Leadership and technology: Mobility and bring-your-own-device insights for midmarket enterprises
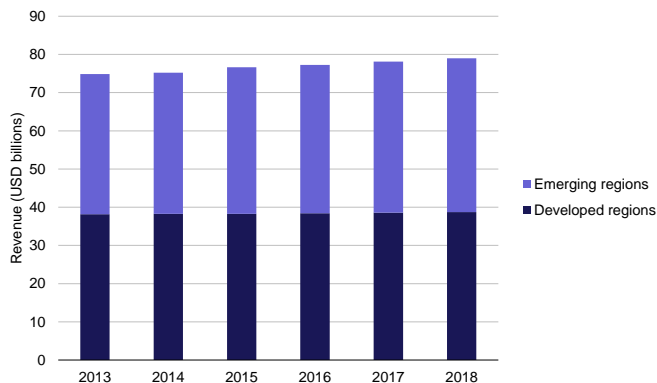## Sponsored by Cisco Systems, Inc -- July 2013

Executive Summary

Midmarket enterprises strive for success in a highly competitive landscape. Being a successful leader means encouraging employees to collaborate and work more efficiently to increase the success of the enterprise. Technology solutions can empower employees for success at work, home, and when mobile, but technology must also be able to support changes that occur in a business without increasing the risks associated with providing excellent customer service, fostering innovation, and engaging with an enterprise's stakeholders.

This white paper looks at the power of mobility as part of the midmarket enterprise's unified communications (UC) platform and the seemingly competing interests of IT departments and other functional areas that often place stress on an organization. Enterprise mobility—much of which is promoted by employees bringing their consumer, personal, mobile devices into the work environment—continues to grow worldwide. These trends associated with the bring-your-own-device (BYOD) concept are putting pressure on IT departments to support all personal mobile devices in all types of work spaces.

To meet their BYOD needs, midmarket enterprises will need to consider implementing unified communications infrastructure that enables full mobility suites including centralized network and device management capabilities. These solutions address both IT and business considerations that arise when enterprises contemplate implementing a BYOD policy. By meeting IT and business needs, these types of unified communications platforms better prepare enterprises to realize the full benefits that mobility can produce.

Analysys Mason forecasts that revenue from mobility—including voice, data, and management services—for midmarket enterprises will grow from US$74.8 billion in 2013 to US$79.0 billion in 2018 (refer to Figure 1).[1]

Figure 1 Revenue from Mobility Services, Worldwide [Source: Analysys Mason, 2013]

---

[1]   In these revenue figures, Analysys Mason includes all mobile voice and data services from the use of smartphones, feature phones, mobile broadband dongles, and mobile device management services for businesses with 100 to 999 employees worldwide. Although the totality of this revenue is not fully attributable to unified communications solutions, the relative size and growth are indicative of the tremendous importance of mobile solutions across the world.

Recommendations for Midmarket Enterprises

When contemplating the purchase of a unified communications platform to support a BYOD strategy, midmarket enterprises must consider a range of factors, such as policy management, existing and future business needs, as well as partner implementation expertise. There are 5 key focus areas to consider:

- Match mobility solutions to various employee work spaces and functional areas to increase their productivity: In order to maximize the investment return from mobility solutions, it is important to understand employees' work-space patterns. A more thorough understanding of these work spaces—for example, in the office, at home, and when mobile—and employees' usage patterns will allow midmarket enterprises to select and deploy the proper mobility tools and the correct management tools for their IT departments. In addition, it is important to consider employees' functional areas when choosing mobility solutions, because requirements can differ by functional area even if the work-space requirements are the same. For example, the requirements of mobile sales people could be different from those of finance department employees.

- Select a vendor who understands work-space needs of its employees: The best vendors of unified communications platforms provide a broad selection of mobility and mobility management solutions. Many enterprises mix various types of mobility solutions to best serve the needs of their employees, partners, and customers. Enterprises that make mobility available anytime, anywhere, and on any mobile device will find much higher adoption of this business technology than less-flexible enterprises. This flexibility will pay off with increased collaboration between employees and more personal interaction between employees and customers.

- Look for an industry-leading unified communications solution that addresses the holistic needs of mobility management: IT departments need tools to manage more than just endpoint mobile devices. For example, many enterprises underestimate the impact that mobility can have on their networks. Proper policy management, mobile security management, integration of mobile and fixed access, and management of collaboration-related software clients on mobile devices are all critically important aspects of mobility management. Although mobile device management is an important aspect of a solution, enterprises must choose solutions that consider a more comprehensive mobile management capability or risk network degradation, increased IT services costs, and employee dissatisfaction.

- The best unified communications platform vendors have self-onboarding capabilities associated with their mobility solutions: BYOD trends and device proliferation are placing large demands on IT departments. According to a recent survey by Analysys Mason, approximately 49 percent of midmarket enterprise employee respondents use their personal devices for work. Expecting IT staff to onboard every new mobile device—smartphone, tablet, and laptop—supplied by employees is unrealistic, given constraints in IT staffing budgets. However, self-onboarding tools allow employees simply to provision their own devices for the work environment while maintaining all proper IT and security policies.

- Pick a vendor that has excellent professional services skills and experience in mobility-related unified communications solutions: Professional services and project management skills matter. Vendor that have the required skill sets and certifications in collaboration technologies will minimize implementation risks and provide better overall support for an enterprise's mobility management needs.

BYOD Trends and Framework for a Midmarket IT Department

BYOD refers to the use of personal mobile devices by employees for work-related purposes. These devices can include feature phones, smartphones, tablets, laptops, netbooks, and other personal mobile devices connected or connectable over wireless or mobile networks. The devices may or may not have access to corporate applications or data, but do have access to personal applications and data.

Increasing numbers of employees want to use their own mobile devices in the workplace. According to Analysys Mason's *Connected Consumer Survey*—a multiyear, multinational study that tracks and measures consumers' changing telecom and media habits, device ownership, connectivity options, and future plans—approximately 49 percent of midmarket enterprise employee respondents use their personal devices for work. This surprisingly large percentage of respondents highlights the trends we have seen in the BYOD trend over the past several years. When given the option, employees would prefer to use their personal mobile devices rather than having to carry separate personal and work-issued devices.

Midmarket IT departments need to address four areas as they develop a BYOD strategy in response to the challenges presented by employees using their own devices (refer to Figure 2). The largest enterprises will invariably have to address all four technology topics now, whereas smaller enterprises might be able to address them over the next few years. However, all enterprises—large and small—will eventually have to consider and adopt some of the elements of this framework because of the near ubiquity of mobile technology and its continued influence in our personal and business lives.

Figure 2 Elements of a BYOD Technology Framework [Source: Analysys Mason, 2013]

Implementation	Application enablement	Management	Security
Device policy	Custom application development	Centralized policy management – network, security, connectivity	Network security
Network enablement and policy	Mobile application customization and configuration	Device, OS, application management	Device and application authentication
Device logistics	Integration	Telecom expense management	Data back-up and loss prevention
Device self onboarding	Data synchronization		Remote lock and wipe
Office space design			Secure connectivity
			Malware protection
			Partitioning

Implementation refers to the execution of a BYOD strategy in the enterprise. There are various aspects of implementation, including the creation of effective, simple-to-understand BYOD policies to establish appropriate device usage; an enterprise network capable of supporting the additional demands of mobility solutions; connectivity enablement and related policies; device logistics to adequately ship and track new or replacement devices; and the ability to self-onboard and provision appropriate business credentials on a mobile device to begin service. Midmarket enterprises should also encourage liaison between IT and other functional areas to help explain the BYOD policies and implementation. Finally, in order to take advantage of additional employee collaboration after implementation of a BYOD policy, midmarket enterprises should rethink the

design of their office spaces. It is important to create new work spaces so employees are encouraged to collaborate in new ways with each other.[2]

Applications enablement refers to the creation and mobilization of business tools and applications on personal devices. It includes the development of custom applications as needed; customization or configuration of existing applications for the mobile environment; integration of various business and personal applications; data synchronization across applications; and allocation of business applications to appropriate employees. An effective BYOD strategy takes advantage of mobile applications, but needs tools and a variety of IT services to enable these applications effectively on myriad mobile devices.

Management refers to the activities and solutions to provide ongoing supervision and administration of the midmarket enterprise network and the mobile devices employees use. IT departments require centralized policy management tools to provide administration of the network, connectivity, and security policies associated with a BYOD program. Centralized dashboards and management consoles allow IT departments to manage all aspects of a BYOD strategy more effectively. IT departments also need tools to deal with the tremendous proliferation of mobile devices, and must grapple with hardware, operating systems, and applications. These device management tools allow the IT department to keep current with patches, firmware, and software releases. Finally, IT departments require expense management tools to aid cost minimization for various telecom voice and data services.

Security refers to the protection of network connectivity and applications, as well as the mobile devices employees use, from unauthorized access. A midmarket enterprise IT department must revisit its overall security position when it adopts a proactive BYOD policy. Security includes overall network security; device and application authentication with single password sign-on;[3] data backup and loss prevention; remote locking and data deletion from lost devices; secure connectivity; malware protection; and partitioning of devices for business and personal use.

Collaboration and Mobile Work Spaces: A New Paradigm

The adoption of a BYOD program affords benefits to a midmarket enterprise. When midmarket enterprises implement BYOD policies, they see increased collaboration between employees, partners, and customers. These benefits come from added opportunities for innovation and collaboration, productivity savings, and increases in customer and employee satisfaction. As such, it is critical to rethink the value of collaboration in common work spaces for BYOD-equipped employees. Consider three mobile work spaces:

- Office: Employees use personal devices in the office to enhance work productivity, provide better customer support, and fuel innovation. Employees use these personal devices at their desks, in conference rooms, on factory floors, and in collaborative settings with other employees.

- Home: Employees often work at home or complete specific work-related tasks at home. In addition, employees often work at home to extend the working day while also meeting their personal commitments. This work space is, in some ways, fairly similar to the office work space, because the employee's

---

2   Five ways IT can help employees use new technology, CITEworld, by Ron Miller, April 24, 2013, http://www.citeworld.com/mobile/21769/five-changes-IT-should-make-right-now.
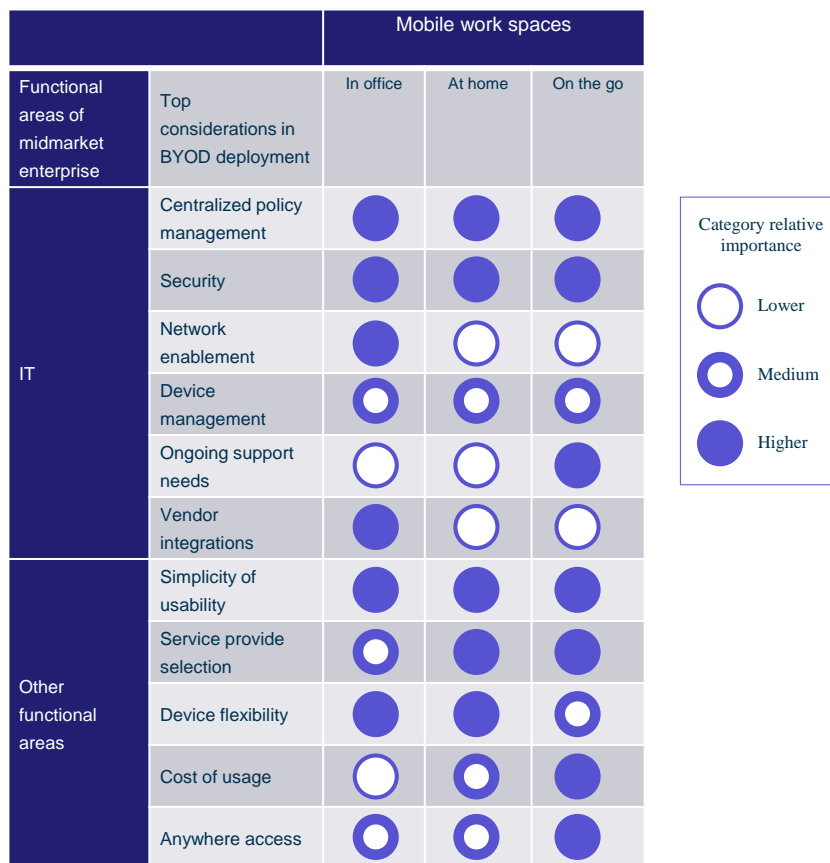
3   Ibid.

environment is more controlled and limited in geographic scope. However, it differs in terms of the network expectations and quality of connectivity, which have varying quality-of-service (QoS) metrics.

- Mobile: Employees use personal devices while traveling between two geographic points. They have less control over work-space characteristics in these circumstances, and often work with highly variable network quality. There are also unique security-related concerns in this work space, including heightened risk of device theft and unauthorized access to data. This work space can include commuting time in a car, train, or bus; working in an airplane; working while walking down the street; and many other activities.

Midmarket enterprise IT departments and other functional areas within the company have several key imperatives when considering the adoption of a BYOD and mobile collaboration policy in these three work spaces (at home, in the office, and when mobile). Figure 3 illustrates some considerations a business should have for a BYOD deployment in three mobile work spaces.

Figure 3 Top IT and Other Functional Area Considerations for BYOD Deployment in Three Mobile Work Spaces [Source: Analysys Mason, 2013]

Functional areas of midmarket enterprise	Top considerations in BYOD deployment	Mobile work spaces		
		In office	At home	On the go
IT	Centralized policy management	Higher	Higher	Higher
	Security	Higher	Higher	Higher
	Network enablement	Higher	Lower	Lower
	Device management	Medium	Medium	Medium
	Ongoing support needs	Lower	Lower	Higher
	Vendor integrations	Higher	Lower	Lower
Other functional areas	Simplicity of usability	Higher	Higher	Higher
	Service provide selection	Medium	Higher	Higher
	Device flexibility	Higher	Higher	Medium
	Cost of usage	Lower	Medium	Higher
	Anywhere access	Medium	Medium	Higher

Category relative importance: Lower, Medium, Higher

IT Considerations of BYOD Deployments

Of paramount interest to IT organizations—and the top IT consideration in all mobile-equipped work spaces—is the adoption of a centralized policy management solution and security posture to support BYOD deployments. One of the most pressing concerns an IT department when implementing a BYOD program is to manage the deployment and protect company assets effectively. Centralized policy management encompassing everything from the network to the device is critically important.

Other top IT considerations for deployment of a BYOD solution vary by work space. For example, in the office, IT departments must provide a network capable of handling the changes caused by mobile devices, so network management is very important. Failure to prepare the network environment for increases in mobility and BYOD work spaces can greatly impinge on the quality of the network. Employees are likely to use mobile devices in different places in the office than traditional PCs and laptops; for example, it is becoming more common to have groups of employees in conference rooms collaborating on tablets, or working outside in the courtyard of a building. We also believe that employees will start using video collaboration more on mobile devices while in the office. IT must have the tools to measure, monitor, and optimize the network to handle these changes in usage characteristics.

Midmarket enterprises often do not have large or technically specialized IT staff; therefore, IT departments must consider the ongoing support needs associated with a BYOD solution. The lack of IT staff also raises the challenge of having to support multiple vendors' mobility solutions in the workplace. For this reason, some IT departments strongly favor a single-vendor solution. Either way, these support requirements can greatly hamper an IT organization's ability to deliver a cost-effective and simple mobility strategy.

Other Functional Area Considerations of BYOD Deployments

The most important business consideration for a BYOD policy is simplicity of use. The increase in BYOD work spaces is promoted primarily by employees desiring device familiarity and simplicity in all their work spaces. It is important that the implementation of a BYOD policy does not significantly increase complexity and discourage employees from using personal mobile devices.

Other top business considerations in the deployment of a BYOD policy vary by work space. Employees often have preferences for mobile service providers. As such, selection of service providers often plays a large role in the implementation of mobility and BYOD solutions, especially in home-based or mobile solutions. In the office and at home, device flexibility is an important consideration. In relatively geographically confined environments like these, employees want the flexibility to choose between devices to perform their work. Although device flexibility is also important when employees are mobile, we believe that employees recognize that certain devices are less effective in certain work spaces. For example, while driving a car, it is inadvisable or illegal to send text messages and, in some locations, talk, on a mobile phone. Or, while standing on a very crowded train or other public facility, it is inadvisable to type on a tablet device. However, it is quite important for the enterprise to control the usage costs of mobile devices and to provide access to applications anywhere the employee is traveling or using a mobile device.

Mobility embedded into an all-in-one unified communications platform can allow midmarket enterprises to start capturing the benefits of increased collaboration and work-space flexibility. Midmarket enterprises adopt technology that is easy-to-use and, although many older mobility solutions have proven themselves complex, costly, and cumbersome to manage, new solutions from the best vendors remove these problems.

Midmarket enterprises must recognize and be prepared for the future of mobility and the BYOD trend—a future where simplicity, flexibility, and access anywhere for end users, and a centralized policy management and security for IT departments, are critically important. Even midmarket enterprises not using mobility today will be using it in 2 to 3 years' time and are preparing to support it. It is critical to purchase technology equipment and unified communications platforms that address these types of IT and business considerations, while providing overall investment protection for your company.

Growth of Mobility

Mobility provides new ways for midmarket enterprises to differentiate their businesses; it provides innovative ways for stakeholders—employees, partners, and customers—to interact; and it allows employees to maintain contact with customers on a more timely and convenient basis, increasing customer satisfaction. Mobility makes businesses more productive.

Following are three examples—organized by mobile work space—where mobility allows midmarket enterprises to increase productivity and employees to stay connected in innovative ways.

- Mobile example: A field technician at a midmarket enterprise has driven 60 miles (100 kilometers) to make repairs on a piece of a customer's equipment. He encounters what looks like a problem in some component of the equipment. He does not want to attempt to fix the problem, because he has not encountered this change in the past. Instead of requesting another technician to be dispatched to the worksite, he uses his smartphone and video-based communications to engage a component specialist in the office at his company. By being able to see the component, the specialist diagnoses the problem and the field technician is able to make the required repairs to the equipment.

- At-home example: A chief financial officer (CFO) of a midmarket enterprise spends the day flying home from a remote office location. He needs to have a collaboration session with his team late in the evening, because it is time to close the books for the month and there is a problem with some key accounts. Instead of having to go to the office to speak with his team and review financial records, he can connect remotely with his team and his company's finance and accounting application with his tablet from home, using collaboration software and a secured connection. The CFO and his team work together for an hour, determine the cause of the problem, and close the monthly books on time.

- In-office example: An innovative, online advertising agency has a new customer, a large pharmaceutical company. Employees in the creative department have an assignment to devise a design for their client's not-yet-marketed allergy medication. In order to encourage new thoughts and creative ideas, the employees decide to have their first brainstorming session outside in the courtyard of their office building. While sitting on the lawn, they each use their tablets to log into their company's collaboration platform and together sketch images for an upcoming team meeting. The sketches allow the advertising agency to put together a novel campaign for their client.

Conclusion

Leadership matters. Technology allows midmarket enterprises to empower their employees and better service their customers. The technology chosen must support future business needs while empowering IT to manage and protect the enterprise's technology environment; otherwise, the technology represents an additional financial risk to the firm. Vendors that supply mobility and BYOD solutions integrated within a unified communications infrastructure are well prepared to meet the needs of midmarket enterprise technology and business challenges. These types of vendors are best positioned to address the growing needs of midmarket enterprises.

IT departments and other functional areas face numerous considerations when choosing to implement a BYOD policy. And these considerations affect BYOD decisions for all of an employee's work spaces. The key IT considerations—centralized policy management, security, network enablement, ongoing technical support, device management, and vendor integrations—necessitate technology solutions that provide robust yet simple-

to-use centralized dashboards and management consoles. The key business considerations for other functional areas—simplicity of use, service provider selection, device flexibility, cost of usage, and access from anywhere—need to be addressed so that employees will fully use mobility tools in new ways, fostering increased innovation and productivity.

Mobility solutions supporting a BYOD policy help turn an IT department from a cost center into a catalyst for business change. Mobility solutions—devices, operating systems, applications, and management tools—continue to evolve. Vendors that supply mobility solutions integrated with unified communications platforms are well prepared to meet the needs of midmarket enterprise technology and business challenges.