OPENTEXT

Getting Ahead of the Mobile Revolution

Leverage the Power of Your Growing Mobile Workforce

Today’s businesses face a technological sea change as employees continue to make BYOD (bring your own device) a staple of their work lives. On one hand, this shift lets organizations leverage the employee engagement and productivity mobile devices and apps support. Yet, on the other, it threatens the ability of IT departments to control and govern their information networks.

In this white paper we examine how the use of mobile devices has changed IT within the enterprise forever, and then outline techniques that can help your organization develop a mobile strategy that delivers end-user and business advantages.

Table of Contents

Introduction

Today's business organizations face a technological sea change as an increasingly tech-savvy employee base continues to make BYOD (bring your own device) a staple of their work lives. On one hand, this shift lets organizations leverage the employee engagement and productivity mobile devices and apps support. Yet, on the other, it threatens the ability of IT departments to control and govern their information networks.

There's no doubt that IT consumerization—the adoption of consumer-designed technology in the workplace—provides organizational value. For one thing, it helps satisfy a workforce raised on perpetual connectivity and collaboration. On top of that, many consumer apps actually provide a better user experience and functionality than the technology organizations might otherwise provide. That means users can easily integrate the lifestyle they're used to—using social media, sharing and networking—with their work life and requirements. However, while this emerging model may deliver productivity and satisfaction gains, it also creates a major challenge for IT departments as they try to manage networks that see enterprise data flowing back and forth across the traditional firewall.

The risk of security breaches; an audit trail that's impossible to follow; a multitude of governance and compliance concerns—essentially you have an IT department that's in danger of losing control of its core responsibility: information. These concerns are not idle. According to a survey of nearly 800 IT professionals, 79% of businesses experienced a mobile security incident between June 2012 and June 2013. The cost of mobile security incidents is also growing, with 52% of large companies reporting costs of over $500,000 and 45% of smaller businesses reporting costs in excess of $100,000.[1]

Far from limiting mobile apps and activities, though, organizations need to take advantage of their mobile potential. They need to provide enterprise software that is not only the optimal work solution, but that allows users to maintain the always-on lifestyle they're accustomed to while corporate necessities like information governance and compliance happen "under the hood." The alternative could do more than erode an organization's competitive edge. Failure to take appropriate action can also reduce a company's speed to market and hamper sales force productivity.

To help better understand this critical trend, this paper looks at the ways organizations currently address the mobile challenge; the flexibility and security capabilities future mobile advancements will demand; and the clear benefits the right solution and strategy can deliver—now and in the mobile enterprise of the future.

[1] Dimensional Research sponsored by CheckPoint Software Technologies Ltd., June 2013. "The impact of mobile devices on information security: A survey of IT professionals." http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report2013.pdf

Organizations Need a New Approach to a Classic Challenge

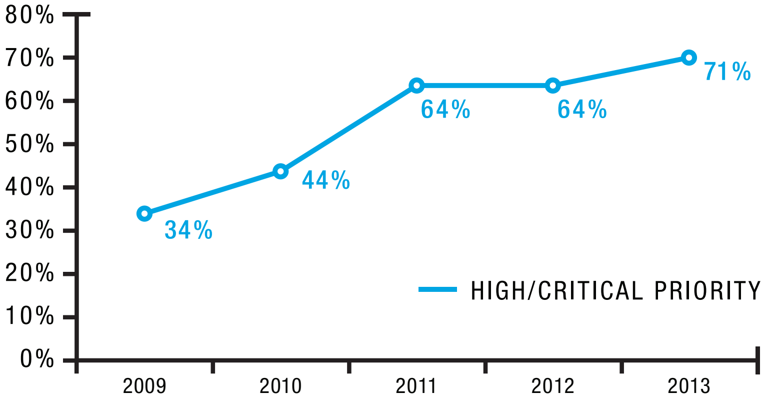
Managing and controlling information sharing has been one of the most basic responsibilities of the IT department since soft copies and virtual folders took over the office. Traditionally, the corporate firewall was the answer—keep the information contained and you keep it safe. This is no longer effective because it's no longer possible. With users intent on maintaining their personal connectivity and businesses keen to leverage the advantages connectivity provides within the workplace—information accessibility, collaboration, productivity, employee satisfaction, employee engagement—IT departments need to find a solution that addresses and unites both realities.

It's clear that the majority of organizations have a basic awareness of this imperative. According to Forrester Research, Inc.'s Forrsights Networks and Telecommunications survey, Q1 2013, **71% of IT decision makers report that supporting worker mobility is a top strategic priority, up from 34% in 2009.**

Social engagement through collaboration doesn't have to stop inside the enterprise, but it does have to be managed by the enterprise.

"Which of the following initiatives are likely to be your firm's top strategic telecom/ mobility priorities over the next 12 months?"

Mobility Support



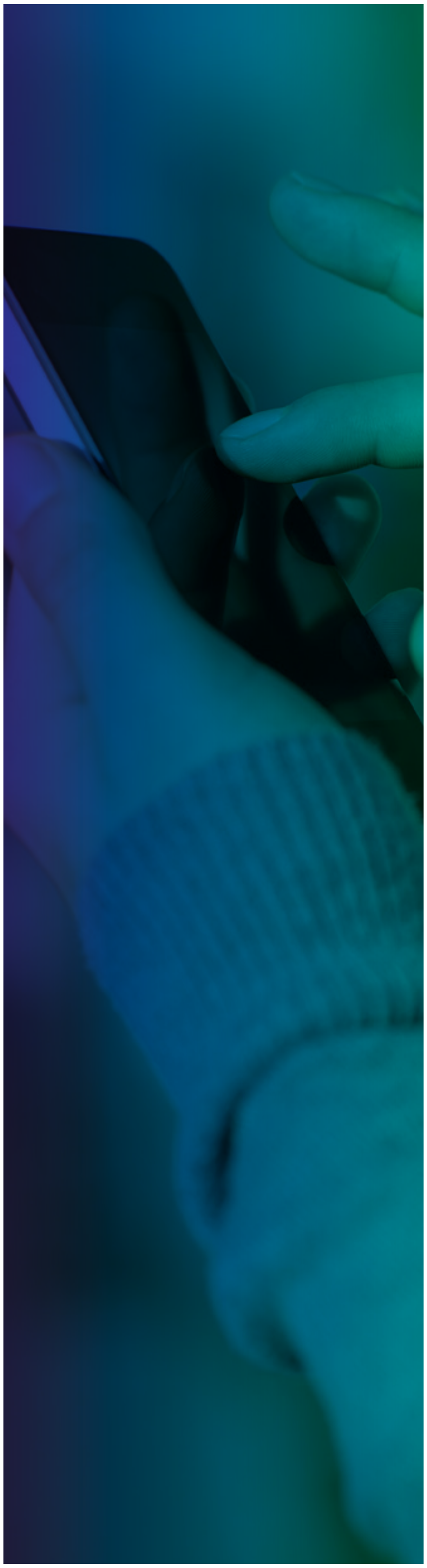
SAMPLE SIZE = NA & EU IT DECISION MARKERS:
2013 (N=2144)
2012 (N=2347)
2011 (N=2042)
2010 (N=1992)
2009 (N=1999)
SOURCE: FORRSIGHTS NETWORKS & TELECOMMUNICATIONS SURVEY, 2009-2013

Indeed, organizations are addressing the issue in a number of ways and with varying success. One way is to attempt to lock down the risk by essentially banning BYOD, as well as the use of sites like Facebook and Twitter from mobile devices. For example, employees may be asked to sign strict usage policies and threatened with instant dismissal for using instant messaging. Implementing such draconian usage policies, however, is a losing battle and tends to fail all around. It not only foments employee resentment, but users inevitably find workarounds that may be even more unsecure—such as making personal flash drive copies, uploading enterprise content to consumer cloud applications or using FTP and file sharing sites—to continue their activities. Moreover, shifting responsibility to employees will not absolve the company from prosecution should things go wrong.

Another option is for IT departments to provide employees with enterprise-owned smartphones and tablets. With the IT department in charge of setting up the devices and loading the requisite corporate apps, they can control what the devices will be used for, how they access the network and how auditable information will be tracked and reported. While this is a great solution for the business, users may be frustrated that they can't access the apps they use every day, with dissatisfaction and productivity risk again ensuing.

A third solution, however, and one that delivers satisfaction and sustainability on all sides of the mobile equation, is for IT departments to not just provide technology they can easily control, but to build custom, tailored applications that integrate with existing back-end systems. In this way, they can not only manage employee technologies, but also consolidate and modernize a range of existing applications and systems while extending fully managed support to smartphones and tablet computers.

With such a core platform in place, IT departments can then develop and distribute apps that help workers get their day-to-day jobs done without compromising their ability to use their own devices, and without having critical data shared across relatively insecure, personal-use apps and networks. These IT-managed apps can be deployed to BYOD users in a container app that remains effectively under the control of the IT department, in that the app and its contents can be remotely wiped if required. It also allows information to be managed even when it is outside the firewall and for audit trail and governance to be effectively maintained. This solution provides the best combination of IT enhancement, user satisfaction and organizational security and governance.



Flexibility Drives the Future of Mobile Productivity

Once a platform that addresses management, security and integration is planned or implemented, organizations can focus on maximizing the productivity potential of their mobile workforce and preparing for the dizzying possibilities mobile technology is poised to bring. Impending innovations such as Google Glass, smart contact lenses, smart watch technology, and a host of concepts we can't yet imagine will transform the mobile universe in myriad ways. Right now, it's critical that organizations have the flexibility to adapt securely, responsively and with agility to future advancements, leveraging their business and strategic potential without exposing enterprise data to risk.

Effectively managing the evolution of business mobility means focusing on three solution areas: the ability to access and work with enterprise content; the ability to store, share and synchronize information both in the cloud and on premise; and the provision of social collaboration capabilities specifically designed for the enterprise.

The ability to access and work with enterprise content

An organization's most basic productivity need is for employees to be able to view, edit and act on information residing in your ECM (enterprise content management) system. This capability must be available not only as a native smartphone/tablet app that's deeply integrated with ECM systems and information, but also in the cloud via web browsers. Indeed, access needs to extend to as many channels and devices as possible to accommodate user habits and trends. At the same time, any mobile app or solution will need to incorporate existing content permission and security policies to ensure compliance and mitigate security threats.

The ability to store, share and synchronize information in the cloud and on premise

Cloud security, which deals with information residing by definition outside traditional firewall boundaries, continues to be a challenge and for some an adoption issue. Organizations must, then, have the ability to extend the corporate firewall to effectively surround and protect their mobile workforce. On the user side, content management in the cloud must become a natural extension of existing productivity tools. Mobile workers need the ability to manage and synchronize information in the cloud from any device, anywhere, and across multiple devices. This is also true for organizations adopting a hybrid approach—one that enables information sharing and storage both within cloud applications and on premise. In either case, organizations must empower their mobile workforce without sacrificing the records management rigor and security demanded by existing internal policies—such as audit trails, version control and permissions—as well as industry regulations.

Social collaboration specifically designed for the enterprise

Most organizations now understand that leveraging the strategic value of social media to enable dialogue between employees, customers and partners and support marketing, brand and communications initiatives is an imperative—as is controlling the potential risks. Social media is an ever-shifting milieu with new channels and services opening up all the time. At the very least, the social workplace must incorporate features such as blogs, wikis, forums and communities without endangering information safety or compliance. This means allowing social media integration with organizational content and allowing content to be posted to Facebook, Twitter or Google, while also building integrated security controls directly into the enabling software to control where, how and for what purpose information is shared.

Moreover, to maximize your ability to adapt to new technology and opportunity, all mobile applications should be built on a common API platform that is connected to information repositories across the enterprise. Ultimately, solutions should not be restricted to mobile, but be deliverable via the web and desktop as well, providing true integration between products, content and services as well as centralized control and management.

Mutually Beneficial Solutions Deliver User and Organizational Advantages

The integration of effective mobile solutions is no longer a feature—it's an expectation for users who demand that their applications work across devices and environments. It's become apparent to organizations that, failing that level of usability, IT-supplied devices are likely to be shunned and potentially insecure workarounds, like copying data to USB sticks and storing it on home PCs, will be adopted.

To gain a full perspective on the benefits of a multi-faceted mobile solution, it helps to see your mobile users essentially as business consumers. They want and will seek out the best products and apps to help them do their jobs—with the proviso that their ingrained ways of communicating in today's connected culture are not significantly impacted. This actually presents an opportunity to organizations ready to seize it.

By providing users with options for working how, where and when they want—on enterprise-grade apps that provide a consumer-based user experience—you can leverage employees' existing skills and technological enthusiasm to drive organizational goals and strategy.

A Mobile Enterprise Strategy Starts with Enterprise-ready Solutions

Some companies are meeting the mobile challenge head on, but others are in danger of letting consumer products shape their business rather than molding those products to serve and support business needs. Achieving the latter requires not only leveraging advanced product capabilities but making them subject to the most effective security, compliance and governance controls.

Consumer devices, however, simply aren't built with the security features demanded by the enterprise. When they are shoehorned into that higher level of functionality without appropriate control measures, their capabilities—while perhaps satisfying owner/user needs and habits—will not be fully integrated with enterprise apps, systems and platforms, and are certainly not secure enough on their own to be part of the overall information network.

OpenText mobile solutions—OpenText ECM Everywhere, OpenText Tempo Box and OpenText Tempo Social—are built for the enterprise by information management experts who understand enterprise needs. With OpenText mobile solutions, you can maintain information security even outside the firewall, ensuring your smooth transition into the mobile future, and your ability to strategically and sustainably realize the advantages to come.

To learn more about how OpenText mobile solutions can help your organization manage mobile networking and information sharing while improving productivity and performance, please contact:

Advisors@opentext.com

The technological character of the enterprise is changing rapidly, and organizations must keep up. In the case of mobile, that change is already under way. We can stay connected in places never before thought possible—mountain tops, beaches, even on airplanes—but it's a communications panacea fraught with enterprise risk.

www.opentext.com

NORTH AMERICA +800 499 6544 ■ UNITED STATES +1 847 267 9330 ■ GERMANY +49 89 4629-0
UNITED KINGDOM +44 (0) 1189 848 000 ■ AUSTRALIA +61 2 9026 3400