Introduction

Mobile devices cause ongoing concern for IT teams responsible for information security. Sensitive corporate information is easily transported outside of managed environments, while the Bring Your Own Device (BYOD) movement has dramatically increased the number of expensive security incidents. In recent months, we have seen several highly visible, high-impact corporate hacks. These highly publicized breaches have significant financial impact as well as risk to the company’s reputation. Mobile security is of utmost concern as the number of personal devices connecting to corporate networks continues to grow.

The following report, sponsored by Check Point, is based on a global survey of 706 IT and security professionals conducted in the United States, Canada, Germany, United Kingdom, Australia and New Zealand. The goal of the survey was to capture data on current attitudes and trends with mobile devices and IT security. This is the third survey on this topic sponsored by Check Point and this report evaluates differences in responses to similar questions asked over the past two years.

Executive Summary

1. Number of personal mobile devices connecting to corporate networks continues to grow
2. The cost of remediating mobile security incidents continues to increase
3. Employee behavior is a significant factor in mobile security

Key Findings

• **Number of personal devices connecting to corporate networks continues to grow**
  - 75% allow personal devices to connect to corporate networks, an increase from 67% in 2013 and 65% in 2012
  - 91% say the number of personal devices connecting to corporate networks is growing
  - 72% more than doubled the number of connected personal mobile devices in the past two years

• **Mobile security incidents are on the rise, and so is the cost of fixing them**
  - 82% of security professionals expect mobile security incidents to increase this year
  - 98% have concerns about the impact of a mobile security incident
  - 95% face challenges with the security of BYOD
  - 64% say cost of remediating mobile security incidents is increasing
  - 42% of executives say a mobile security incident costs more than $250,000
  - 64% cite Android as the mobile platform with the greatest risk, up from 49% in 2013 and 30% in 2012

• **Employee behavior is a significant factor in information security**
  - 87% say careless employees are a greater threat to security than cybercriminals, up from 72% in 2012
  - Employee actions have the highest impact on vulnerability of mobile data
  - 63% say employees likely contributed to recent high-profile security breaches
  - 92% say employee behaviors could have made a difference in preventing high-profile security breaches
  - 56% are managing business data on employee-owned personal devices, up from 37% in 2013
Detailed Findings

Continued growth in the number of companies with mobile devices connecting to corporate networks

IT professionals were asked if mobile devices, such as smartphones or tablets, were allowed to connect to their corporate networks. Most reported broad use of mobile devices within their organizations, with 95% saying that they had mobile devices connecting to corporate networks, including 74% who allowed both personal and company owned devices, 20% who allowed only company-owned mobile devices, and 1% that had only personal mobile devices. The 1% all worked at small companies.

This is a slight increase in the number of companies that allow mobile devices on their corporate networks compared to 93% in 2013.

More corporate networks include personal devices

If we consider only personally-owned mobile devices connecting to corporate networks, 2014 has seen a more significant growth rate than in the past. In 2014, 75% of IT professionals reported that devices owned personally by employees, contractors, or others connect to their corporate networks, up from 67% in 2013 and 65% in 2012.
Companies have an increasing number of personal mobile devices connecting to their networks

IT professionals whose companies do allow personally-owned mobile devices were asked how much growth there has been in the number of personal devices on their corporate networks. The vast majority, 91%, have seen an increase in the number of mobile devices connecting to corporate networks over the past two years. For most participants, the increase was very dramatic with 72% saying they more than doubled the number of personal mobile devices in this timeframe.

Mobile security incidents expected to grow

With the high rate of growth of mobile devices, particularly personal mobile devices connecting to corporate networks, it is unsurprising that the number of security incidents is also expected to grow. Among all IT professionals, about two-thirds (64%) expected to see an increase in the number of mobile security incidents. Interestingly, IT professionals in general were more optimistic than the IT professionals who focus exclusively on security as their entire job. Among the security professionals who spend all their time thinking about securing corporate data and systems, a shocking 82% expect the number of security incidents to increase. Not a single dedicated security professional (0%) indicated that they expected the number of mobile security incidents to decrease this year, although among all IT professionals, including those for whom security was only part of their job, 7% felt that the steps they were taking to ensure security would decrease the number of security incidents.
IT professionals are concerned about the business impact of mobile security incidents

Nearly all IT professionals (98%) have concerns about the impact of a mobile security incident. When asked about their greatest concerns, lost or stolen information topped the list with 82% of IT professionals citing this as an issue, followed by 61% who worried about introducing security weaknesses for future attacks.

Participants who took the time to write in “Other” answers specifically called out worries about reputation and bad press, loss of productivity while correcting problems, and costs to stay within security standards and compliance.

Securing corporate information remains greatest challenge in adopting BYOD

BYOD or “Bring Your Own Device” continues to cause challenges for corporate IT. The majority of participants, 95%, reported that when employees use their own smartphones, tablets, or other devices to work with business information, it creates security challenges.

IT professionals report that the most common challenge faced by IT organizations in adopting a BYOD policy is securing corporate information (72%), followed by managing personal devices that contain corporate and personal data and applications (67%), and tracking and controlling access to corporate and private networks (59%).
The specific challenges and importance of the challenges did not change significantly from year to year, but the overall number of IT professionals facing security concerns as well as the number concerned about particular items, has increased across the board. The overall number of IT professionals who face security challenges rose from 93% in 2013 to 95% in 2014. Most challenges saw a slight increase in number of IT professionals experiencing them, for example concerns about securing corporate information rose from 67% in 2013 to 72% in 2014.

Interestingly, there was a dramatic increase in the ability to finding agnostic security solutions that can manage all operating systems across the wide range of mobile devices used. In 2013 only 14% listed finding agnostic security solutions as a top concern, but in 2014 that number rose dramatically to 42%.

Cost of remediating security incidents is increasing

The costs of remediating a security incident can be wide-ranging once you include staff time, legal fees, fines, resolution processes, and other expenses for each incident where corporate information has been lost or stolen from a mobile device. Most IT professionals (64%) report that the costs of remediating mobile security incidents is increasing, with only a small number (6%) reporting these costs are decreasing.
Because of this wide range of possible expenses, the actual cost of a mobile security incident can be challenging to calculate. IT executives had the most visibility into these costs, which can be substantial. Three-quarters (75%) of IT executives reported that a mobile security incident costs their company more than $10,000, including 42% who said it cost more than $250,000. This is an increase from 2013 where only 37% reported a mobile security incident cost more than $250,000.

Perception of Android security risks grew again in 2014

IT professionals were asked which of the most common mobile platforms they viewed as being the greatest risk to their corporate security. The number of IT professionals saying Android was the riskiest increased and was by far the most frequent platform indicated (64%), followed by Apple/iOS (16%) and Windows Mobile (16%) and Blackberry (4%). Perception of Android security problems continued to grow dramatically as the platform perceived to have the greatest security risk (up from 49% in 2013 and 30% in 2012).

Apple/iOS decreased in perception as the riskiest mobile platform for the first time since this survey began, to 16% from 25% in both of the prior years. Windows Mobile saw about the same results after dropping considerably from 2012 to 2013. Blackberry dropped for the 2nd year in a row as the number of IT professionals who viewed this as the most risky platform decrease by more than a half.
Concern about careless employees is growing

Employee behavior was found to have significant impacts on mobile security in this year’s survey. IT professionals were asked which group of individuals was considered the greatest security risk — careless employees or cybercriminals who intentionally try to steal corporate information. Careless employees continued to be reported as a greater security threat than cybercriminals with 87% of participants citing careless employees as the greatest security risk as opposed to only 13% citing cybercriminals. This is a notable increase from 2012 when the same question was asked and 72% cited careless employees. This reinforces the importance of implementing a strong combination of technology and security awareness throughout an organization.

Employee actions have highest impact on vulnerability of mobile data

Mobile security incidents can have a wide range of impacts. IT professionals 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. Last year, lost or stolen devices was ranked first among IT professionals as the factor that had the greatest impact on the vulnerability of mobile data, followed by malicious applications downloaded to the mobile device.

In 2014, the role of employees rose significantly and is now represented in all the biggest impacts on the vulnerability of mobile data. This includes employees accidentally accessing malicious sites or downloading malicious content, lack of employee awareness about security policies, and employees intentionally ignoring security policies all surpassing lost or stolen mobile devices with corporate data.
Employee behavior can make a difference in preventing security reputation events

Employee adherence to corporate security policies whether it be lack of awareness of security policies or employees intentionally ignoring security policies were ranked among the highest impacts on the vulnerability of mobile data. Recent months have seen a large number of very high profile customer data breaches. IT professionals were also asked if they felt employee behavior could have made a difference in preventing these embarrassing and customer-impacting issues.

Two-thirds of participants (63%) indicated that it is likely employee carelessness contributed to recent high-profile breaches of customer data. The vast majority (92%) said that in their opinion employee behaviors could have made a difference.

More companies are managing employee-owned devices

Once corporate data is on personal devices, it becomes a security risk point if those are not managed properly. In 2014 there was a significant increase in the number of IT organizations managing business data on the personal devices that employees use for work. More than half of organizations (56%) are managing the business data that exists on personal devices, up significantly from just over one-third (37%) in 2014.
Survey Methodology
An independent database of IT and security 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 706 respondents across the United States, Canada, United Kingdom, Germany, Australia and New Zealand 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 third in a series of surveys on this topic sponsored by Check Point. This report compares certain results to the results of similar questions asked in the past two years.

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.