

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



Dimensional Research | January 2012

Introduction

Mobile devices, such as smartphones and tablets, proliferate in today's corporate environments. While there are significant opportunities to leverage these devices to increase the effectiveness of mobile workers, there are also significant concerns about the privacy of sensitive corporate data stored on the devices that IT must handle.

The following report, sponsored by Check Point, is based on a global survey of 768 IT professionals conducted in the United States, Canada, United Kingdom, Germany, and Japan. The goal of the survey was to gather data about current mobile computing trends, including the type of data stored or accessed on mobile devices and the potential for heightened data security risks.

Key Findings

- **Extensive use of mobile devices connecting to corporate networks**
 - 89% have mobile devices such as smartphones or tablets connecting to corporate networks
 - Apple iOS is the most common mobile platform used to connect in corporate environments
- **Personal mobile devices that connect to corporate networks are extensive and growing**
 - 65% allow personal devices to connect to corporate networks
 - 78% say there are more than twice as many personal devices connecting to corporate networks now than compared to two years ago
- **Security risks are on the rise because of mobile devices**
 - 71% say mobile devices have contributed to increased security incidents
 - The Android mobile platform is considered to introduce the greatest security risks
- **Employee behavior impacts security of mobile data**
 - 47% report customer data is stored on mobile devices
 - Lack of employee awareness about security policies ranked as having the greatest impact on the security of mobile data
 - 72% say careless employees are a greater security threat than hackers

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. The IT professionals who took the survey reported broad use of mobile devices within their organizations with 89% saying that they had mobile devices connecting to corporate networks.

Most participants, 65%, reported that their organizations had devices that were personally owned by employees in addition to company-owned mobile devices accessing corporate networks.



Sponsored by

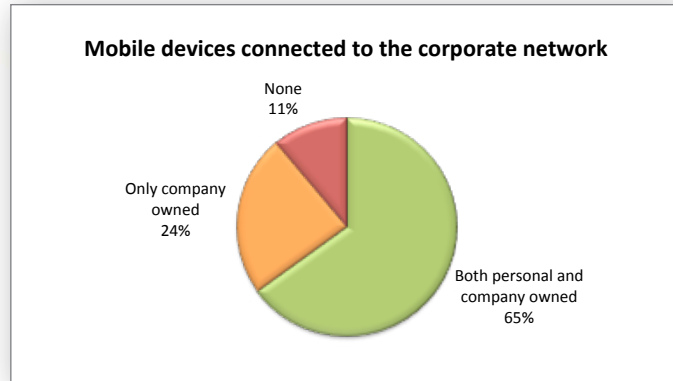


Check Point
SOFTWARE TECHNOLOGIES LTD.

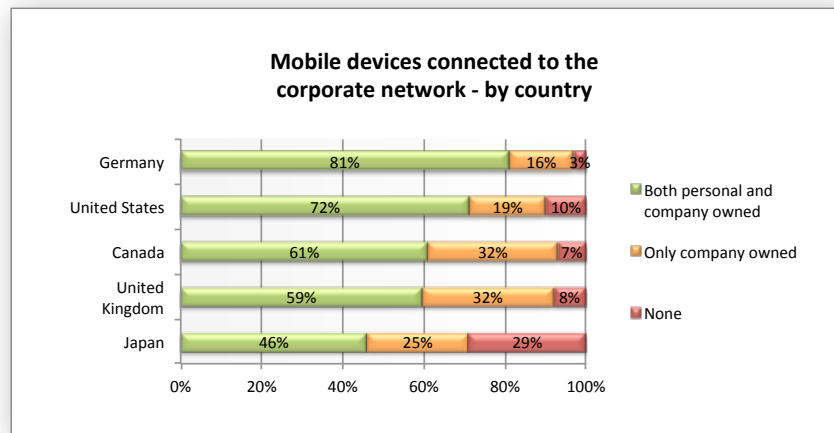
THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS



Dimensional Research | January 2012



Among the countries surveyed, Japan is the least likely (46%) to allow personal mobile devices and Germany the most likely (81%).



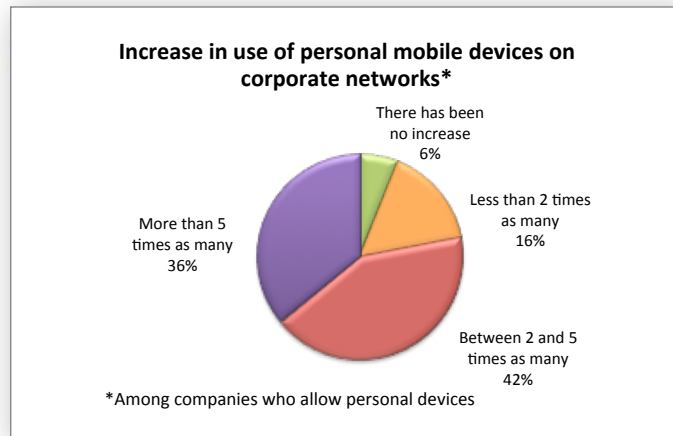
Dramatic growth in use of personal mobile devices at work

Participants who say their organizations do allow personal devices to connect to corporate networks cite significant growth in the number of personal devices in the past two years. Of these, the vast majority, 94%, says that they have seen an increase in the use of personal mobile devices connecting to corporate networks. The growth has been significant with 78% saying more than twice as many personal devices are used at work compared to two years ago, including 36% who say there are more than five times as many personal devices connecting to corporate networks in the past two years.

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

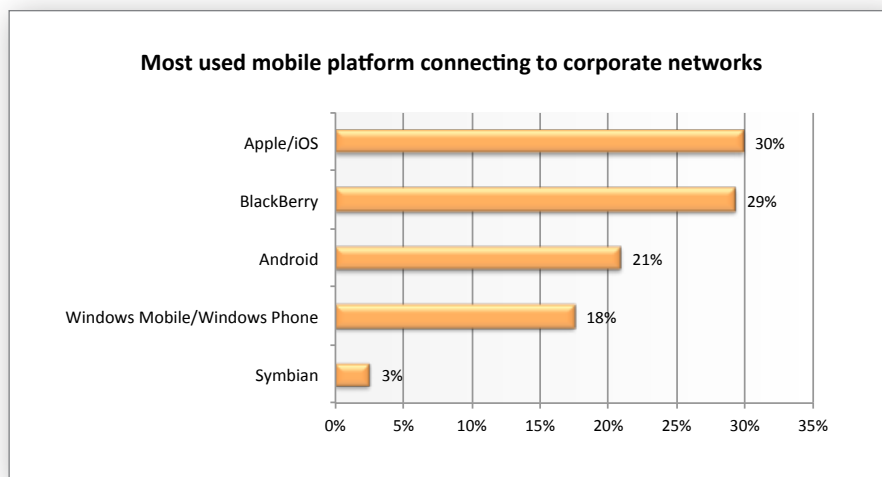


Dimensional Research | January 2012



Apple iOS most used mobile platform

Participants reported that Apple iOS (30%) and BlackBerry (29%) were the most commonly used mobile device types connecting to their corporate networks followed by Android (21%).



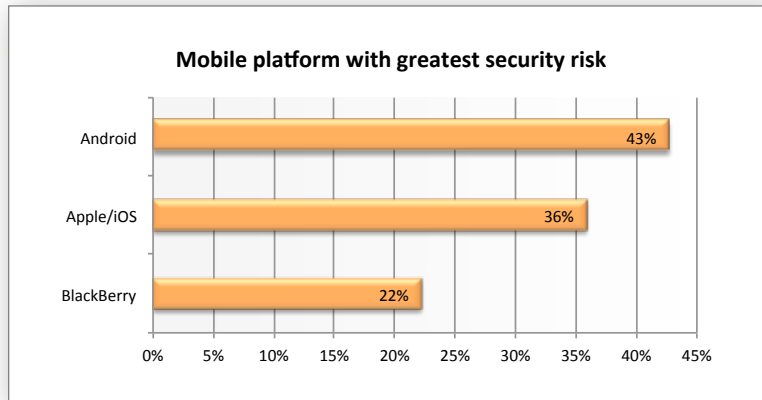
Android viewed as the most risky platform

Participants were asked which of the most common mobile platforms they viewed as being the greatest security risk. Among the IT professionals in this study, Android was named as the greatest risk (43%). And, BlackBerry was the operating system that was perceived as having a lower potential for problems than other mobile platforms with only 22% ranking it as the platform with the greatest security risk.

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

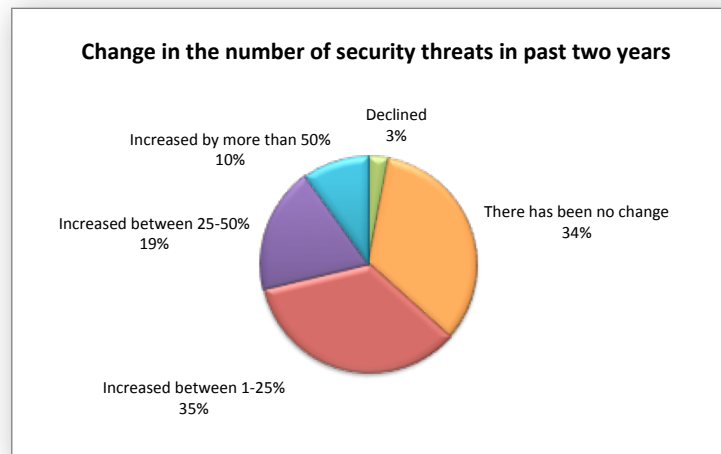


Dimensional Research | January 2012



Mobile devices driving increase in security risk

Participants were asked if they had experienced an increase in the number of security threats to their organizations in the past two years. Most participants, 64%, reported an increase. Only 3% saying security threats have declined. The remainder of participants, 34%, has not seen a change in the number of security threats in the past two years.

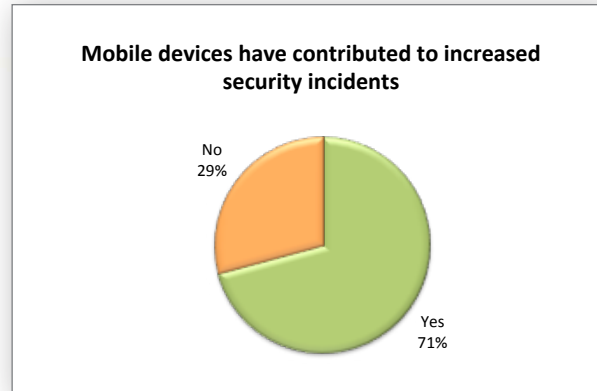


Most of those who have seen an increase, 71%, say that mobile devices are a contributing factor to the increase in the number of security incidents faced by their organizations.

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

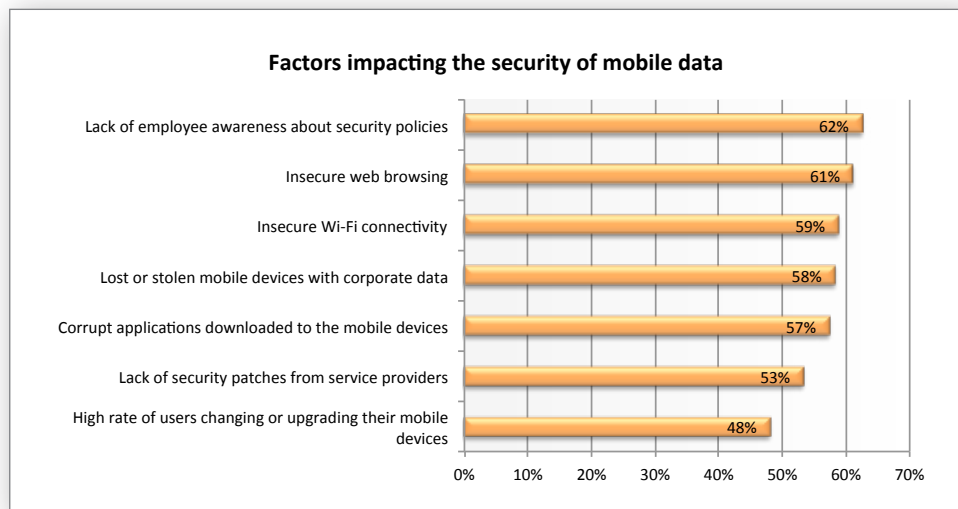


Dimensional Research | January 2012



Lack of employee awareness has greatest impact on security of mobile data

The IT professionals in this study were asked to rank the impact of a range of factors on the security of mobile data. Lack of employee awareness ranked most highly with 62% of the highest score possible followed closely by insecure web browsing (61%) and insecure Wi-Fi connectivity (59%).



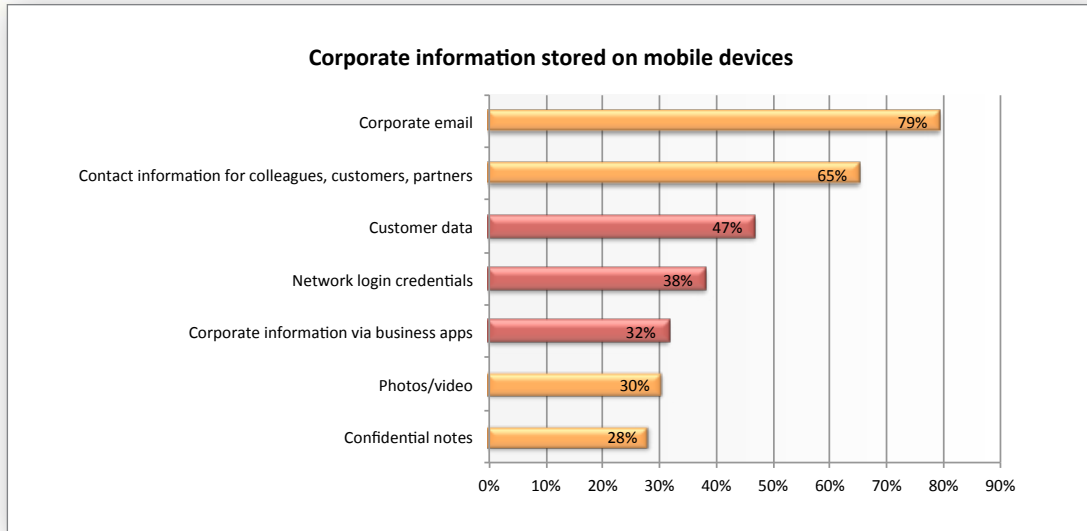
Many mobile devices store sensitive customer and business data

Participants were asked what types of corporate information were stored on mobile devices used by employees. The most frequently reported type of information was corporate email (79%) and business contacts (65%). However, users also reported a significant level of very sensitive information was on their mobile devices, including customer data (47%), network login credentials (38%), and corporate information made available through business applications (32%).

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

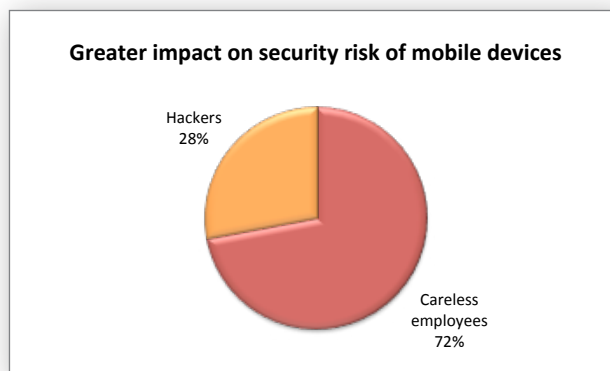


Dimensional Research | January 2012



Careless employees seen as a greater security risk than hackers

Participants were asked which group of individuals was considered the greatest security risk — careless employees or hackers who intentionally try to steal corporate information. Significantly more participants said careless employees pose greater security risks (72%) than hackers (28%), which reinforces the importance of implementing a strong combination of technology and security awareness throughout an organization.



There was significant variance in the perception of the threat of careless employees compared to hackers between different countries. Participants from the UK cited more risk from careless employees (79%) while those from Germany were less concerned about careless employees compared to the rest of the participants (55%).

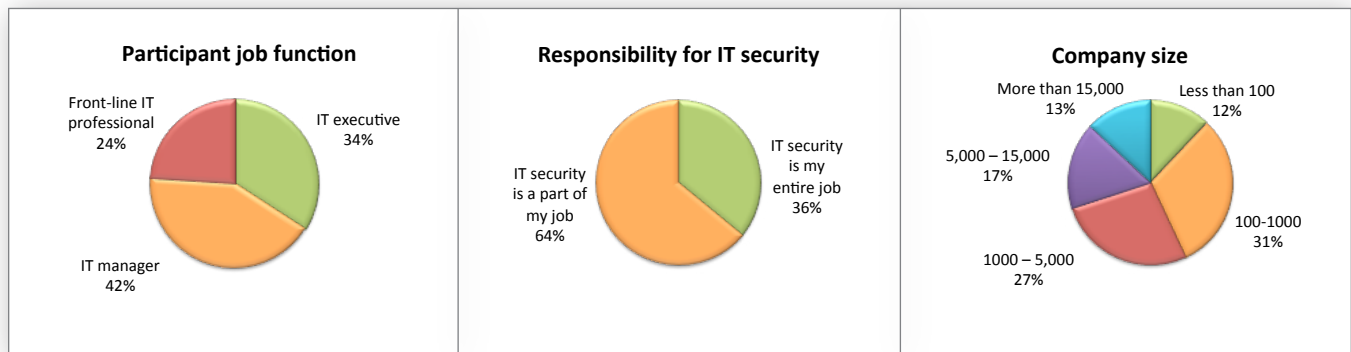
THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS



Dimensional Research | January 2012

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 768 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.



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.dimensionalsearch.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.