McAfee 2011 Report - Mobility and Security.pdf

Mobility and Security

Dazzling Opportunities, Profound Challenges

Mobility and Security

Dazzling Opportunities, Profound Challenges

Contents

Introduction

by Todd Gebhart, Executive Vice President and General Manager Consumer, Small Business and Mobile, McAfee

Decades ago, before the sun rose on the Information Age, computational power was symbolized by the mainframe and the future of communications was something only hinted at in comic strips and science fiction novels. Remember the intrepid comic strip detective Dick Tracy talking into his two-way wristwatch radio? Well, the future arrived some time ago, and we are moving beyond it now and into unchartered waters teeming with opportunity and challenge.

Mobility is changing our lives on all levels–personal, professional, and political. Consider one iconic executive's perspective. At the D8 conference, Apple CEO Steve Jobs said, "The day is coming when only one out of every few people will need a traditional computer. When we were an agrarian nation, all cars were trucks because that's what you needed on the farms." Jobs compared PCs to trucks, stating that while they are still going to be around, "but only one out of x people will need them."[1]

Mobile devices are being used by much of the workforce, over extended periods of time, for a significant percent of tasks previously conducted on desktops.

For this report, McAfee teamed up with Carnegie Mellon University to examine the current state of mobile security, some common problems and some recommendations that all businesses and consumers should consider.

The results of the *McAfee Mobility and Security Survey* indicate several key trends:

- Reliance on mobile devices is already significant and accelerating rapidly; the emerging mobile environment is both diverse and freewheeling
- IT is becoming increasingly consumerized as evidenced by the fact that 63 percent of devices on the network are also used for personal activities
- There is a serious disconnect between policy and reality in the mobile computing environment; both IT directors and users are unhappy
- Lost and stolen mobile devices are seen as the greatest security concern in the mobile computing environment among consumers and IT professionals
- Although the need for mitigating mobile security risks and threats is acknowledged, risky behaviors and weak security postures are commonplace

From bankers to baristas to booksellers, businesses are offering mobile services and consumers are embracing mobile devices.

Mobility is having an extraordinary impact on the nature of computing in the twenty-first century. It offers many dazzling opportunities that also bring with them some profound challenges related to security and privacy. What are these challenges and how they are starting to manifest in enterprises throughout the world?

Will the enterprise come to grips with these challenges and reap the benefits of the many opportunities that come with the age of mobile computing? Where will it end? Wherever it ends, the changes that are already underway are profound.

Mobility in Twenty-First Century Computing and the Consumerization of IT

The dawn of the Information Age began with desktop PCs. In those early years, "Windows" and "Apple," which had once been mere nouns, became globally defined brand names that helped shape a new approach to both work and play. Rapidly, that worldview changed and expanded to include local area networks (LANs), then the World Wide Web, and then laptops, and then in rapid succession to WiFi hotspot, smartphone, a Cloud and a tablet.

"Recent advances in computing technology have resulted in greatly increased speed and storage capacity for mobile computing devices," says CyLab researcher Collin Jackson. "These advances have greatly enhanced our effectiveness and efficiency for both business and personal tasks. However, mobile devices are much more likely to be lost, stolen, or exploited while unattended than those that permanently remain in office spaces."

Indeed, 21 items on the Associated Press list of "50 Things that Changed Our Lives in the Aughts," were technological in nature and most related to mobility: "apps, blogs, BlackBerrys, digital cameras, cell phones, connectivity, online dating, DVRs, Facebook, Google, GPS, information overload, iPods, Netflix, sexting, texting, flat TV screens, Twitter, Wii, Wikipedia, and YouTube."[2]

Consider some recent business news stories. Pew Research Center's Internet and American Life Project found that Americans' use of non-voice programs on cell phones has "grown dramatically" over the last year, with even more of us using our phones as cameras and video recorders, as well as for email, Internet and playing games.[3]

In addition to usage changes, the computing power of these devices has changed dramatically. Researchers at Massachusetts Institute of Technology and Texas Advanced Computing Center recently created an Android app that can take simulations from the powerful Ranger supercomputer and solve them further on the mobile phone.[4]

According to Apple's chief operating officer, 65 percent of Fortune 100 firms are already deploying the iPad or piloting projects, and many analyst firms are predicting an explosion of tablet devices in the enterprise in 2011

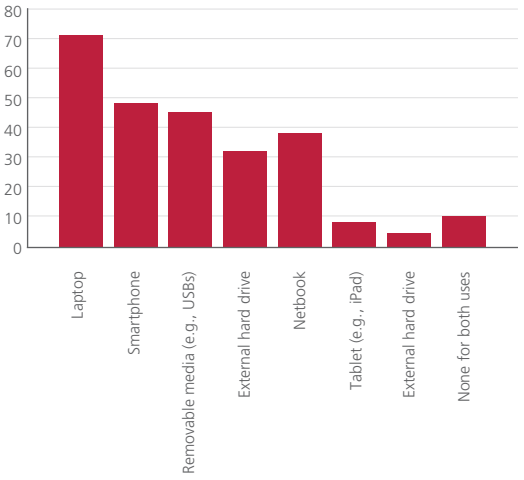
This shift to mobile computing hasn't just changed user's personal lives. It. However, it is changing their work lives too. More users are finding that their employers are not keeping pace with changing mobile technologies. Apple iPhones, Droids, Apple iPads, and other mobile platforms are invading corporations worldwide. It didn't happen overnight, but these devices have slowly crept into the work place and are now poised to take over. According to Apple's chief operating officer, 65 percent of Fortune 100 firms are already deploying the iPad or piloting projects, and many analyst firms are predicting an explosion of tablet devices in the enterprise in 2011.

CyLab researcher Nicolas Christin has conducted research into one-click fraud, a criminal enterprise that successfully exploits vulnerabilities in elements of both online banking and mobile phone computing. Christin believes that the convenience offered by mobile devices, and the ability for sales personnel to have access to company data from any location, has changed the way company information is handled.

"This shift has security implications," said Christin. "In particular, the relatively large number of people using laptops both for professional and personal purposes may lead to security issues. Removable media can easily be targeted by attackers to circumvent network protections such as firewalls, as has been demonstrated by threats such as Stuxnet and other sophisticated malware threats."

The consumerization of IT is all about productivity, but increased productivity is not without cost. In many cases, employers see the benefits of these consumer devices in the workplace but are still highly concerned about protecting confidential corporate data. More than half of the survey respondents in a previous McAfee survey agreed that consumerization of IT increases security concerns, and nearly half (45 percent) felt that managing consumer-owned devices and related technologies within the enterprise network is "critical."

Mobile devices for both work and personal use

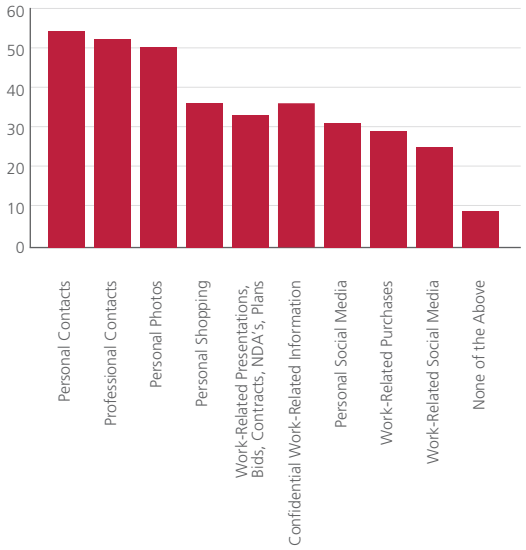


According to the Gartner report, "Forecast: Mobile Application Stores, Worldwide, 2008-2014," January 26, 2011, 17.7 million mobile apps will be downloaded in 2011 (a one hundred percent increase from 2010), and is projected to generate more than $15 billion in app store revenues.[5]

Reliance on mobile devices is already significant and accelerating rapidly; the emerging mobile environment is both diverse and freewheeling.

Organizations are already heavily reliant on the use of mobile devices with almost half of organizations claiming to be "very reliant."

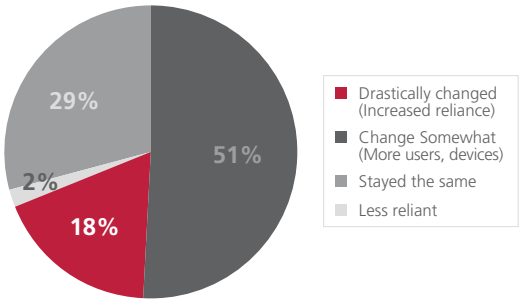
Types of Information and Apps Used on Mobile Devices



Almost half of organizations surveyed are at least very reliant on mobile devices, with 31 percent saying they were "very reliant," and 18 percent saying they were "extremely reliant." Almost seven in 10 organizations are more reliant on mobile devices now than they were 12 months ago. More than half (51 percent) said that has changed somewhat, while 18 percent said things have "drastically changed."

"The proliferation of mobile devices is continuing at a rapid rate, both in developed nations and emerging economies"
Adrian Perrig, CyLab Technical Director

Reliance on Mobile Devices (Not Including Laptops)



Almost as many respondents named laptop computers (45 percent) as their primary work computer as named desktops (47 percent). In seven countries, laptops are more likely to be considered their primary work computer. In India, only 13 percent of those surveyed said their primary work computer is a desktop, while 57 percent said it is a laptop and 16 percent said it is smartphone. The U.K. had the highest number of respondents, with 64 percent relying on their laptops as their primary computer. There was also a greater acknowledgement of laptops as the primary work computer in certain industries: Business and professional services (55 percent), electronics (51 percent), energy and utilities (49 percent) and high-tech and telecom (53 percent).

"The proliferation of mobile devices is continuing at a rapid rate, both in developed nations and emerging economies," says CyLab Technical Director Adrian Perrig. "Smartphones with fast processors, high-resolution touchscreens, location information and ubiquitous connectivity offer fundamentally new applications and services. In our everyday life, we can start to witness transformations in the way we interact with people and services. These transformations will likely continue to accelerate, as new services become available, such as smart vehicles and smart homes. Unfortunately, such new environments also introduce new risks and vulnerabilities, which we will need to counter constantly as these technologies evolve."

Security Implications of Mobility in Twenty-First Century Computing

But what are the security implications of mobility in twenty-first century computing? It is a question that is receiving much attention–and for good reason.

In its 2011 threat predictions, McAfee® Labs™ declared that "Attacks against mobile devices—including iPhones, Android devices, and more—will escalate in 2011 as criminals seek to tap into 'fragile cellular infrastructure' to access often unencrypted business and corporate communications. As mobile devices are increasingly commonplace in corporate and enterprise environments, there are more ways for trade secrets and other critical information to escape into the wild—and McAfee believes cybercriminals will increasingly be looking for it."

There are a wide variety of related risks and targeted at mobile devices. The underlying reason for this is the simple fact that mobile devices are treasure troves of sensitive information about users and the companies they work for.

Consider the contact list on a smartphone. It typically contains vital and sensitive intelligence on who the enterprise does business with, including current clients, promising prospects, critical suppliers, influential analysts and reporters, and others. It can also contain vital and sensitive intelligence on the user's personal life that could be used for social engineering purposes, to guess passwords, and to gain access to a corporate network. This information can be obtained by stealing the device itself, coming across a lost device, installing malware hidden in a seemingly harmless app, or even in some unexpected, accidental way.

Attacks against mobile devices—including iPhones, Android devices, and more—will escalate in 2011 as criminals seek to tap into 'fragile cellular infrastructure' to access often unencrypted business and corporate communications.

Of course, contact lists are not the only source of vital intelligence and sensitive information. Other sources include call records, calendars, SMS, and email correspondence stored on smartphones and laptops. Scrolling through this data can reveal secrets and expose weaknesses. If documents such as spreadsheets, business plans, and bids attached to email messages were to fall into the wrong hands, the consequence would be devastating; and the breach could occur as a result of a commonplace act of negligence, such as leaving a mobile device in the hotel lobby bar (even if you later retrieve it).

Smartphones and laptops also likely contain cameras and audio recording capabilities. The smartphone's camera is one of the reasons that many enterprises prohibit visitors' cell phones in certain sensitive areas of their operations. The intention is to reduce the risk of industrial espionage and other hostile activities. But what if that smartphone or laptop camera were activated remotely and turned against an individual or enterprise? What if a remote attacker turned a smartphone or laptop into a tape recorder concealed in plain sight, and was carried into the enterprise's inner sanctum? What if the photos, videos and audio files on the smartphone were accessed remotely, without the user's knowledge or consent, or fell into the wrong hands because the device was left in a meeting room at an industry conference?

These scenarios are not from the world of Ian Fleming's James Bond novel; they are real-world scenarios from today's mobile computing environment. But the risks related to mobile devices are not limited to powerful laptops and full-featured smartphones. There is great danger in removable media as well, such as a USB memory stick or an external hard drive.

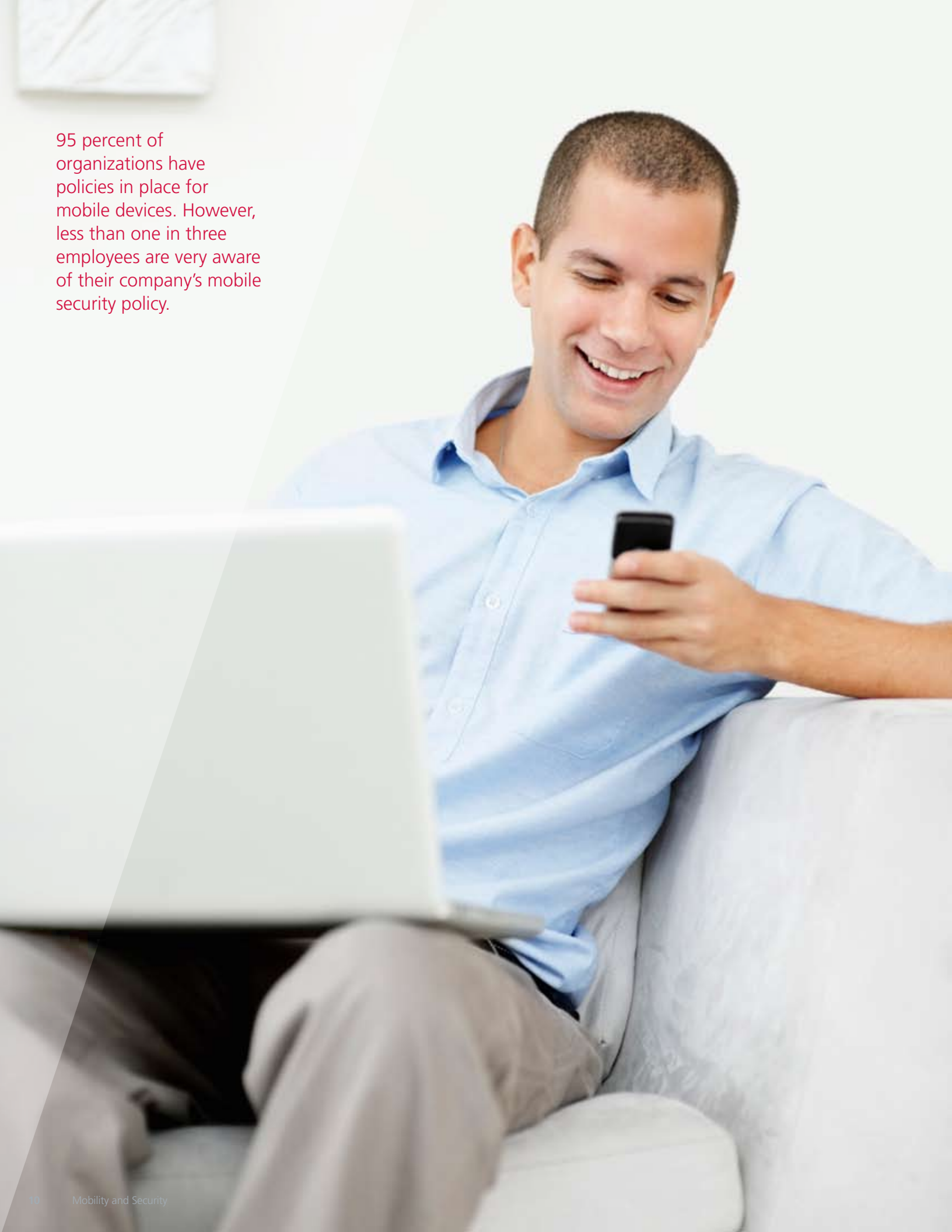
Consider the saga of Wikileaks. This blockbuster news story underscored concerns about USB drives. In the wake of the release of classified U.S. government documents, the Pentagon banned the use of CDs, DVDs, USB drives, and other removable media on classified military computers. Ironically, in a poignant reminder of the ceaseless struggle to make sense of the trade-offs between security and ease of use, there had been a prior ban on such removable media, a response to a worm attack on hundreds of thousands of computers. But that ban was lifted in February 2010. It was in the months after the lifting of the initial ban that the leaked documents were obtained.[6]

There seems to be no end to the potential weaponization of mobile computing. Even the USB cable has been successfully exploited as a means of attack. Two researchers at George Mason University figured out a way to attack laptops and smartphones through an innocent-looking USB cable. Angelos Stavrou, an assistant professor of computer science, and Zhaohui Wang, a student, wrote software that changed the functionality of the USB driver so that they could launch a surreptitious attack while someone is charging a smartphone or syncing data between a smartphone and a computer.[7]

A large-scale, simulated cyberattack conducted by the Bi-Partisan Policy Council in 2010, pointed out that such concerns have reached the corridors of power. The simulation envisioned an attack that unfolds during a single day in which 20 million of the nation's smartphones have already stopped working. The simulated attack, based on a piece of malware planted in phones months earlier through a popular "March Madness" basketball bracket application, disrupts mobile service for millions. The attack escalates, shutting down an electronic energy trading platform and crippling the power grid on the Eastern seaboard.[8]

In the wake of the WikiLeaks release of classified U.S. government documents, the Pentagon banned the use of CDs, DVDs, USB drives, and other removable media on classified military computers.

95 percent of organizations have policies in place for mobile devices. However, less than one in three employees are very aware of their company's mobile security policy.



Security Policy Versus Mobile Reality

There is a serious disconnect between policy and reality and between policy awareness and policy adherence, in the mobile computing environment. Both IT directors and users are dissatisfied with the status quo.

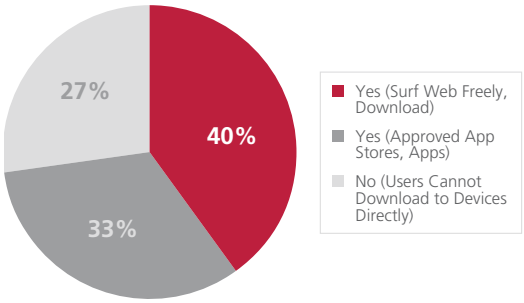
"Unless the device belongs to a large company, with a security policy in place, users tend to use their own device to accomplish job tasks and are not aware of the risks they are incurring," says Monica Mistretta, owner of Netmedia, a Mexican independent publishing company specialized in business technology.

Recognizing that mobile devices pose a security risk, 95 percent of organizations have policies in place for mobile devices. However, less than one in three employees are aware of their company's mobile security policy. Worse yet, fewer than half of companies report that all of their employees understand their mobile device access/permissions.

Furthermore, this disconnect seems to extend to the intent and nature of mobile-related security policies. More than half of those aware of their company's policies view them as stringent or very stringent. But one in five IT departments characterized their policies as severely restricting.

Policy creation and enforcement are proving problematic. Creating mobile device policies is a difficult task–only one in 10 describe the process as being very easy. Only one in 10 find enforcing, monitoring, or reporting data/device use very easy.

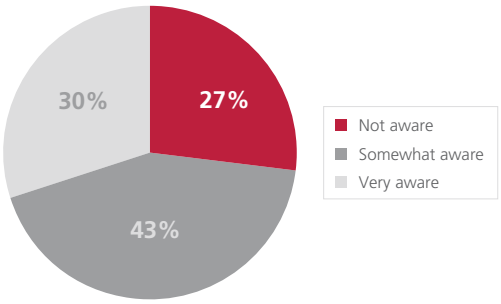
Allowing Users to Access App Stores with Mobile Devices



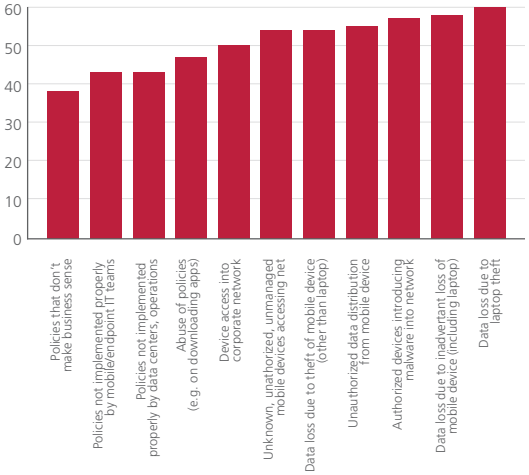
The lack of policy restrictions hints at potential security issues. Four in 10 organizations do not have a policy on the number of devices their employees are allowed to sync. Four in 10 organizations allow employees to access the Internet and download mobile apps freely, using their mobile devices. More than a third of businesses allow mobile device users to connect to the internal network with those devices.

Lost and stolen mobile devices are seen as the greatest security concern in the mobile computing environment. Loss of a device and the theft of a device are the two most commonly reported concerns of users of mobile devices. Loss and theft are also the security issues that worry the most IT directors.

Awareness of Company Security and Data Protection Policies for Mobile Devices



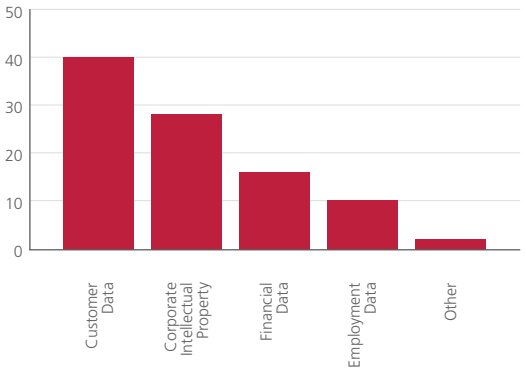
Greatest Security Concerns–Mobile Devices



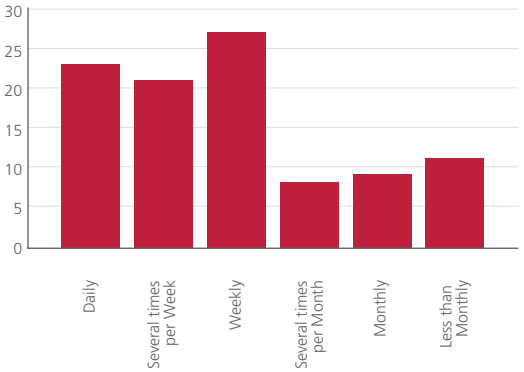
Four in 10 organizations have had mobile devices lost or stolen and half of lost/stolen devices contain business critical data. More than a third of mobile device losses have had a financial impact on the organization and two-thirds of companies that had mobile devices lost/stolen have increased their device security afterwards. One in 10 did not implement further security after device losses because of a lack of budget.

Although the need for mitigating mobile security risks and threats is acknowledged, risky behaviors and weak security postures are common. Fewer than half of device users back up their mobile data more frequently than on a weekly basis. Around half of device users keeps passwords, pin codes or credit card details on their mobile devices. One in three keeps sensitive work-related information on their mobile devices.

Types of Data on Lost or Stolen Mobile Devices



Frequency of Mobile Device Backup



Between one-fifth and one-third of device users said they "feel safe" against the array of possible security threats. It is therefore not surprising that around two-thirds of users would like to have each of the mobile security facilities listed. And yet, one-half to two-thirds of these users would *not* be willing to pay for such services, suggesting that even though they may have purchased the devices, they do not feel they should be paying for the additional security that the workplace may require.

Mobile devices are almost universally used for email, followed by contacts, web access and calendaring, with 93 percent using them for email, 77 percent managing contacts, 75 percent web access, and 72 percent calendaring.

Almost Half of Users Keep Sensitive Data on Mobile Devices

	Passwords/ Pin Codes	Credit Card details
Professional & personal information & data	23%	19%
Only professional information & data	11%	7%
Only personal information & data	17%	15%
I do not use, store or send this information or data using mobile devices	49%	58%

Mobile devices are being used by much of the workforce, over extended periods of time, for a significant percentage of tasks previously conducted on desktops. On average, employees use mobile devices for work purposes between two and 4.5 hours a day. On average, use of laptops was 4.5 hours per day. This was significantly higher in India, where the average was 5.9 hours per day. This was also higher in the energy and utilities sector, where usage was 5.5 hours per day. Use of smartphones was 2.6 hours per day, which was also significantly higher in India, at 3.7 hours per day, and in energy/ utilities at 4.6 hours per day.

Mobile devices are used in a wide range of job functions, with business executives using them most (56 percent), followed by sales and others in the mobile workforce (47 percent). One-third of organizations allow all employees to use mobile devices. This is significantly higher in Canada (55 percent) and in Entertainment/Media/Leisure sector (64 percent).

Mobile devices are almost universally used for email, followed by contacts, web access and calendaring, with 93 percent using them for email, 77 percent managing contacts, 75 percent web access, and 72 percent calendaring.

The mobile computing environment in the organizations surveyed is diverse, and the range of mobile devices used for professional purposes is extensive. Four different types of mobile devices are used by at least one-third of employees both for professional and personal use, laptops (72 percent), smartphones (48 percent), removable media, including USBs (46 percent), and external hard drive (33 percent). Usage of smartphones was significantly higher in China (72 percent) and Mexico (72 percent).

"There is both a lack of separation between devices and a lack of awareness of company policies."

CyLab researcher Patrick Tague addresses several aspects of the survey results that underscore some glaring shortcomings of mobile security and policy management:

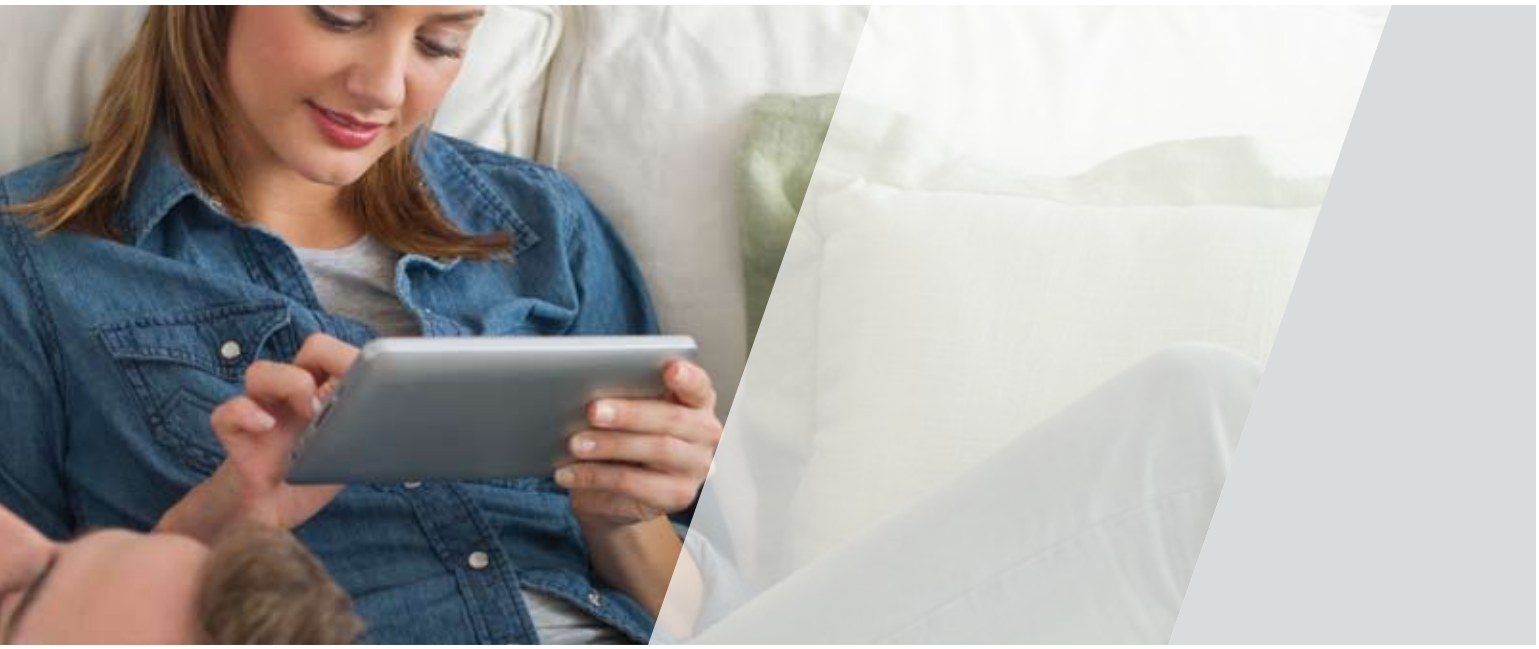
- Lack of separation between devices for personal and business use: Since the importance of device separation has been a recurring problem for many years, especially with the explosion of malware living on the web, I really hoped that policy-makers and administrators would have adopted more strict policies regarding the use of personal devices for business purposes. However, this result is not surprising due to the overhead that would be required to ensure device availability and policy enforcement.

- Overwhelming lack of awareness of company policies regarding security and privacy: In addition to demonstrating the lack of internal education or training regarding company policies, which is a severe limitation of any approach to security management, this lack of awareness hints at additional shortcomings: a necessary lack of policy enforcement (which would immediately alert the administrators of training gaps) and gaps between intended and actual employee behaviors with respect to policies.

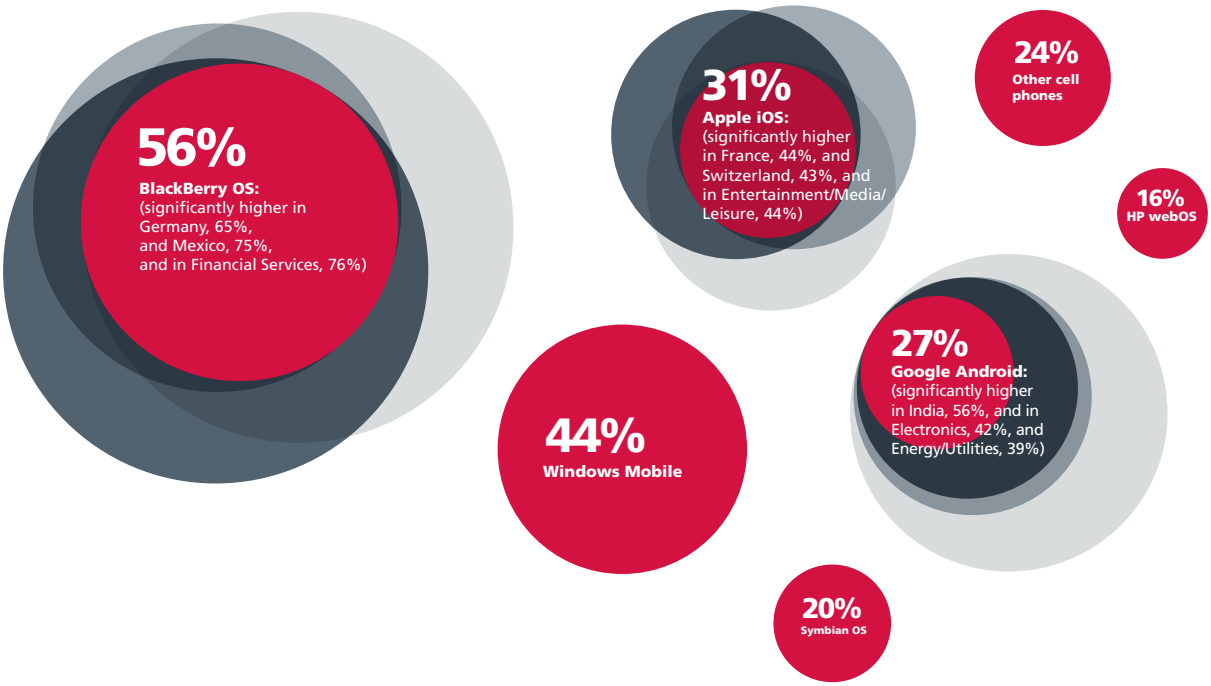
- Apparent unwillingness of the majority of administrators to pay for mobile security products or services: While this result is not terribly surprising, it is very unfortunate as such administrators are undoubtedly exposing their company's employees and assets to unnecessary/preventable risks.

  "I was pleasantly surprised to see that administrators are increasingly incorporating location and other contextual information into security management," says Tague. "These sorts of data provide useful supplements to traditional access control and authentication mechanisms that will undoubtedly improve usability."

Although BlackBerry OS is still the most supported smartphone platform (by more than half of the organizations surveyed), several others show significant market share, and with Verizon's adoption of the iPhone, it is reasonable to expect these numbers to change over the next few months.



Smartphone Support Platforms



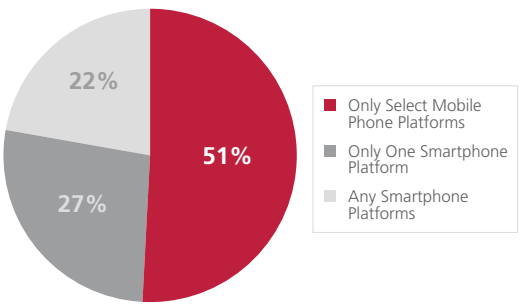
"Most organizations are aware that it will be increasingly challenging to restrict employees to use only the company-issued smart phones."

Satish Joshi, executive vice president, Patni Computer Systems

"Most organizations are aware that it will be increasingly challenging to restrict employees to use only the company-issued smart phones," says Satish Joshi, executive vice president, Patni Computer Systems. "They appreciate the enhanced security risks involved with allowing employees to bring their own devices, however, the exact nature of the risks and their potential impact is perhaps not fully understood."

The current mobile computing environment is a freewheeling one; and in many organizations, the workforce mixes business with pleasure. More than one in five organizations allow use of any smartphone platform in the workplace. Almost half of businesses (49 percent) allow employees to purchase their own mobile devices. On average, organizations report that almost two-thirds of their employees are accessing their corporate network with mobile devices used both personally and professionally.

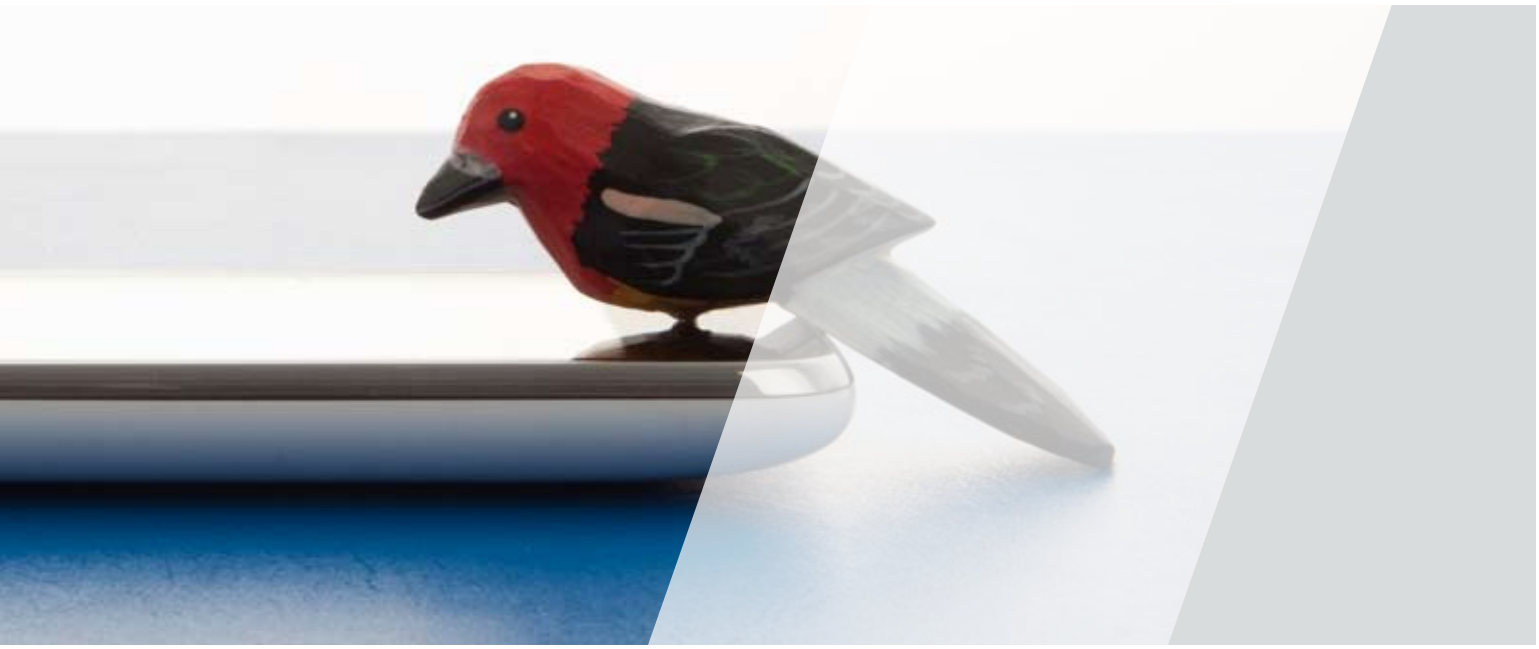
Diverse Smartphone Environments



Laptops and netbooks are the only mobile devices that are more likely to have been provided by the employer than to have been purchased by the employee. Around four in 10 employees are using personal mobile devices that organizations have no control over. One in five employees use devices provided to them by their employers, which the employers do not then manage. A quarter of organizations have no plans to distribute their own apps, encouraging employees to download apps themselves.

Lorrie Cranor, Ph.D, director of CyLab Usable Privacy and Security (CUPS), stresses the need for seamless security:

"It is noteworthy that across the world, we're seeing increased use of mobile devices as primary work computers. In the United States, desktop computers are still used as primary work computers by a little over half of those surveyed, but in many other countries, less than half of those surveyed use a desktop computer as their primary work computer. As mobile devices continue to replace desktop computers, they will likely be used increasingly to store confidential information, and the problem of securing them will also increase."



Location-Based Technology Could Improve Mobile Security

Respondents offered insights into additional technologies and services that may play a greater role as the mobile computing environment evolves further. More than one in five businesses are using location-based technology and almost half are considering do so.

"Using location-based technology is interesting," says CyLab's Michael Farb, one of the developers of KeySlinger, a security app for iPhone and Android smartphones. "It may provide a loss of privacy to the employee, but increased recoverability of the device to the employer. But the recoverability is only useful if the data on the device has been encrypted and not erased or otherwise compromised by the thief."

"I find it disturbing that only 22 percent are using location now, and that 30 percent are not even considering it" Martin Griss, director of the CyLab Mobility Research Center.

Martin Griss, director of the CyLab Mobility Research Center, concurs that mobile user location is an important element of security management.

"I find it disturbing that only 22 percent are using location now, and that 30 percent are not even considering it," says Griss. "Banks already know when my credit card is being used in unusual locations or in unusual ways and immediately try to protect me and limit risk–and the exposure that many companies face is significantly greater than misuse of my credit card. While it is not surprising that using context other than location is still in its early stages since most context-aware work is still in the realm of research, simple behavior monitoring to detect abnormal patterns, perhaps combined with location, is feasible today, and can significantly strengthen mobile security."

You are part of a computing sea of change, driven by users' desire for device choice and employers' need for cost savings."

Recommendations for Businesses and Consumers

Based on interviews with mobile security experts worldwide, McAfee has compiled the following list of recommendations for both businesses and individuals who use their devices to connect to corporate networks. These recommendations are designed to directly address the five trends identified by the research.

Recommendations for Mobile Users

- You are part of a computing sea of change. With devices eclipsing PCs, and virtually every app device-ready, mobile computing offers you an opportunity to be entertained, informed and connected wherever you are. Use this to your advantage to be more productive on the go.
- Driven by users' desire for device choice and employers' need for cost savings, individuals are increasingly bringing their own devices to work. Take advantage of your employers' program and use your technology to be more nimble in your work.
- Familiarize yourself with your employer's mobile device policy and the intent behind it, and decide whether it fits your needs. If so, accept the policy and move on; if not, use two devices–one for personal use and one for work.
- Take steps to secure your device. Install anti-theft technology, and back up your data. Configure your device to auto-lock after a period of time. Don't store data you can't afford to lose or have others access on an insecure device.
- Be aware of mobile device threats. In many ways, they are the same as in the online world. You can be hacked, infected, or phished on a mobile device just as easily (and often more easily) as you can online.

Recommendations for Businesses

- Mobility is ushering a new computing paradigm into the workplace. With devices eclipsing PCs and virtually every business application being device-ready, mobile computing offers an opportunity to make workers more productive, competitive, and happy. Mobility done right is a major competitive advantage in the workplace.
- Consumerization of IT is here to stay. Many smart companies are allowing, encouraging, and, in some cases, providing a stipend for, employee-owned technology to work. Businesses need to find ways to enable, secure, and manage employee-owned technology in an optimal way to drive cost savings.
- Users are changing the way they think about policies. Because employee-owned devices are artifacts of the more entrepreneurial employee-employer relationship, organizations need to apply policies in a nuanced, risk-based way that depends on the industry, the role, and the situational context.
- Data loss and leakage are of utmost concern to individuals and enterprises, and there is no silver bullet. Classify data, even at a high level, and apply data leakage processes and mechanisms in order to protect corporate data while respecting users' privacy.
- User awareness about mobile threats is still nascent. Apply security and management paradigms from laptops and desktops to mobile devices. Educate users about the risks and threats through employee agreements and training.

"Businesses must find ways to protect corporate data, and call it back when an employee leaves, while ensuring the privacy of the employee," says David Goldschlag, vice president of Mobility for McAfee. "Employees are no longer life-long members of the organization, but rather consumers, who often change jobs every few years. When they do, they come with a kit of stuff, but once they leave, they need to give you back the data that belongs to the company. Businesses need a way to facilitate that process while respecting the 'kit' that the employee brings to the company."

Conclusions

The consumerization of IT is forcing businesses to look at ways they can extend BlackBerry-like functionality to non-BlackBerry devices. Businesses now operate in a heterogeneous mobile environment where BlackBerrys are no longer the standard, requiring them to invest in new technologies. Furthermore, mobile users, who are primarily consumers, only want to carry one device and use that device to connect to their company's network. This creates new technical challenges for both organizations and users.

"Mobile devices are more prone to theft or loss, but mobile connections can enable mobility using security mechanisms with device tracking" says Eduardo Tude, founder and chief executive officer of Teleco, a consulting company and leading telecom Brazilian information portal. "An example of this was developed by BlackBerry, which allows locking a smartphone and remotely erasing the data in the device."

But it is not just new technologies that need to be put in place. Businesses need to ask themselves serious questions about policies too. Users are saying that policies are too strict. So there seems to be a disconnect between policies and reality that needs to be addressed from both sides.

Businesses need to set policies, but apply them in a nuanced way and a risk-based way. Should these policies apply equally to everyone? For example, can an executive have more freedom than a bond trader in an investment bank? Users need to understand what their company's policies are and why they're in place. They must understand that they are stewards of their company's information, and that their own livelihood depends on keeping that information secure.

Businesses need to look at the challenge as an end-to-end challenge. Devices are no longer consumer devices or business devices. They are both. Mobile security needs to be incorporated into the device and the network. Service providers and manufacturers must be part of the equation and mobile users should make security part of the criteria for picking a device.

Devices are not just extensions of the computing structure, they are extensions of the user. The way users interact with their personal data mirrors the way they want to interact with corporate data. Knowledge workers want to access their Oracle, SAP, and Salesforce applications from the same device that holds pictures of their children's soccer game. They want one device for work, their lives, and their online commerce.

Businesses of all sizes must come to grips with the profound challenges in order to reap the benefits of the dazzling opportunities that mobile computing provides. These are global challenges, affecting businesses and users in every country and continuing to blur geographic boundaries. Where will it end? The possibilities are endless.

Devices are no longer consumer devices or business devices. They are both. Mobile security needs to be incorporated into the device and the network.

Methodology

In collaboration with Carnegie Mellon University, McAfee took a hard look at the topic of mobile security and the consumerization of IT. The online surveys were administered by international research firm Vanson Bourne. More than 1500 respondents from 14 countries, including Australia, Brazil, Canada, China, France, Germany, India, Japan, Mexico, the Netherlands, Spain, Switzerland, the U.K., and the U.S., participated in the survey. The participants were split between two surveys targeted towards general end users of mobile devices and senior IT decision makers in companies with 100 or more employees.

Contributors

Richard Power, CyLab Distinguished Fellow

Lorrie Cranor, Director of CyLab Usable Privacy and Security (CUPS)

Michael Farb, Research Programmer with CyLab

Collin Jackson, Assistant Research Professor with CyLab

David Goldschlag, Vice President of Mobile for McAfee

Martin Griss, Director of the Carnegie Mellon University Silicon Valley Campus, Director of the CyLab Mobility Research Center

Nicolas Christin, Associate Director of Information Networking Institute

Satish Joshi, Executive Vice President,
Patni Computer Systems

Adrian Perrig, CyLab Technical Director

Patrick Tague, Assistant Research Professor with CyLab

Eduardo Tude, Founder and Chief Executive Officer of Teleco

Monica Mistretta, Owner of Netmedia

References:

1 *CNET, 6-1-10 <http://news.cnet.com/8301-13860_3-20006526-56.html>*

2 *CNET, 12-25-09 <http://news.cnet.com/8301-1023_3-10421920-93.html?part=rss&subj=news&tag=2547-1_3-0-20>*

3 *MSNBC, 7-7-10 <http://www.msnbc.msn.com/id/38126866/ns/technology_and_science-wireless/>*

4 *Wired, 8-20-10 <http://www.wired.com/gadgetlab/2010/08/supercomputing-app-android/>*

5 *CNET, 1-26-11 <http://news.cnet.com/8301-31021_3-20029666-260.html>*

6 *Wired, 12-9-10 <http://www.wired.com/dangerroom/2010/12/military-bans-disks-threatens-courts-martials-to-stop-new-leaks/>*

7 *CNET, 1-19-11 <http://news.cnet.com/8301-27080_3-20028919-245.html>*

8 *Dark Reading, 2-17-10 <http://www.darkreading.com/security/news/222900775/u-s-fails-test-in-simulated-cyberattack.html>*

About the Author

Richard Power, a CyLab Distinguished Fellow, writes and speaks on cybersecurity. From 1995 to 2002, he directed the CSI/FBI Computer Crime and Security Survey, a widely cited study that identified several trends which have come to shape the spectrum of twenty-first century cyberrisks and threats.

Power is the author of *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace* (Que) and co-author of *Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21st Century* (Syngress).

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

www.mcafee.com

About CyLab

Carnegie Mellon CyLab is a bold and visionary effort, which establishes public-private partnerships to develop new technologies for measurable, secure, available, trustworthy, and sustainable computing and communications systems. CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy, as well as security awareness among cybercitizens of all ages.

Building on more than two decades of Carnegie Mellon leadership in Information Technology, CyLab is a university-wide initiative that involves more than 50 faculty and 100 graduate students from more than six different departments and schools.

www.cylab.cmu.edu/

McAfee
2821 Mission College Blvd.,
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for education purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided 'AS IS' without guarantee or warranty as to the accuracy or applicability of the information to any specific situation of circumstance.

McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2011 McAfee, Inc.