www.pwc.com

Managing security in a mobile world

Advisory Services
Security

Employee use of mobile devices has skyrocketed, creating unprecedented threats to information security. Businesses that prepare for these risks can enhance productivity and gain competitive advantages.

Table of contents

The heart of the matter

Employees want to access work files from the same mobile device they use to update their Facebook status, check Twitter feeds and text with the kids. And who can blame them?

Accessing corporate data from mobile devices empowers workers to be more accurate, efficient and flexible. The handhelds and apps are familiar and convenient, and the device is always at hand.

Today, mobile devices have been adopted across industries – including healthcare, insurance, financial services, and retail and consumer companies, to name a few – to enhance employee productivity. Their flexible data input options, portable size and ubiquitous connectivity have redefined when, where and how work is done. As a result, telecommuting has become available to a broader set of employees, an option that enables an organization to better attract and retain top talent, particularly younger workers.

Mobile technologies also offer simplified installation and maintenance of applications, particularly when virtualized or implemented as cloud-based services. When two-step authentication is employed, a mobile device can simplify and improve overall security efforts while reducing IT costs.

To be sure, these benefits are undeniable. And so are the risks.

Consider a smartphone that is left in a taxi or restaurant.

Once lost, the mobile device becomes a security liability for IT, a trove of corporate data and intellectual property, communications records, voicemail messages and customer data that are at risk of theft or leakage.

Threats are not limited to misplaced or stolen hardware, however. Mobile devices also can expose organizations to data loss as a result of malware, worms and Trojans. Further compromising security is the expanded use of mobile social networking apps, which open the door for employees to unwittingly reveal proprietary information or download malware, and cloud computing services that can obfuscate control and ownership of data.

The threat is sure to elevate. Already, 63 percent of devices that access corporate resources are used for work and personal activities, according to a survey by security firm McAfee.[1] And that number will undoubtedly increase as younger employees — digital natives who have grown up with the Internet in their pockets — enter the workforce and bring their own technology with them.

While beneficial in many ways – and obviously the future of workplace technology – mobile technology has profoundly elevated threats to information security. Yet businesses that proactively address these risks and implement effective security capabilities can gain great opportunities for enhanced productivity and competitive advantages.

[1] McAfee, Mobility and Security: Dazzling Opportunities, Profound Challenges, May 2011

An in-depth discussion

Mobile technology has taken the workplace by storm.

Across industries and across the globe, employees have adopted smartphones and tablet computers to create a customized and flexible work environment. These tools wrap powerful apps and rich content in a compelling package that enhances connectivity, productivity and communications. To users, they have become more companion than machine; for many, mobile devices have become an extension of their personal identity.

In the United States, 38 percent of consumers now own smartphones, and the majority of new handsets purchased are smart devices.[2] Tablet computers have gained mind-share — and market share — at an unprecedented clip. Consumers and businesses snapped up 25 million iPads during the first 14 months of sales. That enthusiasm shows no sign of slowdown: Gartner estimates that 326.3 million tablet computers will ship each year by 2015.[3]

As smartphones and tablets have proliferated, the number of mobile apps designed for these devices has quickly eclipsed development and sales of PC software. There will be 1.3 million-plus apps for download on smartphones and tablets by early 2012, according to an IDC forecast.[4]

These apps represent a tremendous convenience for users — and pose an unprecedented risk to information security. The sheer number of mobile apps makes it all but impossible for IT to control use of approved software. What's more, the process of downloading applications can be a dangerous source of mobile malware that can penetrate the enterprise network. In part, that's because only a fraction of mobile devices employ antivirus software. Apple's security model for iOS does not permit third-party anti-virus software to access its file system. Android devices can run anti-virus apps, but available solutions do not measure up to the robust capabilities of software that information security professionals use for laptops and desktops.

This surge in devices and apps has resulted in soaring use of the Internet, either by cellular data connection or Wi-Fi. According to one estimate, mobile data traffic will increase at a cumulative annual growth rate of more than 100 percent.[5] As mobile data traffic rises, risk to the corporate network and data escalates because many users store sensitive work information on their handhelds and transmit this data, without regard to security, via the Internet. In most cases, data is not transmitted across a secure network, which would allow IT to block unwanted sites and employ technologies such as data loss protection (DLP), among others.

[2] Nielsen, In U.S., Smartphones Now Majority of new Cellphone Purchases, June 2011

[3] Gartner Research, Forecast: Media Tablets by Operating System, Worldwide, 2010-2015, 3Q11 Update, September 2011

[4] IDC, Managing Consumerization of IT: CIO Recommendations for Effective Bring Your Own Device Strategies, Doc # LM51T , Nicholas McQuirem May 2011

[5] GigaOm, Mary Meeker: Mobile Internet Will Soon Overtake Fixed Internet, April 2010

The convergence of devices, apps and mobile data transmission has complicated IT's mission to secure corporate data and networks. Many security leaders understand the magnitude of mobile threats, but few have taken action. In PwC's 2012 Global State of Information Security survey, only 37 percent of respondents reported that their organization has implemented a security strategy for mobile devices.[6]

How mobile devices jeopardize security

To safeguard the organization's data and networks, businesses must apply traditional security measures — and more — to mobile devices.

Whether the employee or the business owns the device, the information security department must protect data stored locally and data in transmission; this data includes personally identifiable information (PII) of employees and customers, as well as corporate data and intellectual property.

Traditionally, these tasks have been easier because IT tightly controlled the hardware that is purchased and used on the network. That's all changing, however, as the types of mobile devices multiply and employees insist on using their own familiar, and often more advanced, technology in the workplace. Another complicating factor: Advances in technology inspire users to upgrade devices much more frequently than in the past.

The proliferation of connected handhelds, and the divergent operating systems they run on, has created an IT management nightmare. The market for portable devices is constantly shifting, with products introduced and sometimes discontinued at a rapid clip. IT must constantly monitor this unpredictable progression of devices to understand which models might gain consumer favor and show up uninvited on the corporate network.

As the types of portable devices multiply, so do attempts to exploit them. Today, cyber-criminals target mobile devices in greater numbers and with increased efficacy. Malware targeting smartphones and tablets rose by 273 percent during the first half of 2011 compared with the same period the year before, according to a study by G Data SecurityLabs.[7]

Cybercrime is driven by return on investment, and, as a rule, the more popular the operating system, the more enticing it will be to hackers. The Android OS, which currently claims 45 percent of the US mobile market[8], is the most prevalent target for malware developers today. Android is an open-source platform that, unlike iOS or the BlackBerry operating systems, is not tightly controlled and is thereby inherently more appealing to attackers. The Apple iOS, with 27 percent US market share, is considered comparatively secure, but security risks escalate when users "jailbreak" devices to override the limitations of the operating system. Regardless of OS, all Wi-Fi-enabled handhelds are vulnerable to attacks that allow a hacker to commandeer a user's email and social networking accounts.

[6] PwC, 2012 Global State of Information Security survey, September 2011
[7] G Data SecurityLabs, Share of Mobile Malware Increases by 273 Percent, September 2011
[8] comScore, comScore Reports September 2011 U.S. Mobile Subscriber Market Share, November 2011

A trifecta of ascendant risk

These threats are serious, but they have been eclipsed by a unique set of circumstances. Today, the consumerization of IT, the ascendancy of social networking and the ubiquity of cloud computing have converged to dramatically elevate risk.

As more consumers bring their own technology to work, IT is being forced to open the corporate network and data to employee-owned devices. This consumerization of IT, often referred to as "bring your own device" or BYOD, is an increasing concern for IT. One recent study found that 28 percent of the workforce is using non-company-issued computing devices for work-related tasks, and this percentage is expected to rise to 35 by mid-2013.[9]

At its core, risks for personally owned devices are greater because there may be legal barriers preventing the company from exerting the same controls that are applied to corporate-owned devices. For instance, if stolen, the IT department may not have the authority or ability to remotely wipe an employee-owned handheld.

It is difficult for IT to establish and enforce endpoint controls when a wide variety of nonstandard devices is allowed to connect to the network. What's more, C-level executives often obtain policy exceptions to use their own devices, and that increases the risk of data leakage from the individuals who have access to the company's most important and valuable information.

As consumers fuse their personal and professional lives on one device, many have discovered that their handsets lack adequate storage. Increasingly, they are turning to consumer cloud services to store and sync information. These public cloud services are convenient, yet they jeopardize security because they are out of IT's control. Storage of corporate data on public cloud services raises concerns about data security, ownership of data and data leakage, among others.

Also elevating risks is employee use of mobile apps to access social networking sites such as Facebook, Twitter, and LinkedIn. Today, one in three US mobile users accesses social media sites using mobile apps, and use is growing at solid double-digit rates.[10]

Social networking is inherently risky because it is built on the premise of trust among friends and contacts, providing cybercriminals a uniquely effective attack position. Users may click links from friends that have been infected with malware, or unwittingly share information that enables competitors to gain advantages.

How security enables effective mobility

The hurdles that mobile devices bring to the enterprise are substantial, but certainly not insurmountable. We believe that businesses can transform IT to securely take advantage of mobility while minimizing risks to data, networks and applications.

One thing is certain: Mobile devices will demand new governance, support processes, and skills from IT.

The first step will be an update to the governance model to incorporate mobile information-sharing rules and define the goals and objectives for managing mobility risks. These decisions should be made by a steering committee that includes the marketing, legal and customer relationship departments, as well as the CSO and other

[9] Citrix, IT Organizations Embrace Bring-Your-Own Devices, July 2011
[10] comScore, Social networking on the go, October 2011

risk managers. The committee should identify the business units that will be affected by mobile device use, and pay careful attention to compliance with regulatory mandates and data privacy across the organization.

Mobility and cloud computing are inextricably intertwined because use of mobile devices will increase cloud usage. Cloud services can potentially increase risks that stem from intermingling of data, loss of corporate control across geographies, and employee and partner access of information after they separate from the business. It is essential, therefore, that organizations understand and proactively adopt cloud computing with a focus on mobile security. A critical component consists of virtualization technologies that will enable secure and efficient delivery of applications and data to handheld devices.

The proliferation of mobile devices will also require that businesses train the IT workforce to support secure app development and other mobile technologies. This may require new knowledge, such as an understanding of technologies like encryption, authentication and authorization controls. Certain IT staff also must gain proficiency in scripting languages which are used to build secure apps, as well as understand the security distinctions between native apps and Web-based apps. A renewed focus on monitoring and analysis of network traffic to and from mobile applications will enable IT to ensure security of infrastructure servers.

Mobile device support also will require that IT and help desk staff develop new skills and invest time to understand existing and emerging consumer technologies, as well as multiple operating systems employed by portable devices.

Most organizations with a large, heterogeneous mobile device ecosystem will consider third-party mobile device management (MDM) solutions that enable IT to centrally maintain consistent security controls across all devices. MDM also can help organizations update and consolidate crisis and incidence response capabilities. If a smartphone is lost or stolen, for instance, it can be remotely wiped and deactivated. Similarly, incidence response capabilities should also include the ability to mitigate malware infections as they occur.

Ultimately, the foundation of mobile security will require that businesses anticipate mobile security threats by leveraging a strong strategy for a BYOD environment, implement an effective and centralized security solution for all mobile devices across the enterprise, and employ strong authentication that balances asset protection with user convenience.

Taking the first steps toward a mobile strategy

The mobile landscape is evolving at warp speed. To balance data safeguards against the productivity and employee satisfaction that portable devices enable, organizations must implement a rigorous, comprehensive framework for security.

Correctly developed and deployed, an effective mobility strategy can produce productivity gains as high as 25 percent across the organization. [11] To do so, the mobility initiative should involve stakeholders from IT, finance, marketing and business units in the early phases of planning. To ensure that compliance and privacy measures are met, discussions also must include risk management, legal, compliance, internal audit and privacy departments. We believe that a wide-ranging group of stakeholders is necessary to plan a holistic mobile strategy that optimizes data use and effectively addresses security for the entire enterprise.

[11] AIIM, Capitalizing on Content: A Compelling ROI for Change, March 2011

Mobile security policies must manage the security of the device (whether owned by the employee or the enterprise), the data it accesses and stores, the applications it runs, and all interactions with the corporate network. Exposure of private, regulated data is a key risk and must be considered above all. At the same time, it's also essential to include crucial intellectual property such as trade secrets, patents and industrial designs.

As with any security initiative, security stakeholders must first consider an organization's unique risks and build a mobile security framework on the foundation of existing security measures. While mobile devices are typically seen as a network endpoint, the risks can be better understood by exploring how employees use the technology on — and off — the job.

The business must take stock of all mobile hardware used companywide and determine, to the greatest extent possible, what devices will be approved to access the network in the future. Once a standard for approved devices is in place, IT must implement preventive controls to ensure that unapproved units cannot access the network and also must assiduously monitor employees to ensure that they do not attempt to introduce unapproved devices.

Mobility champions also must decide what types of corporate data the approved devices can store, and determine the most effective security measures, such as encryption or authentication, for protecting data on those units. In doing so, it will be necessary to distinguish enterprise data from personal information, and identify appropriate measures to be taken when data is co-mingled.

An effective strategy also must clearly specify where corporate data is permitted to reside: on the device, on the network, on a public cloud service, or some combination of the three. Next, it will be necessary to classify the types of information that can be exchanged between the device and the corporate network.

The organization should carefully assess applications and services in use to determine the potential for risk. In a flawlessly controlled IT environment, only approved apps and services would be permitted to access the network. Given the phenomenal growth of mobile apps and services, however, this approach will be unfeasible. Organizations that develop their own mobile apps for employees and consumers, on the other hand, can confidently allow network access to these apps. It is critical, however, that internal developers take care — and time — to employ best practices for building secure apps. A rapid development process, which is often employed for building apps, may not allow time to ensure that appropriate security is applied.

Because social networking and cloud services carry unprecedented security risks, controls and standards for their use must be carefully developed, with early involvement between business, IT and security leaders. At a minimum, IT must ensure that cloud and data service providers meet the organization's security compliance requirements. It's also essential to implement mechanisms to enforce the controls and standards.

Once a comprehensive strategy and policy are in place, employees should be made aware of the policies and trained in best practices for secure use of devices. This may be the organization's toughest task. We have seen that employee awareness is often the weakest link in a security strategy -- an unacceptable situation since employee compliance with mobile security is uniquely critical to its success.

What this means for your business

Consumer mania for mobile devices is unstoppable. Already, smartphones and tablet PCs outnumber shipments of laptop and desktop computers.

Consequently, mobile security has become a flashpoint for IT as it grapples with a host of new challenges — and risks — to information security. In today's rapidly evolving threat environment, separating devices and vices will not be easy.

When creating a comprehensive mobile security strategy, mobility champions will need to take a step back and rigorously assess the IT and employee ecosystems, as well as gain a comprehensive understanding of current mobile usage trends and risks.

Taken together, the complex factors necessary to craft an effective mobile security strategy may require expert guidance. That's where PwC can help. We have global expertise helping companies improve risk management and understand the fast-evolving mobile landscape and emerging risk factors. Our team of experienced risk and technology professionals has helped organizations design, integrate and implement effective technology architecture and solutions that encompass mobile security planning as well as managing the impact of a mobile attack.

An effective mobile security strategy can enable your business to harness the productivity and flexibility of today's mobile devices and apps while safely dodging the risks. In a world of tremendous uncertainty, one thing is certain: The time to start planning is now.

Contacts

To have a deeper conversation on security for mobile devices, please contact:

Gary Loveland
Principal, National Security Leader
gary.loveland@us.pwc.com

Brad Bauch
Principal, Houston
brad.bauch@us.pwc.com

Rik Boren
Partner, St. Louis
rik.boren@us.pwc.com

Kevin Campbell
Partner, Atlanta
kevin.campbell@us.pwc.com

Michael Compton
Principal, Detroit
michael.d.compton@us.pwc.com

Shawn Connors
Principal, New York
shawn.joseph.connors@us.pwc.com

Scott Evoy
Principal, Boston
scott.evoy@us.pwc.com

Joe Greene
Principal, Minneapolis
joe.greene@us.pwc.com

Peter Harries
Principal, Phoenix
peter.harries@us.pwc.com

John Hunt
Principal, Washington
john.d.hunt@us.pwc.com

Jerry Lewis
Principal, Dallas
jerry.w.lewis@us.pwc.com

Mark Lobel
Principal, New York
mark.a.lobel@us.pwc.com

Sloane Menkes
Principal, Washington
sloane.menkes@us.pwc.com

Joe Nocera
Principal, Chicago
joseph.nocera@us.pwc.com

Chris O'Hara
Principal, San Jose
christopher.ohara@us.pwc.com

Fred Rica
Principal, New York
frederick.j.rica@us.pwc.com

Sohail Siddiqi
Principal, San Jose
sohail.siddiqi@us.pwc.com

Andy Toner
Principal, New York
andrew.toner@us.pwc.com

www.pwc.com