ClickSoftware
Making Service Click

Mobile apps in the workforce:

Overcoming challenges to reap the benefits of a fully mobile workforce

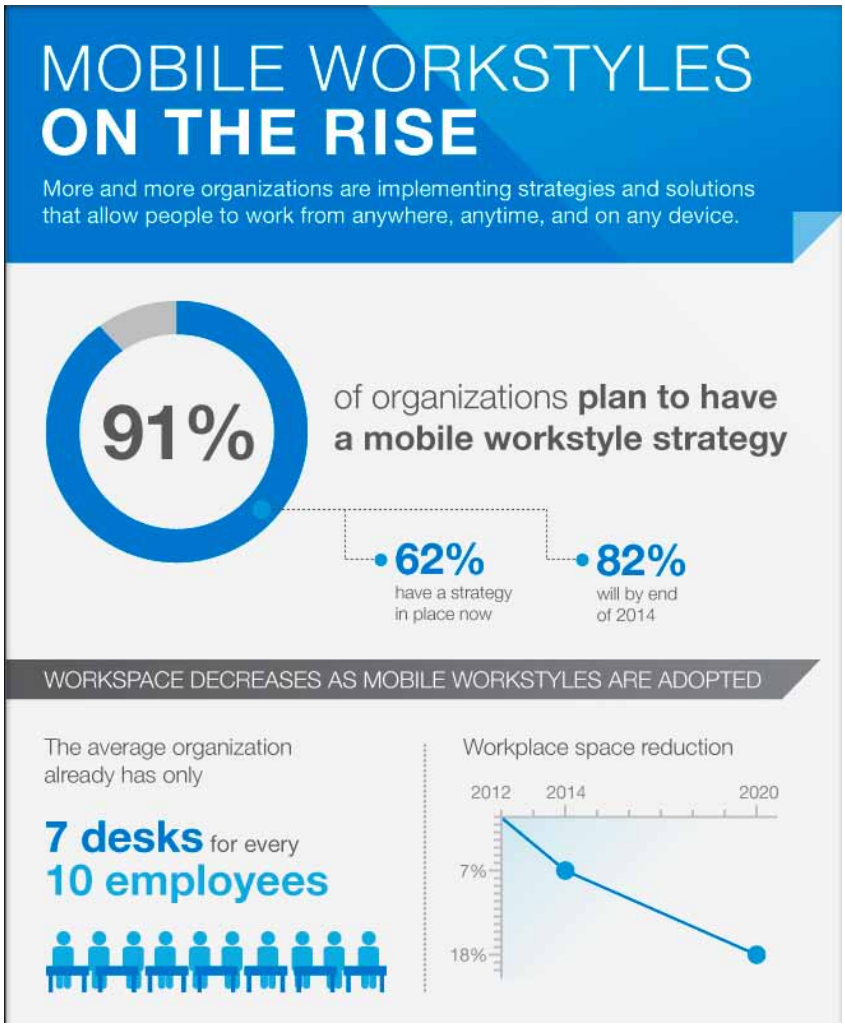
A ClickSoftware Business Paper

Mobile Apps in the Workforce: Overcoming Challenges to Reap the Benefits of a Fully Mobile Workforce

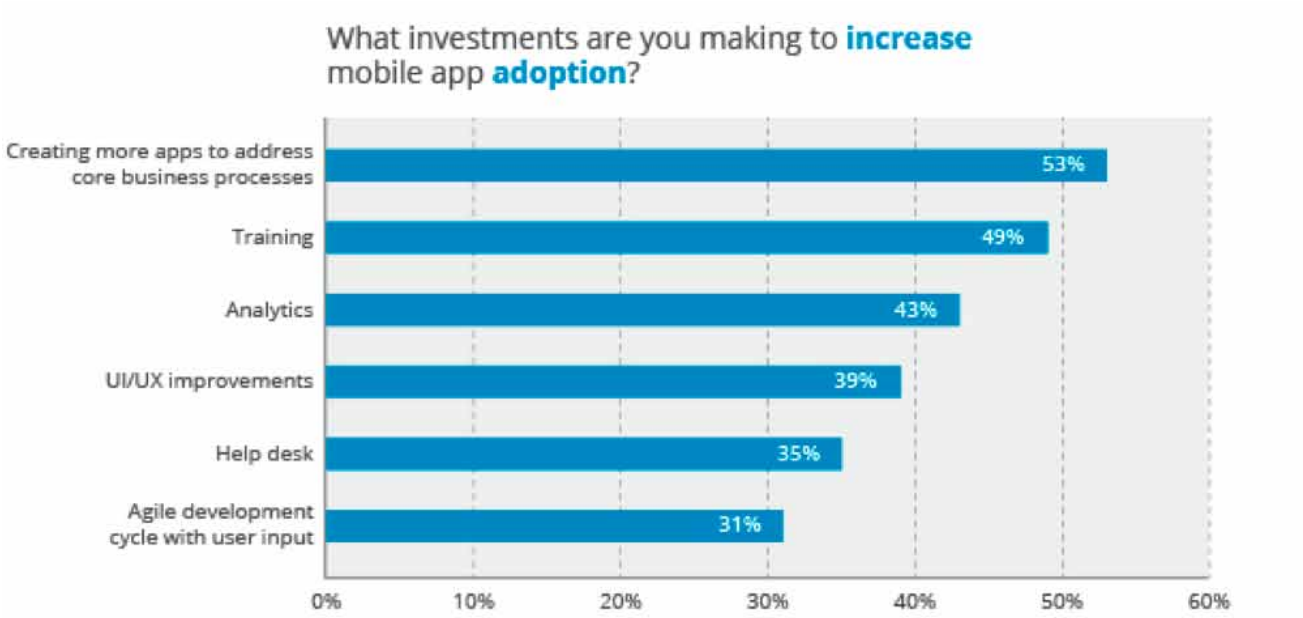
As more companies and organizations go mobile, executives and managers need solutions for better managing field workers, office staff, and back-office functions and systems. Similarly, all of the organization's people, from office staff to field workers, need to be able to communicate and have access to the critical information they need in order to conduct business. Another challenge is giving field workers, dispatchers, and managers access to the most up-to-date, real-time information to enhance collaboration. All of these interactions need to be seamless in order for the workforce to operate at optimal efficiency and productivity levels. The solution to all of these challenges is mobile apps.

Rates of Adoption of Mobile Apps in the Workforce

As the workplace becomes shaped by the demands of a mobile workforce, it is hard to characterize mobile as a trend: it's a reality. Citrix sponsored the Workplace of the Future global survey, which shows that the formula for the future of the workplace is one person using an average of six devices to do her work. Along the same lines, the number of desks per person is reduced as people shift work to more convenient times and locations and workers choose to use their own devices for work, known as Bring Your Own Device (BYOD).



Infographic via Citrix



Infographic via Apperian

As more employees use mobile devices to complete their work, more organizations and workers are embracing mobile apps. According to a CIO article, a recent Apperian survey found that more than 70% of respondents plan to equip more than 1,000 users with mobile apps. More important, 1/3 of respondents are deploying mobile apps to more than 5,000 users in the next two years. It's important to note that mobile adoption relies heavily on help desk support, a BYOD policy, tactics such as gamification, and other factors.

Other key findings of the Apperian Mobile Enterprise Application Survey include:

- Mobilizing business processes is key: 53% are creating apps to address core business processes, which includes internal app development or partners developing apps
- 49% of respondents believe training is crucial
- 43% of respondents are interested in analytics, which indicates that organizations are looking for more metrics about their mobility programs

Additionally, the Lopez Research Enterprise Mobility Benchmark reveled some telling trends in mobile workforce rates and mobile app adoption by companies:

- 68% of companies ranked mobile-enabling the business as a top concern for 2015, surpassed only by securing corporate data
- 60% of companies allow their employees to use personal devices to access business email and calendar apps
- 66% of IT leaders ranked defining a technical mobile add development strategy as their number one mobile concern
- More than 50% of the companies plan to build 10 or more enterprise mobile apps this year

How Mobile Apps Are Being Used In the Workforce

The right mobile apps for field service give the workforce full access to information from back-office systems. These apps work in any environment, whether offline or online. Most times, enterprise business apps are part of a scalable mobile workforce solution that can be configured with the mobile apps. Most mobile apps in the workforce give your workers access to comprehensive data and information on demand. Many organizations give their employees the right to use their own devices, enhanced with mobile apps that enable them to view jobs, service histories, and customer information, plus send messages, capture signatures, record asset details and parts usage, view manuals, collaborate with colleagues, and much more.

There are countless mobile apps available for the workforce today, and they provide several solutions for challenges faced by organizations. Some of the specific solutions provided by mobile apps in the workforce include…

- Work on any device and any operating system, including iOS and Android devices
- Schedule and dispatch so you can assign jobs and track them to closure
- Full offline capabilities that give field workers the ability to work continuously without connectivity and then synchronize business applications when they are back online
- Enterprise mobility apps often are available in collection packs or solution packs that include

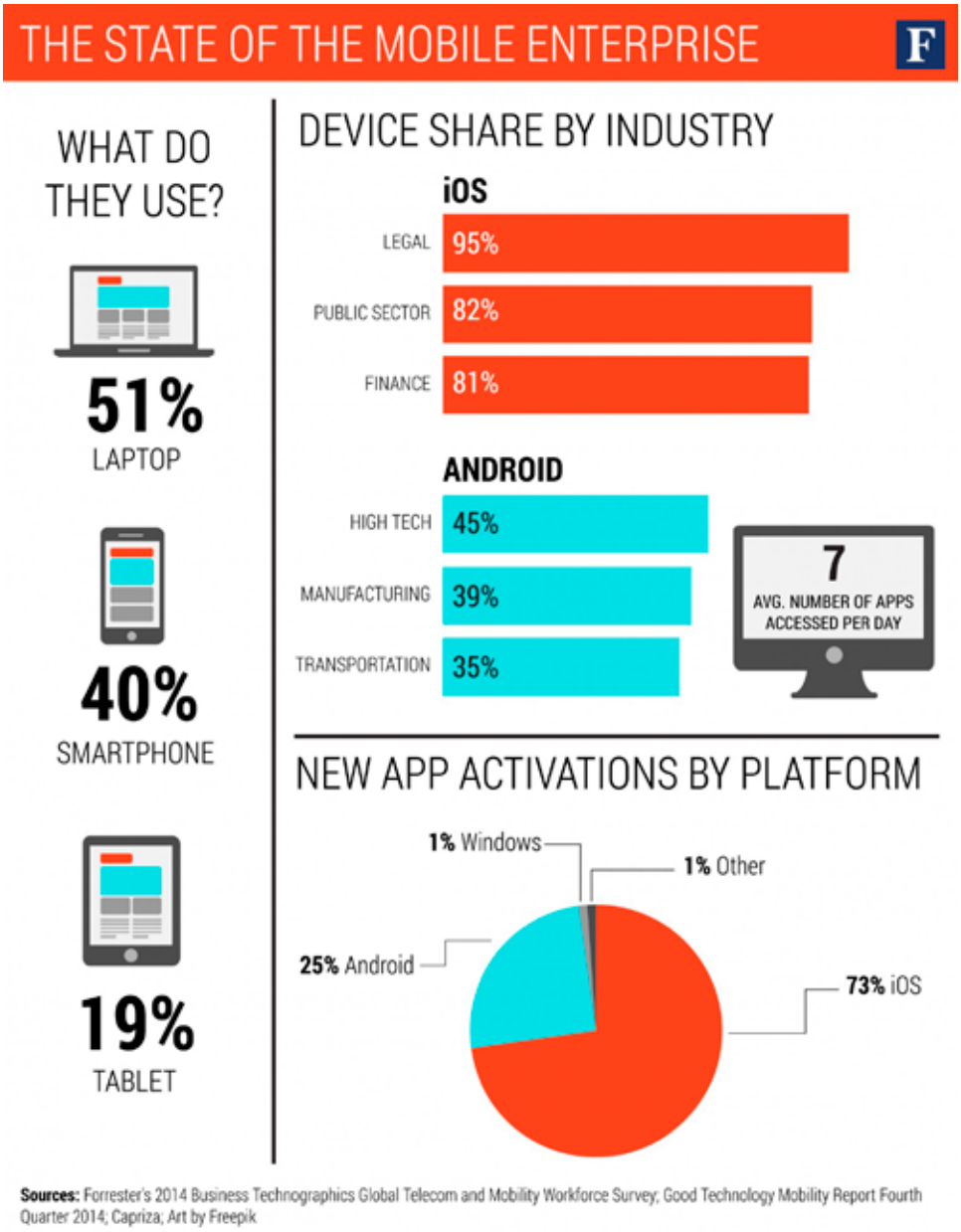


Image via Forbes

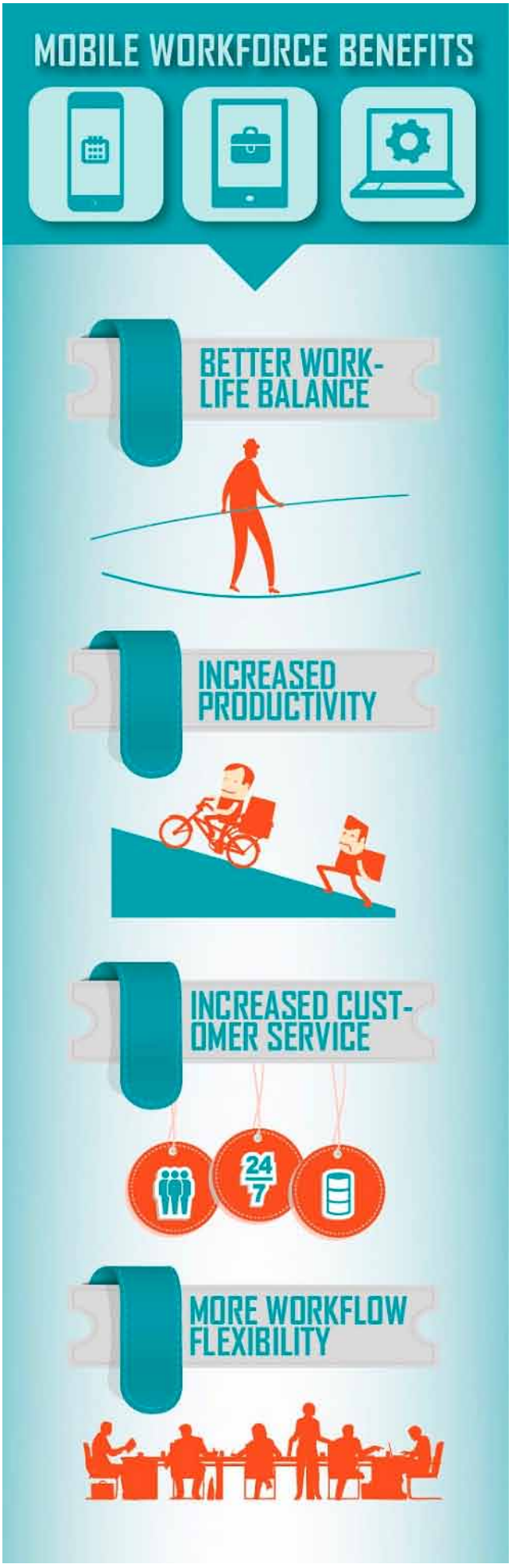
practical, time-saving apps to ensure productivity and efficiency

- Generate work orders, either individually or in batches
- Track and manage parts and inventory, plus ensure vehicles are fully stocked based on scheduled tasks
- Self-scheduling from the field that enables workers on site to request additional time based on their situation
- Manage business and customer data, including assets, warranties, renewals, and contracts
- Real-time chat so that dispatchers, managers, and colleagues can collaborate and communicate

The Benefits of Utilizing Mobile Apps in the

A recent No Jitter article by Melanie Turek, VP of research at Frost & Sullivan, examined the results of a Frost & Sullivan survey that show interest in mobile software applications for employees is strong. From 2013 to 2014, the number of companies deploying at least one mobile worker app rose from 73% to 82%, and 79% plan to deploy additional mobile worker apps during the next year. Why are so many companies jumping into mobile apps for the workforce? Organizations with field staff or employees who are regularly mobile report that mobile apps improve efficiency, profitability, and productivity.

With mobile apps in the workforce, executives can view real-time information relating to each job, plus add jobs and details in real time for workers to view. No longer do organizations rely on paper or spreadsheets to log work, because employees can create and send invoices with evidence and details directly from their mobile devices. Invoices become instant and real time, and everyone can sign digitally, rather than waiting to send and print documents back and forth.



Infographic via HOB Trendtalk

Field workers actually reap the most benefits from mobile apps in the workforce. The portability of mobile devices makes it easier for workers to interact, collaborate, and present, all from one device. With appropriate mobile apps, field workers can access sales and marketing materials from anywhere, any time. Other apps allow the workforce to use a scanner, notebook, calendar, presentation tool, dictator, personal assistant, positioning tracker, performance monitor,, HD video recorder and camera, video editor, and more. With mobile apps for the workforce, organizations turn workers' mobile devices into work tools that go far beyond phone calls and emails.

Challenges with Mobile Apps in the Workforce

People are using mobile apps in all facets of their lives on a daily basis. In an article for Entrepreneur, Sumit Mehra, CTO of Y Media Labs, points out that personal and professional lives have become intertwined and the line between work and home has blurred. As a result, people expect mobile apps for the workforce to be just as well designed and usable as those they use as consumers. Mobile apps for the workforce need to allow for easy data entry, quick access to key functions, and simple navigation for smooth workflows and high productivity. That's why it is so important for mobile apps in the workforce to be designed with a business consumer in mind.

It also is important to recognize that mobile apps cannot exactly match the features of desktop applications, so "good enterprise mobile apps are much more than a migration of desktop enterprise software," according to Mehra. Good enterprise mobile apps should contain the four or five key functions that users typically engage with in business software applications. Additionally, mobile apps should focus on a specific process and include features aligned only to it. Moreover, mobile apps should be easy to navigate and provide users with quick access if they are going to regularly use the app to complete their

work tasks. Finally, mobile apps in the workforce need to employ small typeface, simple graphics, and limited navigational choices so that the graphic interface is tailored to users' needs.

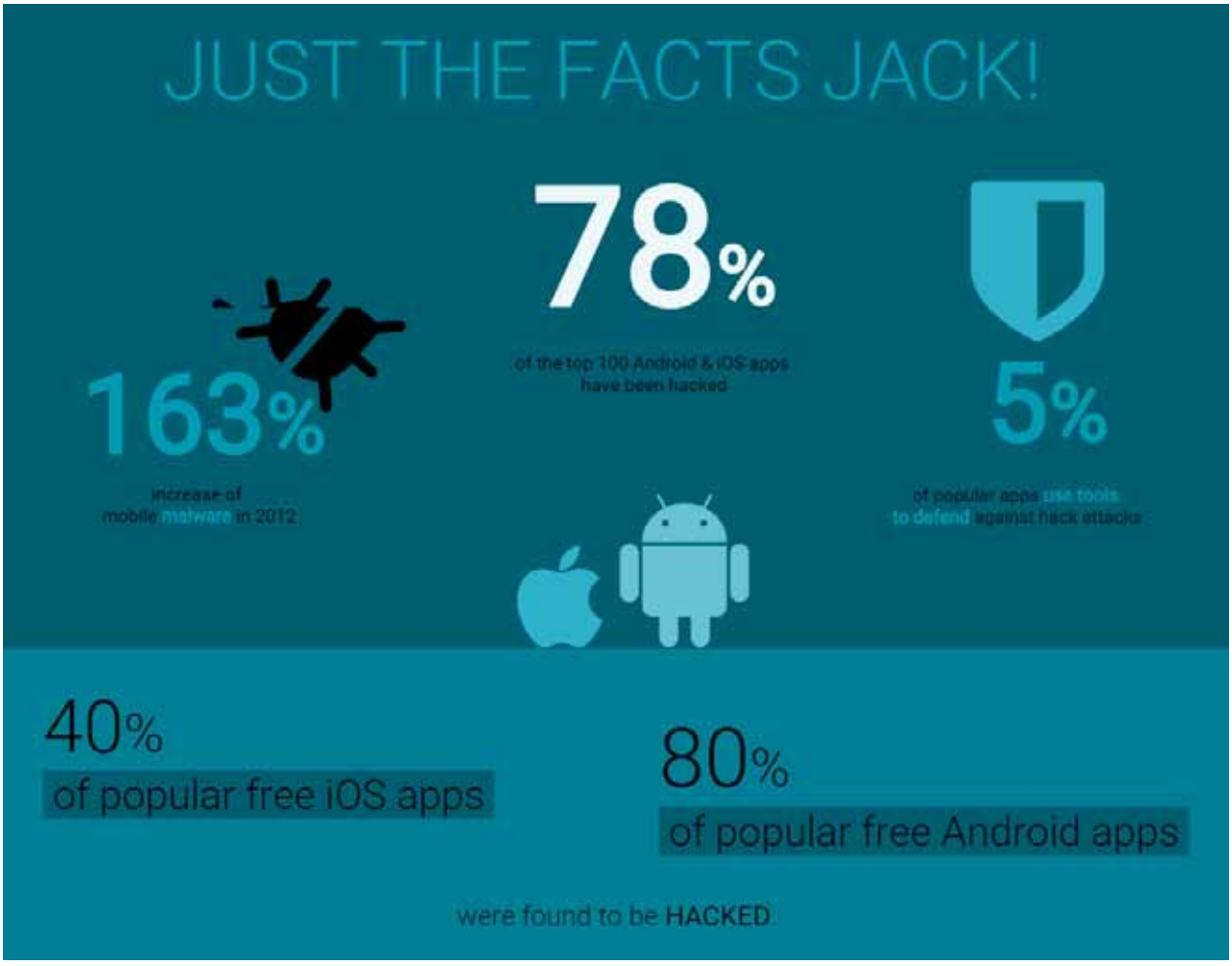
The Need to Secure Mobile Apps in the Workforce

As mobile devices and apps in the workforce become the norm, employees are beginning to use their own devices for work, rather than waiting for company-issued tools to do their jobs. As employees and organizations make use of BYOD programs, organizations are finding that workers are securing those devices "far less adequately than their other important possessions." A 2013 Norton Report from Symantec found that nearly 50% of all smartphone users care enough about their devices to sleep next to them, but they don't protect them. More surprisingly, 48% of smartphone and tablet users don't take basic precautions such as using a device password, let alone installing security software to protect against malicious apps.

As companies utilize mobile apps in the workforce, it is clear that they also must secure their mobile data, in order to protect proprietary information and prevent corporate data from leaking out via apps. The fact that data may be compromised when a device is stolen or when an employee behaves irresponsibly is also troubling for organizations. While the loss may be accidental, sensitive information may be lost via apps without anyone knowing until it is too late, if anyone ever knows at all.

Various forms of security threats exist for mobile apps in the workforce, and they work in a number of ways, including security threats, grayware risks, and performance risks.

- Security Threats – Tracking users, stealing information, infecting devices, reconfiguring devices, piggybacking on accounts, gathering information, compromising two-factor authentication, and leveraging mobile OS vulnerabilities
- Grayware Risks – One of the most pervasive threats in mobile security today, grayware is the area between legitimate software and malware that can be intrusive and aggressive, leak enterprise information, place icons for ads on a device's home screen, change bookmarks, and prompt users to install other apps
- Performance Risks – Many apps cause battery drain or data usage, degrade employee productivity, and drive up mobile data plan costs for enterprises, plus add extra work to IT professionals



Infographic via AutoSend

How to Secure Mobile Apps in the Workforce

Organizations wanting to secure mobile devices against app threats should seek the help of reputable leaders in mobile security. Currently, organizations use a wide variety of technologies and approaches to securing mobile access to enterprise data. In a paper for the SANS Institute InfoSec Reading Room, Jaijumar Vijayan reports that there is support for data protection measures for mobile workers among IT managers, with nearly 32% saying endpoint data protection is of critical importance to managers, and 26% describing it of extremely high importance.

Additionally, the SANS paper shows that organizations reinforce remote access and use of data security in different ways. 25% utilize data loss prevention (DLP) at the endpoints to guard against corporate data loss, while more than 64% require periodic password changes by mobile device users. 57% of respondents have easily accessible security policies and 52% maintain ongoing communications with their workers to reinforce policies around remote access to enterprise data and applications.

Since organizations and IT departments clearly understand the need for mobile app security, they should take steps to secure mobile devices and apps in the workplace. In an eSecurityPlanet article, award-winning technology journalist Paul Rubens offers four steps for securing mobile apps in the workforce. Typically, organizations bring devices under some form of corporate control by investing in a Mobile Device Management (MDM) platform that controls which devices can access specific applications on the network.

An MDM solution can handle device provisioning and configuration, software distribution, encryption and password management, and remote wipe and lock. Essentially, employees can use their personal or corporate-provided devices for business purposes as long as they agree to allow their device to be managed by the MDM solution.

Second, Rubens recommends securing mobile apps in the workforce through policy and training. One way is to impose app download restrictions on mobile devices in the workplace. For example, if a device is used for business, company policy should allow for app downloads only from a corporate app store and not from public app stores. Organizations also should provide user education on mobile apps, so that users understand all of the potential dangers of downloading apps onto their mobile devices. Creating a Mobility User Council with representatives from executives, rank and file, and IT security is a useful step for integrating users into the security process.

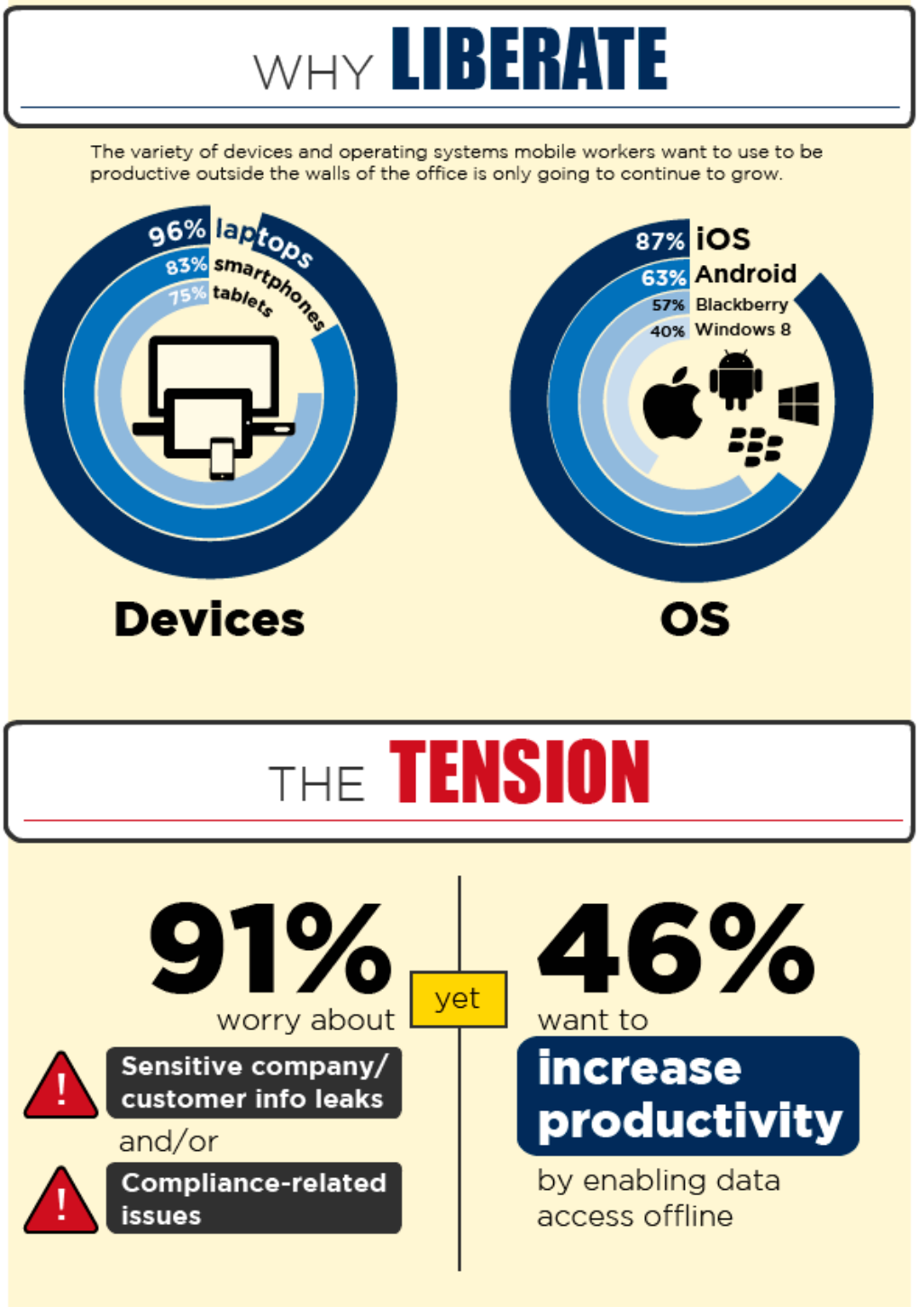
Rubens also recognizes that organizations are beginning to develop and launch their own mobile apps as a means of acquiring, communicating with, and doing business with customers. While these mobile workforce apps “provide an authenticated mechanism for accessing privileged resources such as company databases,” they also pose a risk to organizations: “developers can inadvertently introduce security vulnerabilities when developing custom mobile apps for organizations – often because they are new to the platform, inexperienced with security issues, or unaware of the possible risks.” In fact, the Open Web Application Security Project identifies ten common mobile security development risks and mistakes:

1. Insecure data storage
2. Weak server-side controls
3. Insufficient transport layer protection
4. Client-side injection
5. Poor authorization and authentication
6. Improper session handling
7. Security decisions via untrusted inputs
8. Side channel data leakage
9. Broken cryptography
10. Sensitive information disclosure

Companies seeking to develop their own apps should consider utilizing a mobile security consultancy firm that was not involved in the development process. These consultants have a fresh pair of eyes through which to examine the apps and check for security vulnerabilities.

Finally, Rubens recommends conducting company-wide mobile security audits to examine mobile infrastructure, devices, and apps in order to identify existing weaknesses and determine the organization's next steps. Typical security audit methods include four components:

- Evaluate the organization's overall mobile infrastructure



- Conduct penetration tests on your mobile clients and the servers controlling them
- Assess the security of your mobile devices and apps to determine their susceptibility to data breaches
- Evaluate the gap between current policies and procedures and known best practices

Final Thoughts on Mobile Apps in the Workforce

Certainly, businesses and organizations should embrace mobile apps in the workforce, since the majority of employees already use their own devices for business purposes and mobile app use is proven to increase worker productivity and efficiency. These companies then should determine whether BYOD policies are appropriate, or whether they want to provide company-issued devices to their workforce. Either way, organizations need to manage the risk of mobile apps in the workforce appropriately by minimizing device risks with mobile device management solutions, reducing app risks through policy and training, employing mobile security consultants to minimize the risk associated with developing their own mobile apps, and conducting regular company-wide mobile security audits. The benefits of mobile apps in the workforce far outweigh the risks, as long as companies approach their use in security-minded ways.

ClickSoftware

Making Service Click

About us

ClickSoftware (NasdaqGS: CKSW) is the leading provider of automated mobile workforce management and service optimization solutions for the enterprise, both for mobile and in-house resources. As pioneers of the “service chain optimization” concept, our solutions provide organizations with end-to-end visibility and control of the entire service management chain by optimizing forecasting, planning, shift and task scheduling, mobility, and real-time management of resource and customer communication.

Available via the cloud or on-premise, our products incorporate best business practices and advanced decision-making algorithms to manage service operations more efficiently, in a scalable, integrated manner. Our solutions have become the backbone for many leading organizations worldwide by addressing the fundamental question of job fulfillment: Who does What, for Whom, With what, Where and When.

ClickSoftware is the essential choice for delivering superb business performance to service sector organizations of all sizes. The company is headquartered in the United States and Israel, with offices across Europe, and Asia Pacific. For more information, please visit www.clicksoftware.com. Follow us on Twitter.

Visit us online at: www.clicksoftware.com

☎ Contact us

www.clicksoftware.com

Americas +1 (888) 438-3308 (from US or Canada) or +1 (781) 272-5903 ,+55 (0) 2139580434 (from Brazil)

Western Europe +44 (0) 1628 607000 , **Central and Eastern Europe** +49 (0) 69 489813-0

Asia Pacific +972 3 765-9400 (from Tel Aviv) , +61 (0) 3 9946-6400 (from Melbourne) , +91 124-4947050 (from New Delhi)