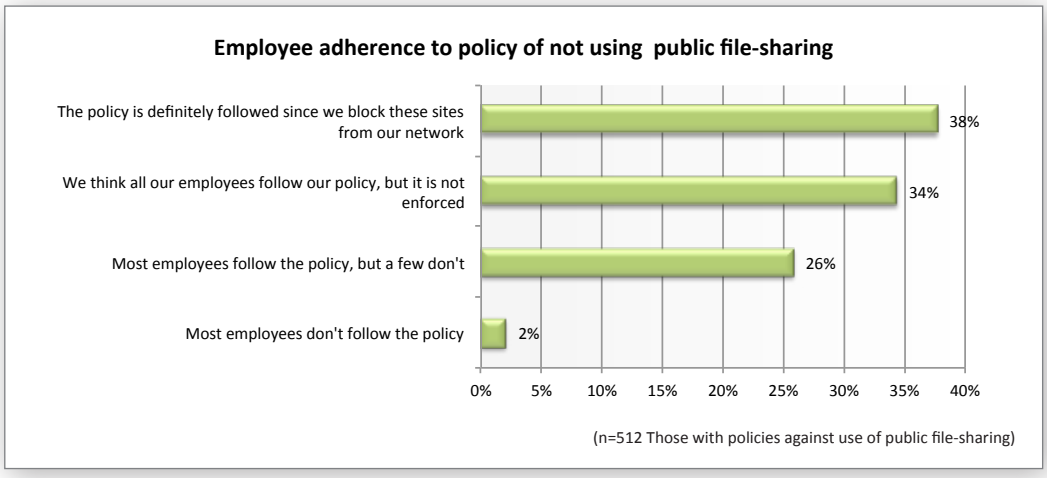


IT may not allow use of file-sharing sites, but policy is often not enforced

The use of mobile devices has driven the adoption of file-sharing sites such as DropBox, Box, Google Drive and iCloud, which some IT organizations see as a concern for security of corporate data. Participants were asked if employees are allowed to upload and share work information to public file-sharing applications. Organizations are divided on their policies with some allowing all employees to access these sites (35%) and some not allowing any employees (25%). Most allowed some employees while preventing others (40%).



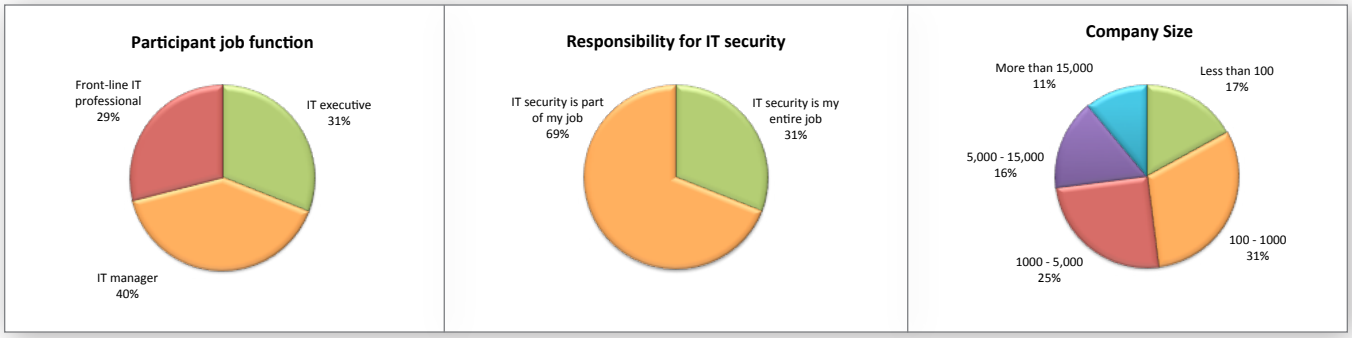
However, these policies are not enforced uniformly. Organizations who do have policies that some or all of their employees not use public file-sharing applications were asked whether they thought these policies were followed. Only 38% actually enforce their policies by blocking these sites on the corporate network, while 28% admit that some employees don't follow the policy.



Survey Methodology

An independent database of IT professionals was invited to participate in a web survey on the topic of mobile devices and information security sponsored by Check Point. A total of 790 respondents across the United States, Canada, United Kingdom, Germany, and Japan completed the survey. Each respondent had responsibility for securing company systems. Participants included IT executives, IT managers, and hands-on IT professionals, and represented a wide range of company sizes and industry verticals.

This survey is the second in a series of surveys on this topic. This report compares certain results to the results of similar questions asked one year ago.



About Dimensional Research

Dimensional Research® provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information visit www.dimensionalresearch.com.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.