AUGUST 2016 MARKET REPORT

ENTERPRISE MOBILITY EXCHANGE

Market Report: Mobile Security: Solving the Number One Challenge Within Mobility

Sponsored by:

www.EnterpriseMobilityExchange.com

August 2016 Market Report

Mobile Security: Solving the Number One Challenge Within Mobility

About the Authors

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 behavior 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 virtualization. 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

Security: Top of Mind When Supporting an Increasingly Mobile Workforce

With the growing bring-your-own-device (BYOD) trend, the proliferation of devices and applications raises some serious concerns for both business and IT leaders. While mobility can introduce great benefits in terms of productivity and collaboration, among others, a number of ancillary and support considerations must be weighed. A robust mobility strategy includes not only the technology components (ranging from devices to applications), but also the processes and staff needed to shape, implement, and maintain mobility initiatives. Given the heightened focus on cybersecurity (even beyond IT groups) over the last several years, it is not surprising that nearly half (46%) of organizations believe information security technologies and skillsets will be most important when it comes to carrying out mobility strategies (see Figure 1)[1].

Based on ESG research (even outside the confines of enterprise mobility), the three most commonly identified challenges related to managing the applications and endpoint devices that employees used to perform their daily job functions involve various aspects of information security. Specifically, organizations cited the security of endpoints (50%), threat detection and/or prevention (47%), and corporate file access and protection (34%) as some of the biggest issues they encounter when it comes to enabling end-user computing environments. As the workforce becomes increasingly mobile, risk for the business escalates—with lost and stolen information opening new doors for cyber-criminals.

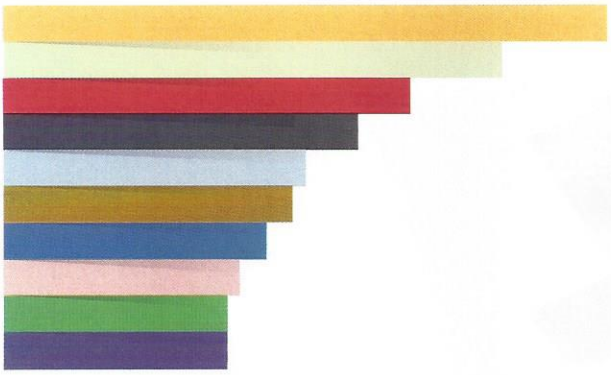
Clearly, information security is at the top of the priority list of many IT departments, especially in the context of supporting end-user computing environments and initiatives. It comes as no surprise then that more than one-third (34%) of respondents identified proactive threat detection as one of the five biggest influences on their organization's enterprise mobility strategy (see Figure 2)[2]. Indeed, without the proper security planning, tools, and processes, the mantra of data anytime, from anywhere, on any device is likely to be as appealing to a cyber-criminal as it is to a mobile employee.

[1] *Source: ESG Research Report, Security, Productivity, and Collaboration: Trends in Workforce Mobility, May 2015.*

[2] *Ibid.*

Figure 1.
Most Important Technologies and Skillsets to Ongoing Support of Enterprise Mobility Strategy

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

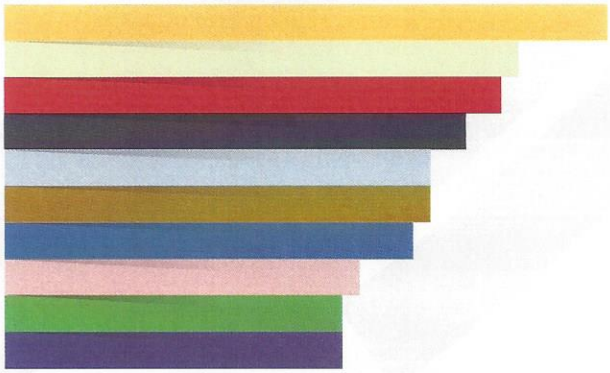


- Information security 46%
- Data protection 38%
- Mobile device management 31%
- Wireless networking 27%
- Helpdesk / Service desk 23%
- Networking administration 22%
- Application development 20%
- Social enterprise / collaboration technologies 18%
- Mobile application development 17%
- Corporate content / Knowledge management 17%

Source: Enterprise Strategy Group, 2016

Figure 2.
Factors with Greatest Influence on Enterprise Mobility Strategy

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



- Protective threat detection 34%
- Improvement of employee productivityvia mobile enablement 29%
- Improvement of communication and collaboration between employees 28%
- Improved/enhanced security of 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 your login experience 19%

Source: Enterprise Strategy Group, 2016

**Lesser factors from the survey included Support for Microsoft Windows on Apple devices; simplified means of managing desktop, apps, and date for contractor/temporary employee; and hardware refresh.*

Mobility Is Critical for a Productive Workforce

The PC has revolutionized the way businesses operate—in terms of both organizational and individual workflows. Employees interact with a pane of glass to communicate, collaborate, access information, learn, record data, and perform a variety of other business-oriented tasks. Laptops have helped create the portability of this environment, but it is the recent increase in the variety of alternative endpoint devices—most notably the smartphone and consumer simple applications—that are creating the mass behind the way businesses deliver and enhance an end-user workspace. The mobility movement is proving itself critical for employees to be able to perform their primary job functions. A vast majority of midmarket and enterprise organizations consider the ability for their employees to access business applications and IT services anytime from any location to be either critical (43%) or at least important (45%). Looking ahead 18 months revealed that this trend shows no signs of reversing course, with the number of organizations identifying mobility as critical, increasing to 52%[3].

With so many organizations placing a premium on mobility, it follows that many would attempt to support these initiatives with structure and process in the form of an all-encompassing mobility strategy. What benefits have been gleaned from these strategies to date and, conversely, what challenges or negative impacts have been experienced? More than one-third of organizations believe that mobility strategies have served to improve employee productivity (36%), and/or increase IT technology expenses (35%)[4]. Given the heightened focus on, and challenges associated with, securing a more mobile workforce, it is vindicating that nearly one-third (31%) of respondents have derived an improvement in IT control from their enterprise mobility strategy. The other most commonly cited business impacts included improvements in collaboration and communication, both internally (i.e., between employees, teams, departments, etc.) and externally (i.e., with partners).

Who Is Responsible for Mobile Computing Security Policies?

Mobile computing security is a rather amorphous topic at many organizations. It not only covers the basics—confidentiality, integrity, and availability of mobile devices, applications, and network connectivity—but also extends to applications, business processes, identities, privacy laws, etc. Of course, mobile computing also includes some new considerations because most devices today are distributed with cameras, GPS connectivity, and microphones. Finally, mobile devices may belong to employees and not the organization itself.

All of these factors suggest that mobile computing security policy creation, review, and updates should be cross-functional activities with participation from IT, information security, compliance, legal, business, and HR teams at the very least.

According to ESG data, it appears there is a disconnect between mobile security policy creation and the processes for ongoing policy reviews and modifications. Of those organizations with mobile computing security policies in place, policy creation is reportedly strictly the domain of the IT department (IT operations, IT security, and general IT). While policy review and modification are still dominated by IT, respondents said that other groups, such as corporate governance, compliance, and legal teams, are also included in the process (see 3)[5].

We suggest that IT and security managers gather more input from their line-of-business counterparts during the initial mobile security policy creation phase. IT representatives should take time to understand who will be using mobile devices and for what purposes. Furthermore, CIOs and CISOs should assess future mobile computing plans as they relate to employees and external parties like business partners, customers, and suppliers. This upfront planning should help organizations identify long- and short-term security requirements, create more suitable policies, and determine what types of controls are needed for policy enforcement.

[3] *Ibid.*

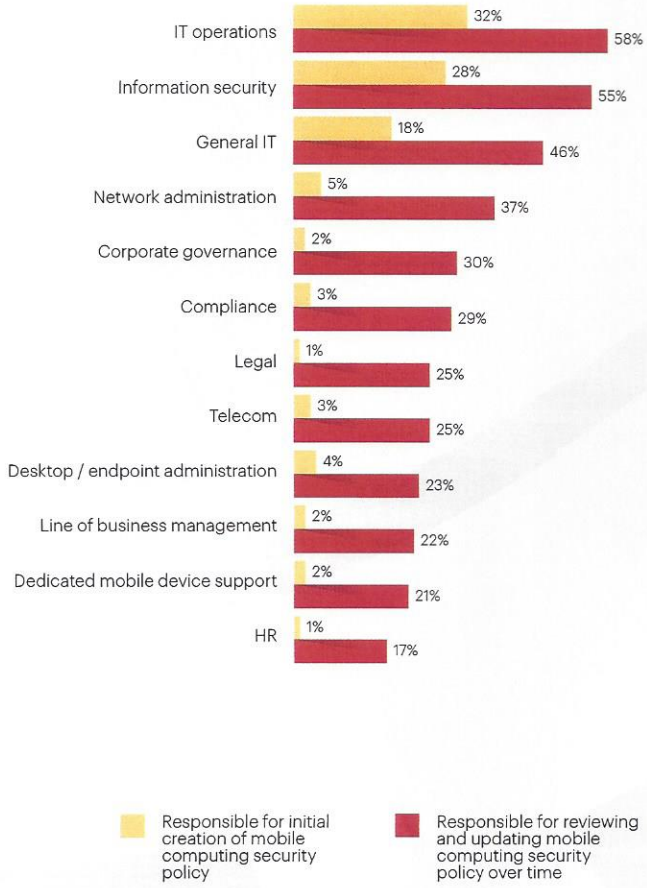
[4] *Ibid.*

[5] *Source: ESG Research Report, The State of Mobile Computing Security, February 2014. All ESG research references and charts in this market report have been taken from this research report unless otherwise noted.*

Mobile Security: Solving the Number One Challenge Within Mobility

Figure 3.
Individuals/Groups Responsible for Mobile Computing Security Policy

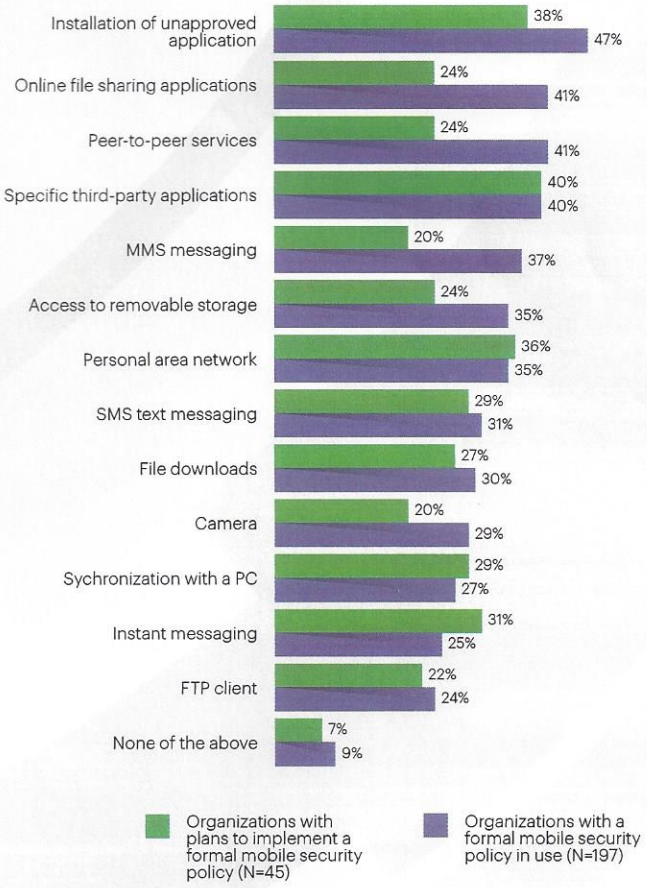
Which of the following individuals/groups are responsible for reviewing and updating your organization's mobile computing security policy over time? Which of these individuals/groups were most directly involved in the initial creation of your organization's mobile computing security policy?



Source: Enterprise Strategy Group, 2016

Figure 4.
Types of Mobile Device Capabilities Organizations Disallow

As part of its current or planned mobile computing security policy, does/will your organization disable or disallow access to any of the following mobile device capabilities and/or services?



Source: Enterprise Strategy Group, 2016

Security Policies for Mobile Devices

In addition to acceptable use policies and user training, security managers also mandate and enforce specific policies around mobile devices themselves. Security professionals claim their organizations most often disable or disallow installation of unapproved applications, including specific third-party applications, and block access to online file sharing and peer-to-peer services with mobile devices (see Figure 4).

Security professionals seem most anxious about rogue applications, data leakage, and network threats. This represents standard security best practices and sound risk management. What is interesting, however, is the relative lack of concern around mobile device-specific functionality such as cameras, PC synchronization, and instant messaging that carry inherent security implications. CISOs should assess these potential security risks associated with mobile device-specific functionality as they relate to different use cases and user roles.

Mobile Computing Security and the IT Organization

Mobile computing projects tend to go from proof of concept (POC) to enterprise-wide deployment in a short timeframe. This rapid transformation demands broad collaboration from a number of groups, including application developers, network administrators, security professionals, and IT operations staff.

We pursued the cross-functional IT mobile computing model further, asking security professionals to identify which IT groups participate on this team. As it turns out, cross-functional IT mobile computing teams tend to be skewed toward IT operations (43%), followed by information security, general IT staff, and dedicated mobile device support staff.

This division of labor makes sense during the genesis phase of mobile computing initiatives due to the following requirements:

The influence of the IT operations team extends beyond mobile device management. As it turns out, 39% of security professionals claim that the IT operations group is most responsible for mobile device security as well (see Figure 5).

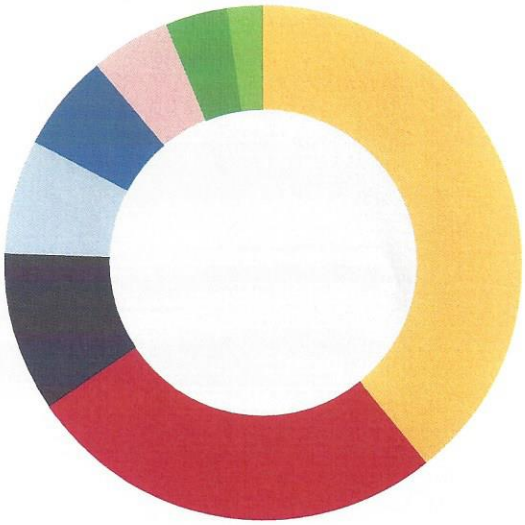
Onboarding.
When organizations approve BYOD or mobile computing projects, they immediately face the challenge of provisioning accounts and configuring endpoints. IT operations teams tend to lead this effort.

Network access controls.
Mobile devices need secure access to the network, whether via campus-based WiFi access points or VPNs for remote access. Once again, these tasks are handled by IT/network operations groups.

Mobile device traffic management.
Tablets and smartphones are bound to drive new types of traffic on the corporate LAN. IT/network operations teams are called upon to fine-tune the network to accommodate diverse network requirements.

Figure 5.
Individuals/Functional Groups Responsible for Mobile Device Security

Which of the following individuals or functional groups are most responsible for mobile device security services (i.e., monitoring network traffic/user behavior for suspicious/malicious activities, installing/managing anti-virus software, keeping up with latest mobile threats, etc.) in your organization?



IT operations	39%
Information security group	26%
General IT staff	10%
Telecom staff/administrators	7%
Network administrators	6%
Dedicated mobile device support staff	5%
Desktop/endpoint administrators	4%
Help desk	2%

While this may seem counterintuitive, it makes sense because it adheres to the beset practice principle that "a well-managed device is a secure device." Activities like device hardening, configuration management, storage encryption, and remote wiping are most often handled by IT operations teams. Nevertheless, security teams do—and should—still play an active role in mobile device management and security today. It's likely that their responsibilities will only increase as the mobile computing infrastructure grows more complex and the mobile computing threat landscape grows more dangerous.

Mobile Application Development and Security

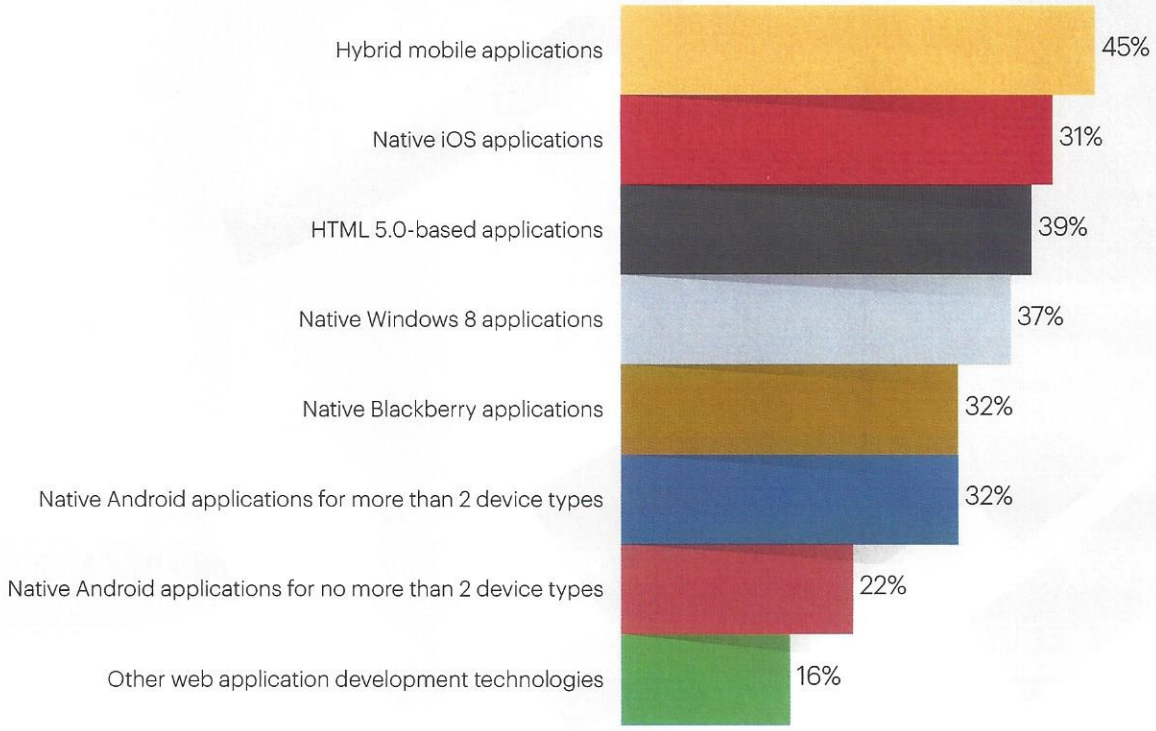
As previously noted in Figure 4, 88% of enterprise organizations stated that they consider mobile device use as critical or very important for business processes and worker productivity[6]. To support increasingly vital mobile computing use cases, many organizations have become extremely active with mobile application development. In fact, 42% of enterprises claim that they are developing a significant amount of custom mobile applications.

Respondents were also asked to comment on the various mobile software development models used at their organizations. As it turns out, many organizations have a multitude of development models and target platforms—45% develop (or are interested in developing) applications using a hybrid model, 41% develop (or are interested in developing) applications for native iOS platforms, 39% develop (or are interested in developing) applications using HTML 5.0 technologies, and 37% develop (or are interested in developing) applications for the Windows 8 platform (see Figure 6).

[6] *Source: ESG Research Report, Security, Productivity, and Collaboration: Trends in Workforce Mobility, May 2015.*

Figure 6.
Current/Expected Mobile Application Development Platforms

Is your organization developing or interested in developing mobile applications on the following platforms?



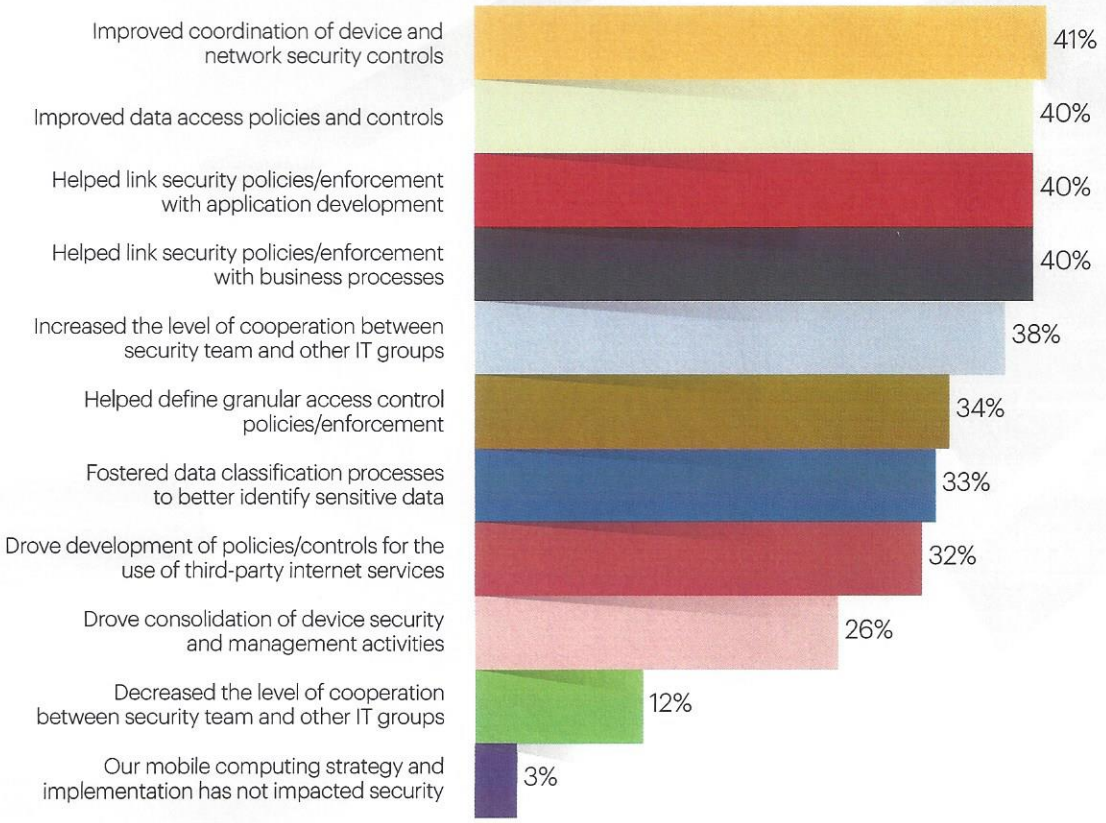
Source: Enterprise Strategy Group, 2016

The Bigger Truth

As organizations approach mobile computing security, they often find themselves at a crossroad. Down one road, mobile computing represents IT chaos, fraught with privacy concerns and scalability challenges associated with supporting all distributed endpoint devices, applications, and underlying infrastructure that comprise the mobile ecosystem. On the other path, however, mobile computing presents an opportunity to learn from the past and include a security focus from the onset of mobile computing projects. As such, we wanted to solicit input on potential security improvements and best practices that were actually derived from current mobile computing initiatives. It is reassuring to see that security professionals do see a number of serendipitous effects associated with mobile computing—41% believe that their mobile computing strategy improved coordination of device and network security controls, while 40% claim that their mobile computing strategy helped them improve data access policies and controls, link their security policies/enforcement with application development, and/or drive increased cooperation between the security team and other IT groups (see Figure 7). CISOs should take note of these results and strive for similar benefits as part of mobile computing projects. The fact is that mobile computing, cloud computing, and IT consumerization trends remove control points from corporate IT. Given this, CISOs must establish strong security policies, controls, and oversight over those areas that IT continues to own.

Figure 7.
How Mobile Computing Strategy and Implementation Has Impacted Security

In general, how has your organization's mobile computing strategy and implementation impacted security, if at all?

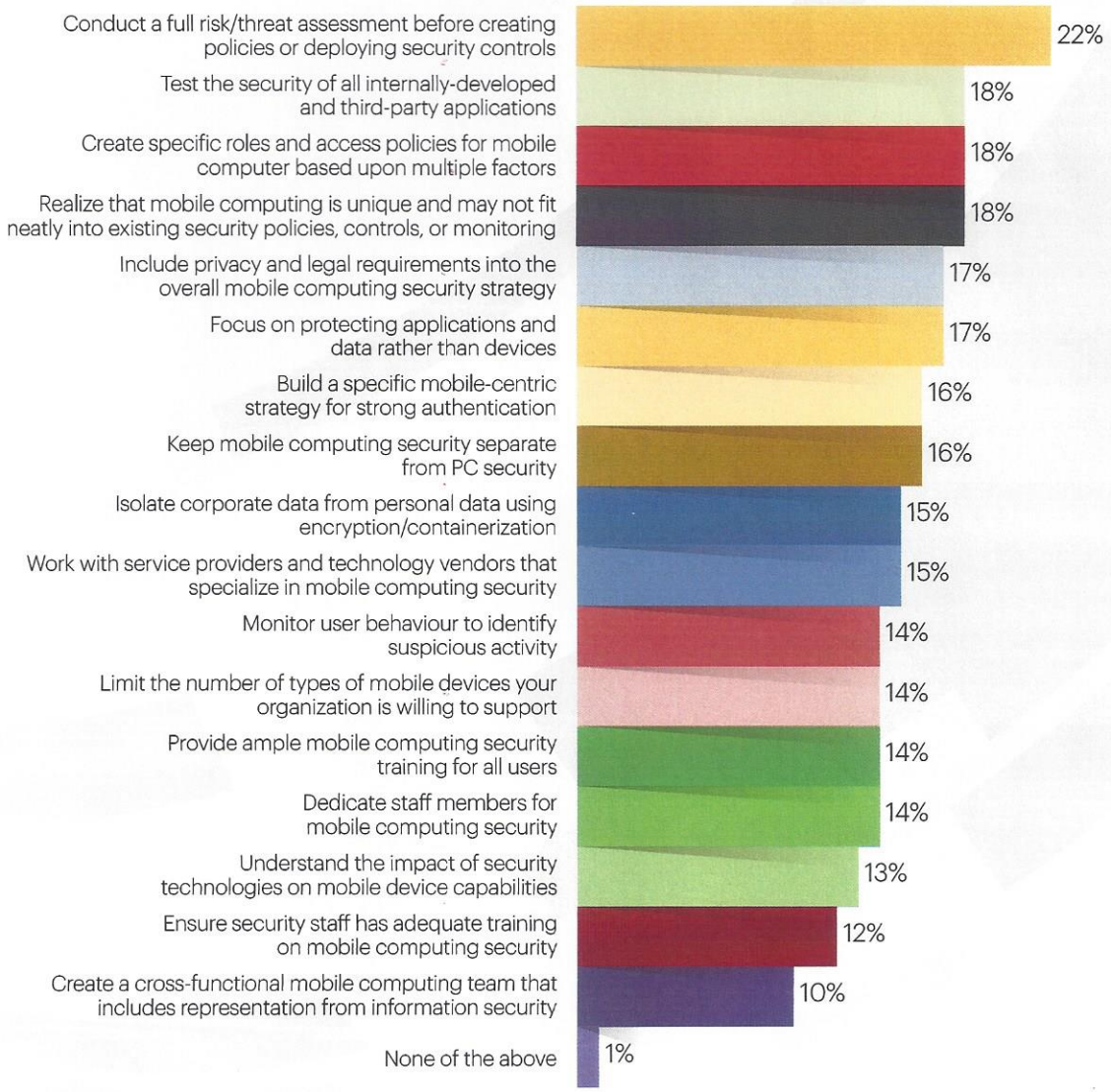


Source: Enterprise Strategy Group, 2016.

Even though mobile computing is still in its genesis, ESG asked security professionals to identify their "lessons learned." Based on experience, security professionals have lots of ideas for mobile computing neophytes such as conducting formal risk assessments before creating policies or deploying security controls, testing the security of all internally-developed and third-party applications, and creating specific roles and access policies for mobile computing based upon multiple factors (see Figure 8).

Figure 8.
Mobile Computing Best Practices

Based on your organization's own experience with mobile computing security, which of the following security best practices do you believe would be most important for an organization just beginning to support mobile devices for its own employees to consider?



Source: Enterprise Strategy Group, 2016.

Conclusion

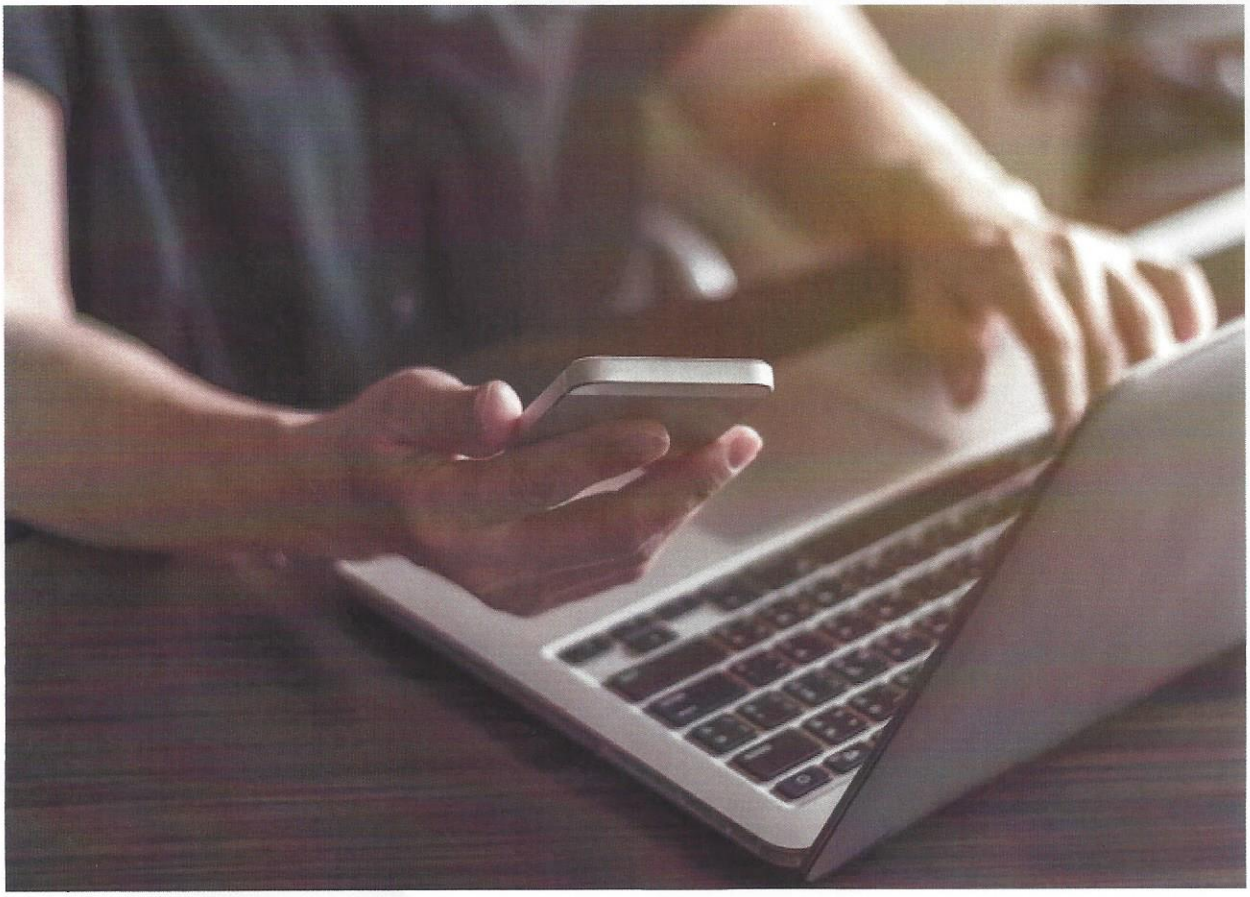
Mobile computing offers numerous benefits to businesses, but the complexity of creating a viable strategy and efficient implementation are proving to be a daunting task. Proactive businesses will be diligent in researching the types of solutions comprising their mobility initiatives, and will also determine the most effective ways to manage those solutions, based on the specific needs of their organizations.

Businesses should also explore companies that can help with initial consulting and assessment services, employ solutions that manage devices and applications, and take advantage of accessing cloud resources. The challenge, as well as the opportunity, lies in how companies can streamline business processes as they strike a balance between increasing employee productivity and ensuring system security.

The first step of a mobility strategy should begin with assessing, analyzing, and creating a project roadmap. Upon completing the initial (albeit critical) step, companies should look at choosing an enterprise mobility management (EMM) solution to capture, control, and manage mobility initiatives. EMM aides businesses by regulating and protecting mobile devices, applications, services, and platforms, while providing secure mobile workspaces.

EMM TAKES THE CHAOS OUT OF TRYING TO MANAGE VARIOUS SOLUTIONS SEPARATELY

In essence, EMM takes the chaos (and headache) out of trying to manage various solutions separately—ultimately helping organizations reduce costs, protect business-critical information, improve productivity and enhance the user experience. EMM helps the IT organization control access to devices, applications, and data, while allowing users to securely access business systems and digital content, and embrace initiatives like BYOD. Due to the impact of mobility, it is common for businesses to turn to experienced companies that can help support large scale mobility initiatives that span mobile application development, data security, device management, and support services during the crucial and complex transition to enterprise mobility.



Mobile Security: Solving the Number One Challenge Within Mobility

Sponsor Spotlight

AT&T makes managing mobility simple. Our Enterprise Mobility Management solutions help you harness the full power of mobile technology to transform every aspect of your business—giving you a real competitive edge. AT&T has helped many organizations innovate faster, made their data work harder, and helped their people work smarter.

We strip out 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 virtually—anytime, anywhere and on virtually any device. You can focus on driving your business while we design, deliver and support a highly secure, agile mobility platform.

We know mobility inside out. We've been at the forefront of mobility since the very beginning, and we draw on all of that experience and expertise to help you plan and deliver a strategy that gets results. And by working closely with the most innovative companies in this space we continue to push the boundaries of what mobility can help you achieve.

All this experience has helped us build a comprehensive Enterprise Mobility Management portfolio. It includes solutions for: creating successful mobility strategies; managing and securing mobile devices; applications and content; developing cutting-edge mobile apps; controlling mobility costs; and helping your people work together in innovative and collaborative ways.

And because we're also a network provider, we can provide end-to-end assistance across every part of the mobility spectrum—from strategic consulting to network migrations.

Let us help you give your people what they need, when they need it—without driving up costs or adding more IT complexity. This is enterprise mobility, only simpler.

The problems we solve

- Engaging mobile first customers: Today's customers expect the same quality of service and access to information on mobile that they'd get through any other channel and these expectations will continue to grow. Businesses must act now to deploy highly secure mobile apps that are engaging to customers and scalable to meet future demands.
- Empowering the mobile workforce: Businesses are under increasing pressure to embrace mobility and keep up with growing employee demands for anytime, anywhere access to information and services. The potential productivity benefits can be huge, but only if devices, applications and content are managed and secured effectively.
- Creating a mobility strategy: Defining an overall strategy for mobility—and ensuring it can keep up with constant changes in technology and user behavior—is a major challenge for many organizations. Businesses must prioritize which changes will provide maximum benefit, and they must ensure costs are kept under control.
- Limited IT resources: Embracing mobility has become a business necessity, but new solutions cost money and can have a major impact on existing infrastructures and IT resources.
- Managing complexity: IT organizations need to retain control of mobility in the BYOD era by centralizing the management of security, access, policies, content distribution, application, and device provisioning. All this needs to accommodate a growing range of devices, operating systems and mobile carriers, while balancing appropriate security with the need for constant access.

Mobile Security: Solving the Number One Challenge Within Mobility

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 practices 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 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:

MARCH
FS.EnterpriseMobilityExchange.com
London, UK

MAY
EU.EnterpriseMobilityExchange.com
The Netherlands

JULY
US.EnterpriseMobilityExchange.com
Atlanta, US

SEPTEMBER
UK.EnterpriseMobilityExchange.com
London, UK

SEPTEMBER
APAC.EnterpriseMobilityExchange.com
Phuket, Thailand

OCTOBER
cloud.enterprisemobilityexchange.com
Miami, US

NOVEMBER
LasVegas.EnterpriseMobilityExchange.com
Las Vegas, US

2016 Market Report Offerings

January:
Wearable Devices – Enterprise Expectations and Initiatives

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:
Unleashing IoT Value by Harnessing the Power of Data

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/20MoH2a
http://bit.ly/1ROkFAx
http://on.fb.me/1OElNsC
http://bit.ly/1MKyI5y
http://bit.ly/1kMNfHx