APRIL 2016 MARKET REPORT

ENTERPRISE
MOBILITY
EXCHANGE

Market Report: Overcoming the Top Five Barriers to Becoming a Mobile-First Enterprise

In association with:

AT&T MobileIron MOBILE LABS NETMOTION WIRELESS tangoe

WWW.ENTERPRISEMOBILITYEXCHANGE.COM

About the Author

Mark Bowker,
ESG Senior Analyst

Mark Bowker is a senior analyst responsible for the enterprise mobility coverage at ESG. Leveraging 20+ years of IT industry experience, Mark researches what it takes to support today's workforce as seen through both IT and end user lenses.

Fascinated by the transformation in workforce behaviour brought about by mobility, and how businesses are embracing mobility-enabled workflows and processes, Mark's research spans alternative desktop, application, and data delivery strategies to enterprise mobility management technology, mobility's impact on IT and business, and the broader IT vendor marketplace.

Leah Matuson,
Research Analyst

Leah Matuson is a Research Analyst at The Enterprise Strategy Group (ESG) primarily focusing on enterprise mobility, cloud computing, and virtualisation. Leah leverages more than twenty years of experience as a writer, editor, and journalist in the technology sector, creating clear, compelling content for the web and print media, including articles, white papers, case studies, and technical and marketing literature.

Contents

Introduction

Today, business is being transacted around the clock, from anywhere, and on a wide variety of devices. A burgeoning mobile workforce and enhanced business processes ignited by mobile applications are calling for more flexibility in how, when, and where employees can work (and with whom), as well as pushing for easy and secure access to the information and applications they need to be more productive and do their jobs more efficiently.

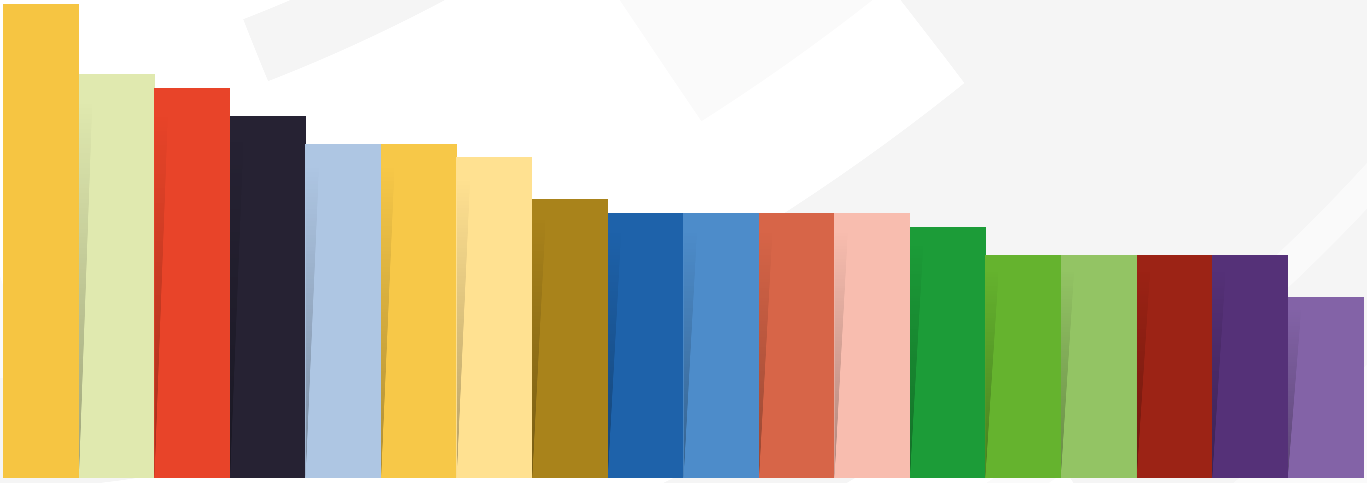
But while businesses are embracing more flexibility in work styles, IT has the unenviable task of delivering on a variety of security, threat detection, network, file protection, and user productivity challenges. IT must not only secure business-critical data and endpoint devices (both corporate-owned and personal), but also meet compliance, and provide an enhanced user experience (think improved security, access, collaboration, and communication)—all the while working with siloed platforms, inadequate solutions, and legacy applications.

What's Influencing Enterprise Mobility?

Regardless of the challenges, more and more enterprises are embracing mobility. To gauge this development, ESG recently surveyed IT professionals in enterprise and midmarket organisations to find out what has had the greatest influence on shaping their organisation's enterprise mobility strategy. According to ESG research, 34% of IT organisations reported that proactive threat detection has the greatest influence on their organisation's mobility strategy, followed by 29% who cited improvement of employee productivity via mobile enablement. In addition, 28% reported that improvement of communication and collaboration between employees as the greatest influence on shaping their organisation's enterprise mobility strategy (see Figure 1).

Figure 1.
Factors Influencing Enterprise Mobility Strategy

Which of the following have had the greatest influence on shaping your organisation's enterprise mobility strategy?



■	Proactive threat detection	34%
■	Improvement of employee productivity via mobile enablement	29%
■	Improvement of communication and collaboration between employees	28%
■	Improved/enhanced security for corporate applications and endpoint devices	26%
■	Compliance and auditing requirements	24%
■	Change in office productivity application consumption model	24%
■	Windows OS upgrade	23%
■	Bring-your-own-device policy	20%
■	Flexwork/telework initiative	19%
■	Improvement of login experience	19%
■	Support for Microsoft Windows on Apple devices	19%
■	Simplified means of managing desktop, apps and data for contractor/ temporary employees	19%
■	Hardware refresh	18%
■	Business executives request	16%
■	Enablement of a net-new business initiative	16%
■	Initiative to create new customer experiences using the latest mobile technologies	16%
■	Corporate endpoint device rollout	16%
■	Pressure from employees and/or business units	13%

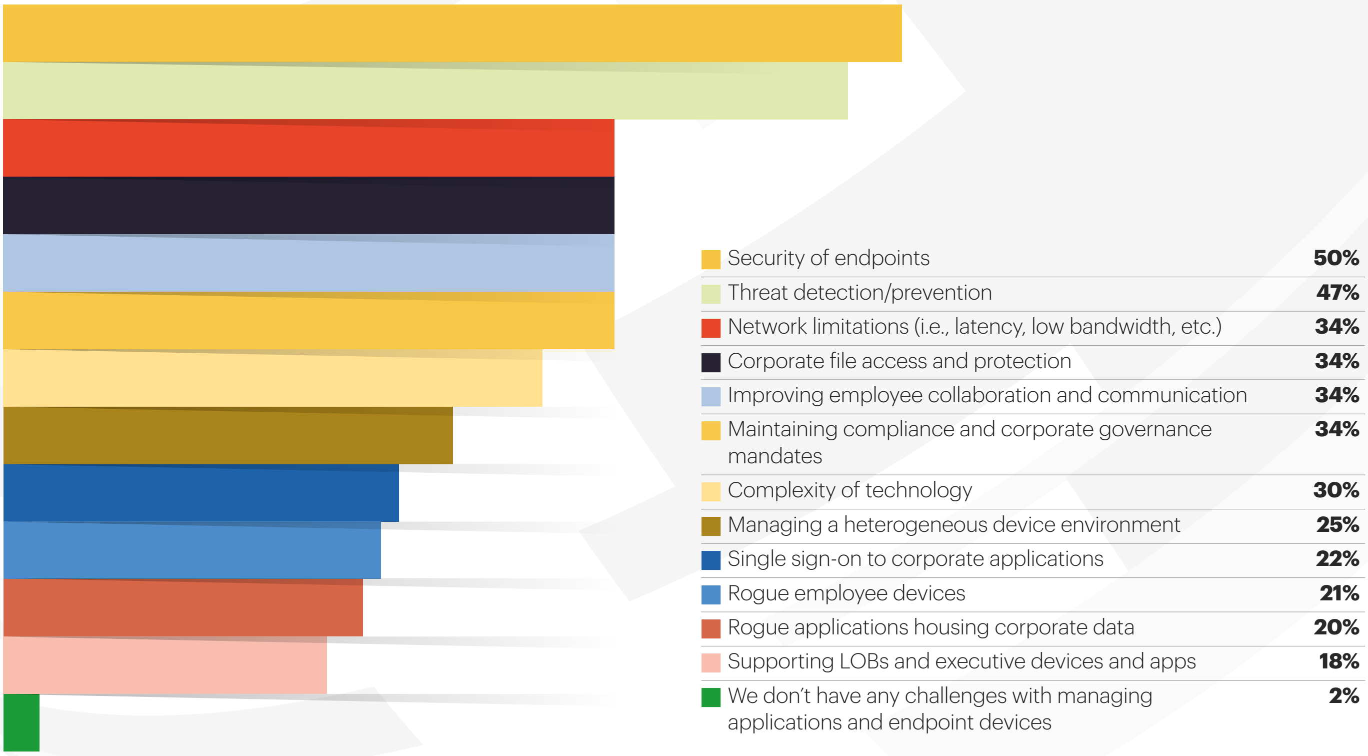
Top Five Barriers to Becoming a Mobile-first Enterprise

So, what's the issue? What's stopping organisations from being able to provide workers with the tools they need to be more productive, in a secure environment, while also giving them an enhanced user experience? The fact is that organisations across the board are facing a number of barriers that are preventing them from becoming a mobile-first enterprise.

According to recent ESG research, 50% of all IT professionals stated that security of endpoints is the greatest challenge their organisation is facing with regards to managing the applications and endpoints employees use to perform their daily job functions, while 47% answered that threat detection/ prevention as their greatest challenge. Furthermore, 34% of those surveyed indicated that network limitations, and corporate file access and protection were among their greatest challenges, with 30% pointing to complexity of technology (see Figure 2).

Figure 2.
Challenges Encountered When Managing Applications and Endpoint Devices

What are the greatest challenges your organisation faces when it comes managing the applications and endpoint devices your employees use to perform their daily job functions?



A closer look at those top five most-cited barriers reveals a complicated situation for IT:

- **Security of endpoints, threat detection, and compliance.** Security perimeters evaporate as mobility initiatives pour into organisations. This leads to significant challenges when it comes to protecting corporate-owned and personal endpoint devices (think laptops, smartphones, Androids, PCs, Macs, tablets, etc.). And if employees can't get at their information quickly, they could easily download applications directly from the web (risking inadvertently downloading malware or viruses, or accidentally disclosing sensitive information), making it that much more difficult to prevent costly security breaches, while also having to grapple with meeting regulatory compliance.

- **Network limitations.** With many enterprises using legacy and siloed solutions, applications, and systems (on-premises, in the cloud, and hybrid), a less-than-cohesive infrastructure makes it difficult for IT to deploy mobile applications with a high degree of certainty that they will work as they're supposed to. Having employees easily access and actually use those applications is another matter.

- **Corporate file access and protection.** Employees want to easily access corporate applications and information, anytime, anywhere, from both corporate-owned and personal devices. If that access isn't forthcoming, workers may opt for alternate ways to access that information—such as downloading apps from the web, and using unsecured networks or systems.

- **Unified communication and collaboration (UCC).** Communication and collaboration are the hallmarks of enterprise business today. Without simple-to-use tools and access to secure file sharing programs, workers often feel compelled to find their own methods—using unsecured applications or networks, often at the expense of corporate security.

- **Complexity of technology.** IT organisations are faced with a surplus of technology choices to help overcome mobility challenges, and embrace mobile-first initiatives. Since any technology decision can have a massive impact on user satisfaction and productivity, businesses have a challenging task ahead of them: culling through a variety of technologies, and understanding how they integrate with one another

Becoming a Mobile-First Enterprise

Regardless of the many challenges encountered on the way to becoming a mobile-first enterprise, there are clearly champions within organisations ensuring mobility initiatives continue to move forward. So who is leading the charge? Based on ESG research, CEOs and senior business managers are taking the lead in influencing mobility strategies, while IT is ensuring that core application and critical business processes are aligned.

What are these champions actually doing to address these challenges—from security and network limitations, through ensuring file access and unified communication and collaboration, to deciphering the complexity of technology?

Security of endpoints, threat detection, and compliance. Organisations need to address the risks associated with mobile endpoints as they shape their mobility strategies around proactive threat detection. Proactive threat detection is designed to provide information about threat factors, malware, and indicators of compromise (IoCs)—such as malicious IP addresses, files, and URLs.

It's critical for Chief Information Security Officers (CISOs) to use this intelligence to reinforce security controls (i.e., firewalls, web threat gateways, endpoint security, etc.) for heightened threat prevention, including risk analysis and assessments, password protection, two-factor authentication, encryption of data at rest or in-flight, and remote wipe. Creating and implementing comprehensive BYOD policies, and calling on experienced IT professionals to lead these initiatives, is also just as important.

For a risk management program to be effective throughout an organisation, IT must use best practices in a number of areas, in various ways, including:

- **Performing risk management metrics.** Present clear risk management metrics to executive management. Avoid using technical details, and tailor reports toward business risks such as: cost of a data breach, lost revenue, share price declines, litigation, and loss of reputation.

- **Standardising AV vendors.** Assess current AV products and practices. Consider standardising on one AV vendor across the company. Look to move beyond AV and deploy additional layers of advanced malware software and endpoint forensics tools.

- **Evaluating endpoint visibility, access, and security (EVAS).** Evaluate EVAS to attain the right level of continuous monitoring for endpoint profiling. EVAS tools can be used to monitor and manage all devices connected to the network (e.g., PCs, servers, mobile devices, IoT, etc.). A number of organisations are also integrating EVAS data with other security technologies (e.g., SIEM, threat management, MDM, etc.) to enhance threat intelligence and security analytics with endpoint profiling and security information.

Network limitations. Employees are accessing applications and data from a variety of locations including internal wired and wireless networks, remote Wi-Fi hotspots, and cellular data networks. While these networks can be a valuable means of access, they are also complicated by potential security vectors, as well as bandwidth and latency.

- **Incorporating network access control (NAC).** NAC should be part of an overall endpoint security strategy. Organisations are now embracing NAC to enforce granular access controls based upon corporate governance or compliance requirements. Leading NAC solutions can also be used to enforce network access controls for mobile and other types of non-PC devices. NAC can help organisations decrease the endpoint security, as well as the overall cybersecurity, attack surface.

- **Restricting access with micro-segmentation.** Business managers may want to restrict or limit access to sensitive data depending upon attributes such as a user's role, device type, and where the user is located (e.g., physical location, network location, etc.). CISOs may also want to monitor device and user activities to spot anomalous behaviour. Generally, organisations should embrace solutions that can create policies and secure connections between the mobile application and the business application, and, ideally, the data associated with the application.

- **Securing the Wi-Fi infrastructure.** Secure, reliable, and scalable Wi-Fi is required to meet the sheer number of endpoint devices and bandwidth requirements. Rudimentary requirements that enable an employee to roam between access points (AP) should be part of a critical system, which should also offer employees self-service access for untrusted guest devices, monitoring software, and integration with enterprise mobility management (EMM) solutions.

Corporate file access and protection. In addition to the IT organisation, multiple internal stakeholders ranging from senior business managers and knowledge workers to legal departments are involved in decision-making and purchasing processes regarding online file access services.

Today, consumer-oriented, public cloud file sync and share solutions are common fixtures in corporate environments since they are easy to obtain, simple to use, and enable employees to access content from any device, at any time, and then share it with colleagues and partners from any location. While convenient for the workforce, this process can leave vast amounts of corporate data at risk, outside of IT's protection, management, and monitoring. This untenable situation can lead to violations of industry compliance or corporate governance regulations, while also risking breach of proprietary information, harm to reputation, and financial loss.

- **Managed services.** Consider employing managed services to perform tasks such as user authentication, access control, reporting, and brokering to ensure that IT is able to capture visibility into the environment, while also maintaining flexibility and securing access. Businesses can also choose between on-premises data storage and public offerings that are collectively managed by a single service.

- **Digital rights management.** Digital rights management provides additional corporate protection by enabling IT and employees to set policy at the file level to restrict processes that include "do not forward," and documents tagged as "company confidential." Companies can also invoke email message encryption allowing employees to securely share files via email.

- **Data encryption.** Encrypted data protects information—from its creation and transport, to its ultimate resting place. Companies must ensure that security best practices are being followed, which means communication streams, files, and mobile access to application data should be encrypted.

Unified communication and collaboration. The way in which employees interact, communicate, and collaborate is poised for change. A younger generation of end-users expects to communicate in a variety of ways that mimic their personal communication experiences—which means that legacy communication systems will not be able to sustain the rapid change, and benefits, that mobility solutions are producing.

- **Monitoring and analytics.** The quality of the conversation and employee interaction are essential for a productive workforce. Because employees will not hesitate to stop using systems that deliver a poor experience, it's essential for IT to have monitoring capabilities in place to proactively detect performance degradation, as well as any potential networking, security, application, and access challenges.

- **Going beyond voice and video.** UCC systems should also include social enterprise communities that enable teams to work together more effectively, share information easily, and track status seamlessly. Access to the environment should be available across a variety of devices and locations in order for employees to interact often, and work smarter together.

- **Modifying employee behaviour.** The environment should invoke a change in employee behaviour that enables the business to operate more efficiently. Business UCC environments will mimic many of the consumer tools to which employees are accustomed, and which they use easily and effectively in their personal lives.

Complexity of technology. As they consider effective mobility solutions, IT professionals can become burdened by an existing surplus in technology. Most companies have invested in some form of application delivery, device management, or data protection but, in an effort to advance their initiatives further, they are caught in a holding pattern, and overwhelmed by the variety of available technology and approaches.

- **Place strategic bets.** Mobility can be a daunting task if embarked upon as a solo journey. Invite strategic IT vendors into the business. Request a technology update and visibility into a strategic roadmap. Share top IT and business initiatives related to mobility. Observe how the IT vendors react to, and comprehend specific and unique challenges.
- **Start with achievable strategic wins.** Prove the value of mobility with key employees who are willing to embrace and accept changes in their behaviours and business processes. Understand the tools that IT requires to protect applications and data as well as what it takes to deliver an optimal end-user experience.
- **Prepare for rapid evolution.** Mobility software and devices are going through a massive wave of innovation that will continue for the foreseeable future. Select technology that can adapt to this rapid change, and identify capabilities that may not appear valuable today but could become strategic over time.

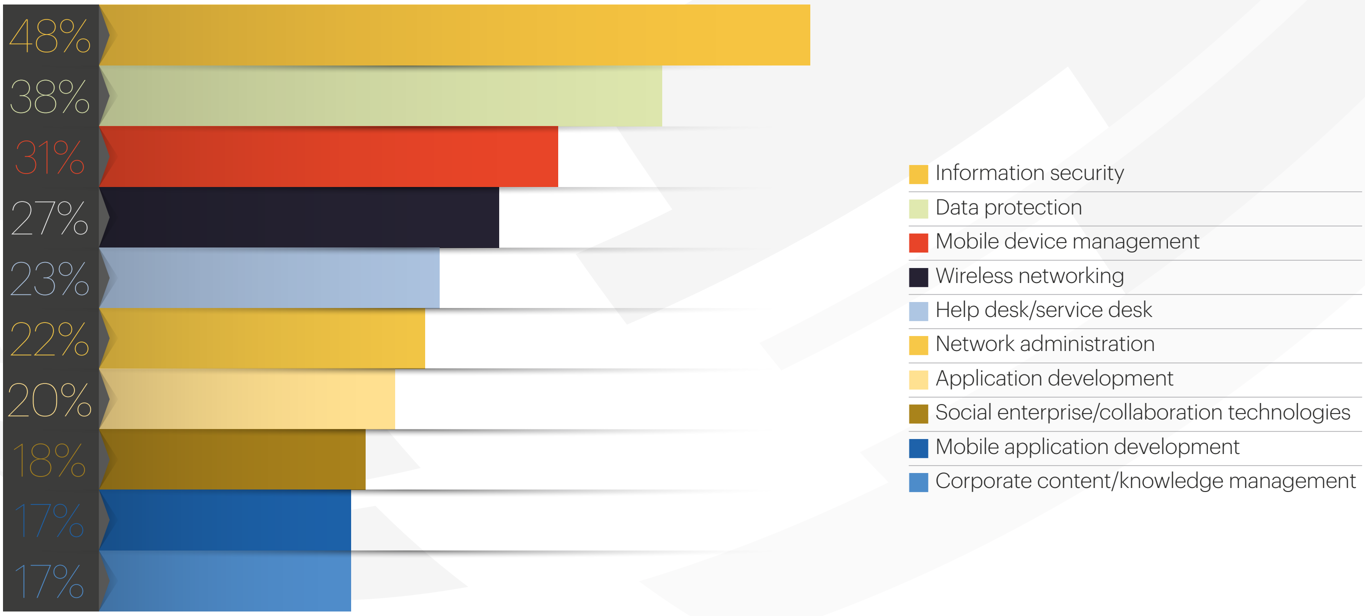
Overcoming Organisational Barriers with the Right Skillsets

Although an organisation can invest in the latest and greatest technology, if it cannot overcome organisational barriers and retain the right skillsets, then the business will struggle to advance its mobility initiatives. Having the right people with the right skillsets is essential to creating, deploying, and supporting an effective enterprise mobility program.

With security top of mind in most mobile initiatives, employees who understand the challenges of protecting their organisation's devices, data, network, and infrastructure are invaluable. In fact, based on ESG research, 46% of IT professionals cited information security as one of the most important skillsets to the on-going support of their mobility strategy, while 38% of those surveyed cited data protection skills. Additionally, 31% indicated that mobile device management skills were one of the most important (see Figure 3).

Figure 3.
Essential Technologies and Skillsets Supporting Enterprise Mobility

Which of the following technologies and skillsets are or will be most important to the ongoing support of your organisation's enterprise mobility strategy?



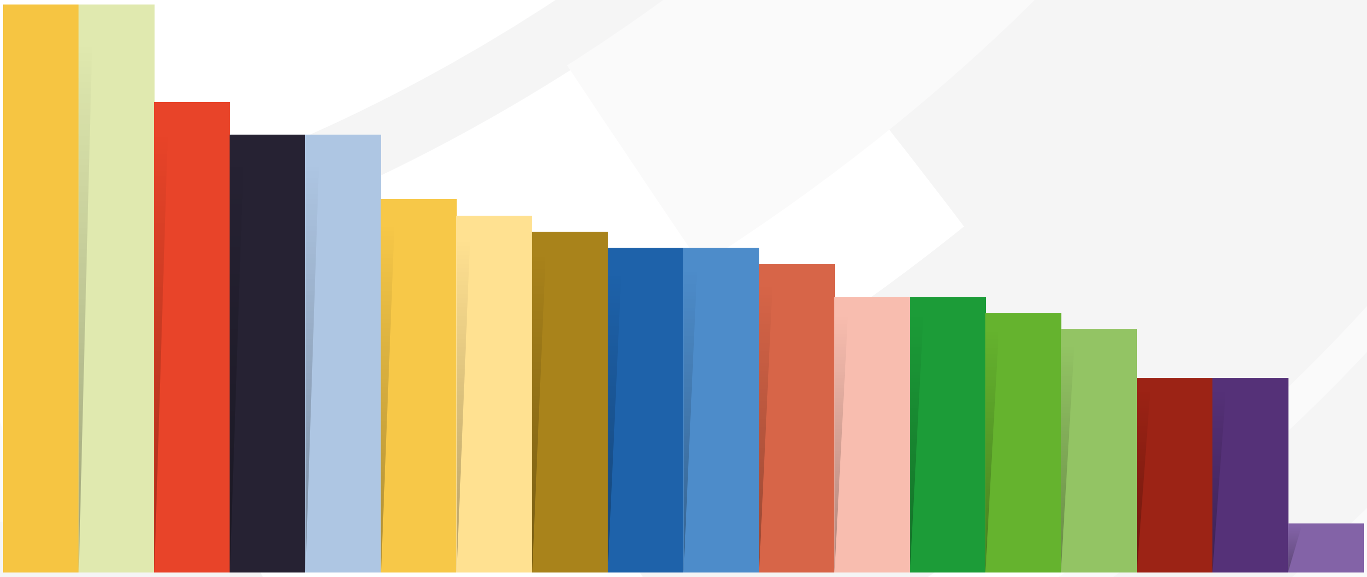
Embracing Mobility: Benefits Across the Organisation

The outlook and promise of mobility is proving beneficial to organisations that can overcome the barriers to becoming a mobile-first enterprise. For those organisations that have wholeheartedly embraced enterprise mobility, many are now reaping a number of benefits—from improving security, through increasing worker productivity, to enhancing communication and collaboration among employees as well as external partners.

Based on ESG research, more than one-third (36%) of IT professionals reported that employee productivity was positively impacted as a result of their enterprise mobility strategy, while 29% stated their organisation benefited from improved IT control (i.e., security). Additionally, 27% of those surveyed indicated that collaboration between employee teams and departments improved, while the same percentage cited that communication and collaboration with external partners improved

Figure 4.
Business Impacts Experienced as a Result of Enterprise Mobility Strategy

To date, which of the following business impacts (either positive and/or negative) has your organisation experienced as a result of its enterprise mobility strategy?



■ Increased IT technology expense but improved IT control	35%
■ Improved employee productivity	35%
■ Improved IT control (i.e., security)	29%
■ Improved communication and collaboration with external partners	27%
■ Improved collaboration and communication between employees, teams and departments	27%
■ Reduced IT operational expenses	23%
■ Challenges with collaboration and communication between employees, teams and departments	22%
■ New business/revenue stream based on mobile capabilities	21%
■ Reduced expenditures associated with existing business process	20%
■ Reduced IT staff requirements	20%
■ Increased occurrences of security breaches	19%
■ Reduced application licensing expenses	17%
■ Challenges with communication and collaboration with external partners	17%
■ Lost or stolen devices compromising corporate data	16%
■ Regulatory compliance violation	15%
■ Reduced corporate-owned device expenditures	12%
■ Reduced productivity	12%
■ None of the above	3%

The Bigger Truth

The business benefits of mobility can be significant for companies that are willing to recognise the potential hurdles, plan ahead, and be able to quickly address and overcome difficulties. Challenges exist in the areas of security, networking, file access, UCC, and IT also has their work cut out for them when it comes to sorting through the technology surplus. Still, companies are seeing measurable benefits. And, while the right technology choice is important, companies must also address organisational challenges to help create centralised support across different IT disciplines.

ESG has witnessed organisations that have created tiger teams and mobility centers of excellence (MCoE), reaping the benefits of positive business impacts (e.g., constructive changes in employee behaviour, and improved productivity).

These changes help companies more easily embrace shifting technology and business priorities, giving them the impetus and ability to confidently accelerate and evolve an effective mobility strategy.

It is vital that IT professionals and business executives recognise and meet the challenges of enterprise mobility, proactively working together to provide a resolution that delivers an enhanced, productive user experience to employees, while mitigating any additional IT risk. Understanding the challenges can help businesses avoid potential pitfalls, and allow them to creatively invest in solutions that aid in solving short-term challenges, and help meet long-term mobility goals.

ENTERPRISE
MOBILITY
EXCHANGE

April 2016 Market Report

Overcoming the Top Five Barriers to Becoming a Mobile-First Enterprise

Sponsors Spotlight

AT&T makes managing mobility simple. Our Enterprise Mobility Management solutions help you harness the full power of mobile-first technology to transform every aspect of your business—giving you a competitive edge.

We strip out all the complexity of managing mobile devices, applications and content, making it easy for you to connect people to each other and to the information they need—anytime, anywhere and on virtually any device.

And by working closely with innovative strategic alliances, we continue to push back the boundaries of what mobility can help you achieve. This is enterprise mobility, only simpler. **www.att.com/emm**

MobileIron is the security and applications backbone for modern end-user computing and provides the foundation for companies around the world to transform into Mobile First organisations. With MobileIron, companies can protect corporate data, securely deliver apps and content, and let employees choose the devices they want to use. MobileIron has been named a category leader by top industry analysts and has been granted 26 patents for its modern enterprise security innovation. More than 10,500 companies worldwide have chosen MobileIron for mobile security.
www.mobileiron.com

Mobile Labs provides enterprise-grade mobile device clouds that improve efficiency and raise quality for agile, cross-platform mobile app and mobile web deployments. The company's patented device cloud, deviceConnect™ is available in both public and on-premises configurations. deviceConnect provides affordable, secure access to a large inventory of mobile devices across major mobile platforms to developers, test engineers, and customer support representatives, among others. At the heart of enterprise mobile app deployment, deviceConnect enables automated continuous quality integration, DevOps processes, as well as automated and manual app/web/device testing on real managed devices. For more information please visit **www.mobilelabsinc.com**

NetMotion Wireless develops mobility management software for enterprises and organisations with mission-critical connectivity requirements. The company's products address the unique challenges created by these workforces by providing the security, visibility, and control that IT departments demand, while minimising the connectivity challenges faced in the field, so mobile workers can be more productive. Thousands of enterprises around the world are using NetMotion products to keep millions of mobile workers connected to applications. NetMotion Mobility®, an intelligent mobile VPN, is a key component to any mobile-first deployment.
For more information visit www.NetMotionWireless.com or start a free trial today!

As a leading global provider of IT Expense Management software and services, Tangoe knows that the health of your mobility program is paramount to success in this ever-changing technological world. We invite you to build on the knowledge you acquired through this report and visit us online for a special offer: download the Tangoe Mobility Starter Kit containing up-to-date information on the current mobility market, including the latest reports from leading analyst firms. Use the link below to gain free access.
https://www.tangoe.com/tangoe-starter-kit-iqpc/

ENTERPRISE
MOBILITY
EXCHANGE

April 2016 Market Report

Overcoming the Top Five Barriers to Becoming a Mobile-First Enterprise

About Enterprise Mobility Exchange

Enterprise Mobility Exchange is an online community for global mobility professionals and business leaders who are leveraging mobile technology and services to improve operational efficiency, increase customer acquisition and loyalty, and drive increased profits across the entire enterprise.

At Enterprise Mobility Exchange we're dedicated to providing members with an exclusive learning environment where you can share ideas, best practice and solutions for your greatest mobility challenges.

You will receive expert commentary, tools and resources developed by experienced mobility professionals and industry insiders. With a growing membership and global portfolio of invitation-only bespoke meetings, Enterprise Mobility Exchange ensures you keep your finger on the pulse by delivering practical and strategic advice to help you achieve your business goals.

SIGN UP FOR FREE to the Enterprise Mobility Exchange now!

Our global events include:

ENTERPRISE MOBILITY EXCHANGE
MARCH
FS.EnterpriseMobilityExchange.com
London, UK

ENTERPRISE MOBILITY EXCHANGE
MAY
EU.EnterpriseMobilityExchange.com
The Netherlands

ENTERPRISE MOBILITY EXCHANGE
JULY
US.EnterpriseMobilityExchange.com
Atlanta, US

ENTERPRISE MOBILITY EXCHANGE
SEPTEMBER
UK.EnterpriseMobilityExchange.com
London, UK

ENTERPRISE MOBILITY EXCHANGE
SEPTEMBER
APAC.EnterpriseMobilityExchange.com
Phuket, Thailand

ENTERPRISE MOBILITY EXCHANGE
NOVEMBER
LasVegas.EnterpriseMobilityExchange.com
Las Vegas, US

2016 Market Report Offering

January:
Wearable Devices – Enterprise Expectations and Initiativ

February:
Mobile Applications – What's Next for Businesses?

March:
Why Big Data and Analytics Matter

April:
Overcoming the Top 5 Barriers to Becoming a Mobile-First Enterprise

May:
Keeping Up in a Connected World – The Future of M2M in the Enterprise

June:
Exploring the Mobile Enterprise – 5 Exclusive EME Case Studies

July:
Field Services – Finding New Value From Mobile Technology

August:
Mobile Security – Solving the Number One Challenge With Mobility

September:
Top 5 Mobility Mistakes – Lessons Learned for Future Success

October:
Wi-Fi Infrastructure and Connectivity

November:
Engaging Customers With Mobility – Innovation through Communication

December:
Looking Ahead to 2017 – The EME Analyst Insight Report

For more information regarding these reports, email EMEsponsorship@iqpc.com

JOIN THE DISCUSSION ON SOCIAL MEDIA!

http://bit.ly/2OMoH2a

http://bit.ly/1ROkFAx

http://on.fb.me/1OElNsC

http://bit.ly/1MKyI5y

http://bit.ly/1kMNfHx

WWW.ENTERPRISEMOBILITYEXCHANGE.COM