What is Driving Next Corporate IT Demand?

Digital work by default.

Teamwork over distance.

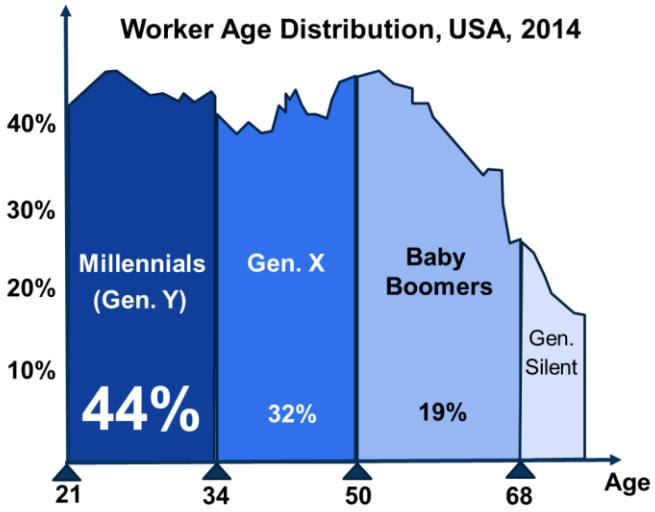
Reverse mentoring as win-win.

Enterprise Culture is Transforming Smart Employee

Digital Lifestyle Translates from Consumer to Corporate

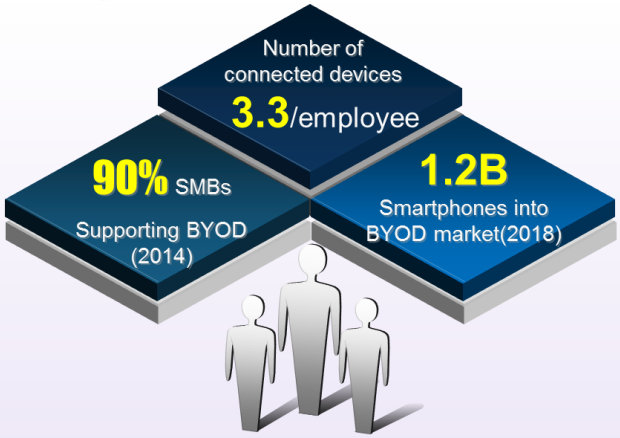
Work Smart & Screen Shift

Today, enterprise customers behave more like consumers and it has became the main driving force behind the demand for increased mobility. The largest cohort of 'On-Demand' worker age is MILLENNIALS, which accounts for 44% in US, are used to get "just in time" information and connection by social platform. The leading examples of employees' requests are BYOD(Bring Your Own Device) and CYOD(Choose Your Own Device). People like using their own devices even for work-related tasks and learning . Therefore the new trends in the corporate world are: shared dialog, shared learning, and reverse mentoring for the goal of bettering both participants in the long haul.



Workplace Evolutions

Growing Trends



The Screen shift from the employer to the employee means transferring the cost of purchasing, maintaining and replacing devices. It is fast becoming standard practice in the corporate world. More companies are allowing employees to utilize their own personal mobile devices to access the network for communication and collaboration, wireless presenting, file download and share and more. Therefore, creating strategic program must be undertaken in a collaborative and concerted effort between an organization's employees, IT team and management.

Source: IEK (2016)

Smart Enterprise Survey

Smart Transformation

Corporate Core Strategies

IT budget shift from CIO to board-level decision makers

Over next five years, DX implementation in enterprises will be more than double.

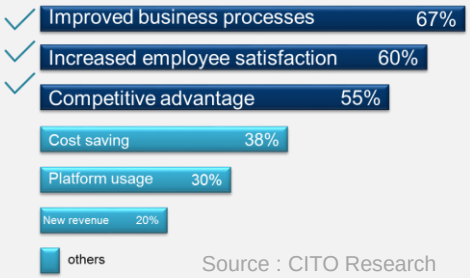
2017y 65% — CEOs of the G2000 enterprises will have digital transformation (DX) at the center of their corporate strategies.

2018y 65% — FT 500 European companies will have deployed full, information-based, economic models or "digital twins" of their products/services, supply networks, sales channels, and operations.

2018y 80% — B2C companies will have created immersive, authentic omni-experiences for customers, partners, and employees. 60% of B2B-centric companies will have done the same.

Source : IDC

Top 3 Needs of Enterprise Mobile Benefits



Source : CITO Research

Relationship | Operations | Info-based

The investment strategy of enterprise mobile are expected to create new value to realize the corporate objectives. User considerations not only for B2C but B2E(business-to-employee) users. Applications in support of business processes and operations as infrastructure assessment to validate its capability of supporting and improve competitive advantage.

UX flows across different devices such as BYOD and CYOD. The enterprise mobility is different from traditional PC's structure, it's critical for communications and the apps are not simply ported cause of the stakeholders are varied and vast. The enterprise IT stack is being fundamentally reshaped and IT budgets of mobility including software, hardware and service are growing from 25% in 2015 to 76% by 2017(IDC).

Mobile & Cloud First

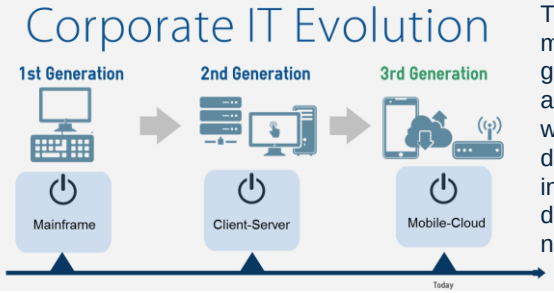
UX with Wireless Connection

Renew mobile use cases and key stakeholders

Re-Define 3rd IT Platform

Content Collaboration for Innovation

Share economic and big data analysis to get deeply insight



The device mesh drive more and more corporate to make faster decision with interconnected data and get deeply insight by 3rd IT platform of big data analysis. The connection models expand quickly with greater cooperative interaction between devices to emerge. Corporate need to identify information to provide strategic value, and access data to leverage Information of Everything to fuel new business designs and innovation.

Source: IEK (2016)

Mobility in the Enterprise

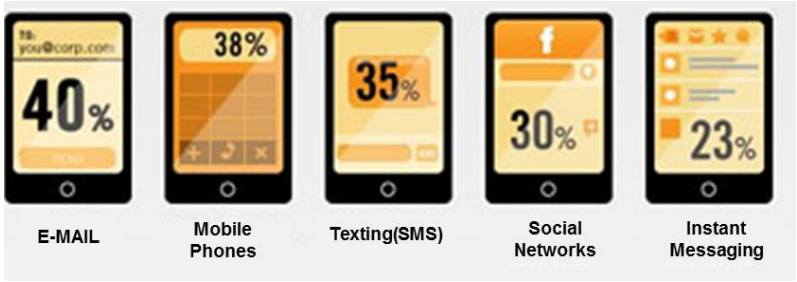
How and Why Business Using Mobile

Today, one in every five phones sold is a smartphone. Both employees and customers are using them, and business are tapping into the devices to connect with them.

Corporate Pickup

Emerging technologies in the workplace

Business are adapting to the changing technological landscape and applying new users to common platforms.

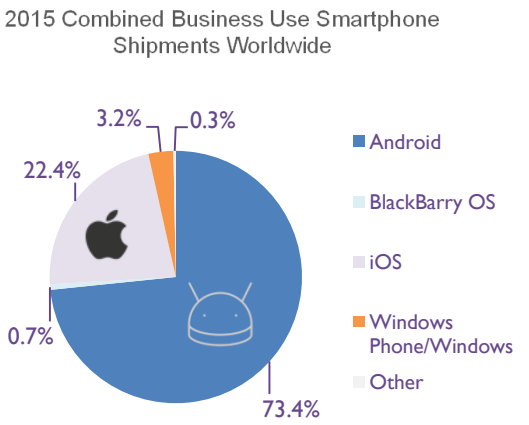


- Mobile workers are increasing globally, and most mobile phones used by working adults will be used for work.
- Organizations continue to struggle with BYOD policies and programs:
  - Corporate liable device programs are in fact here to stay, and CYOD programs are dominant worldwide.
- BYOD is considered attractive by a majority of enterprises, but with caveats:
  - Observed or perceived potential for capex and opex savings.
  - Broadening deployment of enterprise mobility management (EMM) and security solutions to ensure proper management and security of corporate data on individual-liable devices is a substantial undertaking.
- Device OEMs and OS providers integrating enterprise-friendly features:
  - Samsung KNOX, Android for Work, Apple Device Enrollment Program and enterprise applications for iOS, Windows 10 unified OS, cross platform solutions from BlackBerry, enterprise applications for wearables.
  - Ruggedized device manufactures are shepherding enterprise organizations down a path to OS migration.

Combined Business Use by OS

Mobile OS	2015(M)	14/15 % Change
Android	248.5	7.6%
BlackBarry OS	2.2	-26.6%
iOS	75.9	16.8%
Windows Phone/Windows Mobile	10.9	26.5%
Other	1.0	11.2%
Total	338.8	10.0%

Source: IDC (2016)



Source: IEK (2016)

What is Driving BYOD Growth ?

Mobile Devices

- Consumer devices are driving business adoption
- Cost of devices is going down
- Highly competitive market

Mobile Workforce

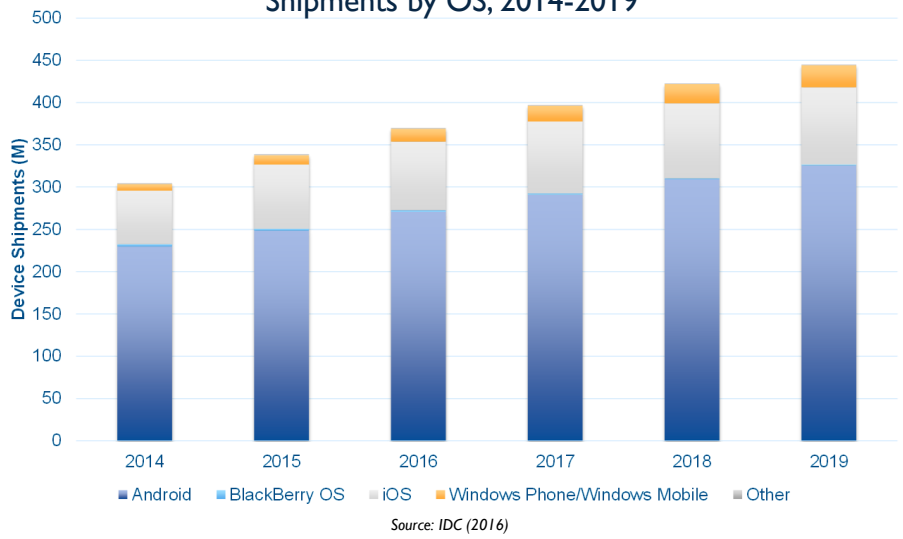
- Mobile workers are increasing
- Mobility is enabling workers to be more productive
- Bringing more devices into the workplace

Solution Providers

- Targeting the enterprise
- Tools to manage mobile strategies and challenges
- Enabling innovation and easy deployment

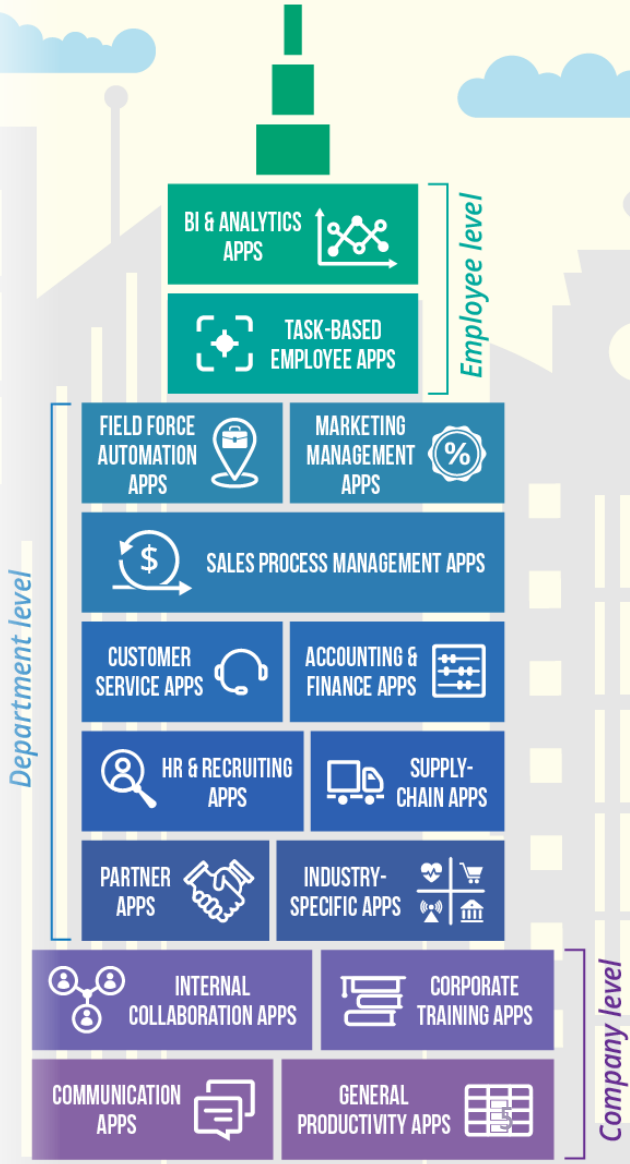
Enterprise Mobility

Worldwide Business Use Smartphone Shipments by OS, 2014-2019



Source: IDC (2016)

MOBILE ENTERPRISE APPLICATION TYPES



Corporate BYOD Infrastructure of Wi-Fi Network

- Mobile devices and app stores have enabled bring your own device (BYOD), BYOA and, more recently, DYOA, which is a form of communication development . BYOA and DYOA have the potential to improve employee productivity and effectiveness or to reduce the development burden faced by the IT organization, but also pose many security and compliance challenges. This research explores the BYOA and DYOA landscape and provide best practices for organizations addressing the current and future challenges of these behaviors.

- BYOA is already common among employees who need to create, capture and share information. Over 90% of employees, who own personal smartphones or tablets, use third-party apps that are not provided by their employer for at least some work-related tasks. BYOA examples include mind mapping tools, cloud file sharing, Gmail, image editing, information management tools such as Evernote, social networking, browsers such as Chrome, messaging tools such as WhatsApp and personal organizers (to name but a few). There are probably tens to hundreds of thousands of apps in the Google and Apple stores that could be useful to an employee. In the longer term, BYOA will take on new forms, for example, asking virtual personal assistants (VPAs) such as Cortana or Google Now for help with business tasks is a form of BYOA and will evolve to DYOA as VPAs gain more access to business data and more process automation capabilities. BYOA will also evolve from apps on traditional devices to apps on wearables and even personal IoT objects.

Corporate BYOD infrastructure of Wi-Fi network

Source: IEK (2016)

Enterprise Organizations Need to Consider

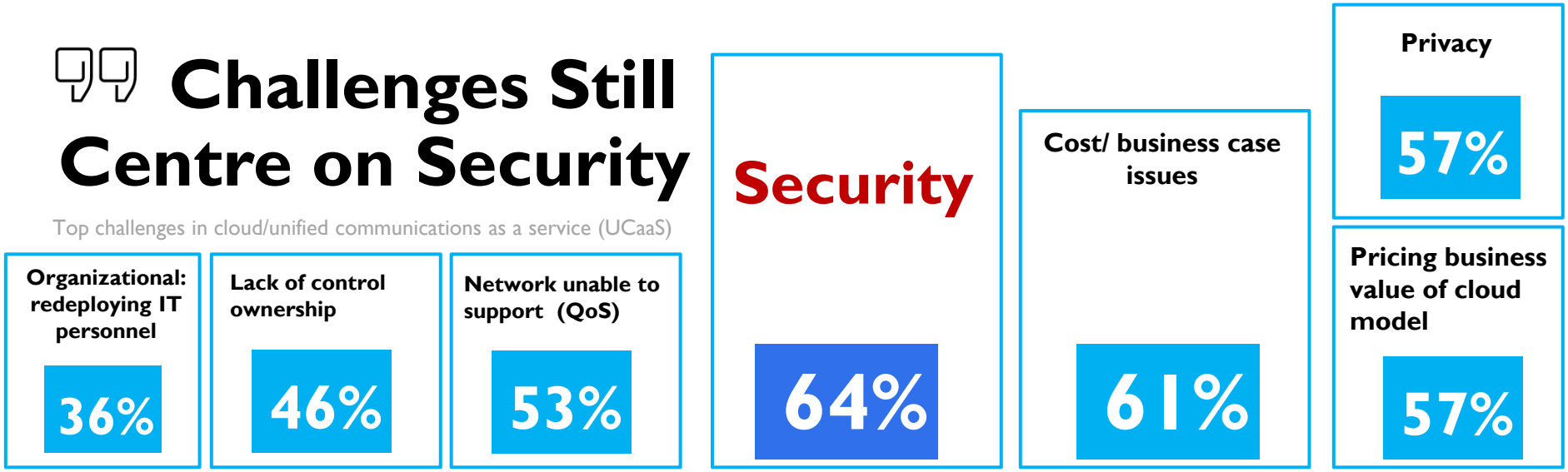
- **Security, eligibility, and compliance**
- **Device and policy management**
- **Life cycle management**
- **Fragmentation**
- **Complexity of the solutions**
- **Legal accountability sand liability**

Security Is the Key for Adopting or Not

- Businesses are adopting UC&C in an effort to increase productivity, control and reduce costs, and encourage collaboration both internally and externally. Current users and UC&C intenders said increasing productivity was the most important factor in their decision to adopt UC&C. But intenders ranked reducing opex (34.%) and faster decision making (30.4%) as key drivers of their decision to deploy UC&C, whereas current UC&C users said improving employee collaboration (41.2%) was more important than reducing opex or faster decision making. Videoconferencing to desktop or mobile devices with or without telepresence (TP) is a key part of many multinational companies' (MNCs) deployment road map.
- Flexibility, reliability, and scalability of solution would be key considerations. Consider adjacencies such as open application programming interfaces (APIs), video analytics, and Web real-time communications (WebRTC) to gain competitive advantages. The rollout of LTE and next-generation networks (NGNs) will create a positive effect in terms of better and cheaper bandwidth.
- Companies continue to migrate part or all of their telephony systems to Videoconferencing and UC&C. Customers are looking more and more at the business value that a communication solution can bring for them, rather than just pure cost and budgeting. VCaaS or hosted solutions would encourage more small and medium-sized enterprise (SME) uptake.

Challenges Still Centre on Security

Top challenges in cloud/unified communications as a service (UCaaS)



Source: IDC (2016)

Source: IEK (2016)

WLAN Security Survey 1

THE Importance OF USING WLAN SECURITY

Just as in wired networks, no one can guarantee a completely secure networking environment that will prevent all penetrations at all times. Security protection is dynamic and ongoing-not static. Network managers and WLAN manufacturers need to keep one step ahead of the hackers. Network managers must also turn on their WLAN security features. Security experts recommend that enterprises deploy several layers of defense across the network to mitigate threats. Additional security components might include firewalls, intrusion detection systems (IDSs), IPS, and virtual LANs (VLANs). Network managers also reduce risk by wisely designing and installing their wireless networks, by implementing proven security measures, and by using products and software developed by experts in network security.

Source: IEK (2016)

InstaShow™, the true plug & play wireless presentation solution, with AES 128-bit security encryption and WPA2 authentication protocol that ensure corporate intellectual property remains private and safe from tempering or unintended disclosure.

WLAN Security Solutions

- **Open Access**

  All Wi-Fi Certified wireless LAN products are shipped in "open-access" mode, with their security features turned off. While open access or no security may be appropriate and acceptable for public hot spots such as coffee shops, college campuses, airports, or other public locations, it is not an option for an enterprise organization. Security needs to be enabled on wireless devices during their installation in enterprise environments. some companies are not turning on their WLAN security features. These companies are exposing their networks to serious risk.

- **SSIDs, WEP, and MAC Address Authentication are Basic Security Option1:**

  Basic security includes the use of Service Set Identifiers (SSIDs), open or shared-key authentication, static WEP keys, and optional Media Access Control (MAC) authentication. This combination offers a rudimentary level of access control and privacy, but each element can be compromised. “SSID” is a common network name for the devices in a WLAN subsystem; it serves to logically segment that subsystem. An SSID prevents access by any client device that does not have the SSID. By default, however, an access point broadcasts its SSID in its beacon. Even if broadcasting of the SSID is turned off, an intruder or hacker can detect the SSID through what is known as “sniffing”-or undetected monitoring of the network. The 802.11 standard, a group of specifications for WLANs created by the IEEE, supports two means of client authentication: open and shared-key authentication. Open authentication involves little more than supplying the correct SSID.

- **WPA or WPA 2 Pre-Shared Key are Basic Option 2:**

  Another form of basic security now available is WPA or WPA2 Pre-Shared Key (PSK). The PSK verifies users via a password, or identifying code, (also called a passphrase)

  on both the client station and the access point. A client may only gain access to the network if the client's password matches the access point's password. The PSK also provides keying material that TKIP or AES use to generate an encryption key for each packet of transmitted data. While more secure than static WEP, PSK is similar to static WEP in that the PSK is stored on the client station and can be compromised if the client station is lost or stolen.

	WPA	WPA2
Enterprise Mode (Business, Government, Education)	• Authentication: IEEE 802.1X/EAP • Encryption: TKIP/MIC	• Authentication: IEEE 802.1X/EAP • Encryption: AES-CCMP
Personal Mode (SOHO, Home/Personal)	• Authentication: PSK • Encryption: TKIP/MIC	• Authentication: PSK • Encryption: AES-CCMP

IEEE 802.1X Authentication and the Extensible Authentication Protocol

Source: IEK (2016)