ISMG
INFORMATION SECURITY
MEDIA GROUP

2016 Mobile Security & Business Transformation Study

Learn How Mobility Has Forever Changed the Way Enterprises Conduct and Secure Business

INSIDE

- Complete Survey Results
- Expert Analysis
- Insights from Jason Hardy of IBM Security

IBM

Tom Field

Ninety-nine percent of the enterprise workforce currently uses mobile devices – smart phones and tablets – to perform their jobs today. And nearly 60 percent of security leaders describe their organizations as either partially or fully mobile, deriving enhanced productivity and other business benefits.

But 63 percent also say that mobility comes with a greater number of security risks and concerns than expected. And 59 percent say more IT resources are required to support the increased number of devices and applications.

These are among the key findings of the 2016 Mobile Security & Business Transformation Study, which examines how mobility has transformed how enterprises conduct business. In this study, respondents detail:

- The impact of mobility on global enterprises;
- How mobility has truly transformed how enterprises conduct – and secure – business;
- The current state of mobile security, and how enterprises will improve it in 2016.

This survey was conducted online during the winter of 2015/2016, and we had over 200 respondents from organizations across industry sectors and global regions.

Join me in a review of the full survey responses, and then let's analyze the degree to which mobility has truly transformed how we conduct business.

Best,

Tom Field
Vice President, Editorial
Information Security Media Group
tfield@ismgcorp.com

About this survey:

This anonymous survey was conducted online by the ISMG research team during the winter of 2015/2016, targeting C-level security and technology leaders from ISMG's audience base. The survey attracted more than 200 respondents from organizations across industry sectors and global regions, with emphasis on the U.S., U.K. and E.M.E.A.

Table of Contents

Features

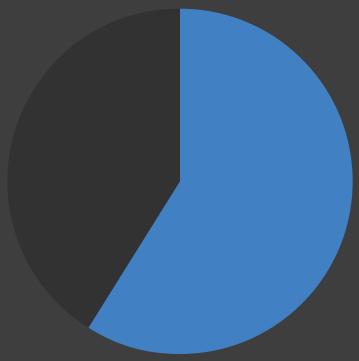
Survey Analysis: How to Transform Business via Mobility – Analysis and Insight from IBM's Jason Hardy.

Survey Results: Mobility may be near ubiquitous in some organizations, but that does not mean they are necessarily exhausting innovation from these devices.

2016 Mobile Security Agenda: Among the most important points to know about resources available for mobile security in the year ahead: 60 percent of respondents expect a budget increase.

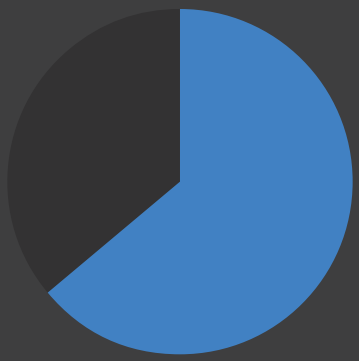
By the Numbers

Some standout figures from this survey.



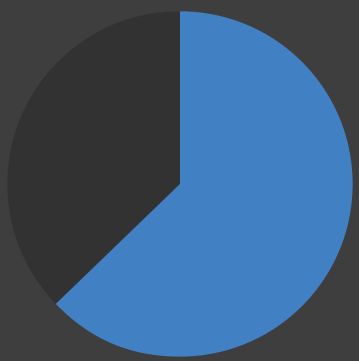
59%

59 percent of security leaders describe their organizations as either partially or fully mobile.



64%

64 percent of employees have easier access to the information they need when and where they need it, allowing them to be more efficient and responsive.



63%

63 percent also say that mobility comes with a greater number of security risks and concerns than expected.

How Mobile is Transforming the Enterprise

Analysis and Insight from IBM's Jason Hardy

Note: In preparation of this report, ISMG's Tom Field sat down to discuss the survey results with Jason Hardy, worldwide market segment manager within mobile security at IBM Security. Following is an excerpt of that conversation.


Jason Hardy

Enterprise Transformation?

TOM FIELD: What's your gut reaction to these results? Do you find that they validate or challenge the hypothesis you had going into the project?

JASON HARDY: My goal for this survey was to try to get beyond the hype of mobile and get some solid data around the topic of how mobile is transforming the enterprise. Our respondents told us that, in almost all cases, mobile is being used within their enterprise. They are taking steps to deploy mobile security strategies, and 60 percent said they'll spend more in 2016 than they did in 2015 on mobile. So that's a good sign.

We saw the companies say they're not only seeing productivity gains, but they have been able to measure these gains and attribute them to mobile. A lot of times that's the challenge. You put a program in place; your gut tells you it's successful, but you struggle with being able to actually tie results back to that program.

FIELD: Did any of the results actually surprise you?

HARDY: In 2014 we did a mobile security survey to see where companies were in terms of maturity. We found they were deploying the MDM solutions. They were taking steps to protect devices and secure content, but very few were addressing application, access and fraud risk.

And when we did this [new] survey, we found more of the same. That was really surprising to me. MDM and EMM have been deployed, and there are plans to do more of the same, but security seemed to stall at that point.

The problem this creates is that while mobile and mobile threats continue to grow, enterprises have stalled. We're protecting devices, but we really haven't gone further down the path of dealing with application security or dealing with malware and fraud.

Rise of the Apple iOS

FIELD: What do you conclude from what the respondents are now telling us about their preference for Apple devices?

HARDY: That was something we didn't expect based on previous results. In general iOS and Android, which are the obvious leaders in the mobile space, have to be supported within the enterprise. Generally speaking, Android is more consumer-focused, while Apple is focused on the enterprise. So when you think about the BYOD model or just the fact

that even corporate-owned devices end up with consumer apps on them, organizations need to have policies in place that allow them to support both platforms.

There is some perception that one platform is more secure than the other. Both have their vulnerabilities. Enterprises need to be ready to support them and be aware of the vulnerability of each platform.

"We're protecting devices, but we really haven't gone further down the path of dealing with application security or dealing with malware and fraud."

Security Concerns

FIELD: Nearly 60 percent of our respondents say that security concerns do inhibit their mobile deployment. What are the top security issues that you see, and how are organizations responding to them?

HARDY: When we first started developing this survey, I used the idea of our mobile security framework as a blueprint for the topics I wanted to research. The framework is designed as a guide to help enterprises think about the full spectrum of mobile threats that exist in the market, and then develop a mobile security strategy that considers all of those threats. We talk about protecting devices and then moving on to securing content and collaboration, safeguarding applications and data, and then finally managing access and fraud. Our message is that you need to think about these challenges holistically.

The consistent number one concern I hear from the market is, "How do I protect devices?" They are worried about what happens if that device is lost or stolen. What data is at risk, and what access might someone gain to their environment with that device?

Protecting devices is a great place to start, but understand that it's just a starting point. You can't lock down the device and assume that the other threats will be held at bay by the secured device. You can lock down that device, but if the user downloads an app that has security flaws in it, the threat is now on the mobile device and has bypassed the physical security measures that have been put in place.

So, what are organizations doing? Our survey results are consistent with what I've seen in the market. CISOs are deploying the EMM solutions as that first step. It's always the number one topic when I talk to people.

Business Benefits

FIELD: We saw that nearly 60 percent of our respondents say that they are what they would consider a fully mobile organization. And by that, they say that they are seeing enhanced productivity and some other business benefits. My question for you: Do enhanced productivity and other business benefits constitute a true business transformation?

HARDY: We're in the early stages of mobile-driven true business transformation. I compare where we are today with mobile with where we were in the mid-to-late 1990s with the web. Everyone was putting up a website because that is what they were told to do. They didn't know how or if it was going to transform their business, but they knew everyone was doing it, and so they did it as well. There were companies that were seeing real business results, but most were still figuring it out. That's where mobile is today.

There is no question that mobile is transforming how we live our lives and how we do business. But the question is: What are the benefits, and are we able to measure them? In our survey, 26 percent of respondents said they are seeing increased revenue as a result of mobile strategy. Twenty-six percent isn't a huge number, but based on where we are with companies just figuring out mobile and then actually being able to link the increased revenue back to mobile

initiatives, that is pretty impressive. It shows companies are having success with mobile and are doing things that are transforming how they function.

FIELD: What are some of the truly progressive things you see organizations doing?

HARDY: Some companies are doing progressive things, but many are just working on basic mobile enablement, like deploying mobile apps and providing mobile access to resources that were previously accessible on laptop and web applications.

One example I have is a customer in the facility management field that is deploying smartphones to their associates. These associates work at remote customer sites. By deploying smartphones to these remote employees, it allows these users to get their daily work assignment and reach out to management resources to resolve issues more efficiently.

What I found interesting about what they were doing is that many of their end users have never had a cell phone, let alone a smartphone. This company is essentially handing out mini-computers to a population of users that has never had a computer as part of their day-to-day job. They are changing how these people work on a daily basis.

That is a pretty progressive step just in terms of enabling people that you might not have ever imagined being technology-enabled in the past.

"There is some perception that one [mobile] platform is more secure than the other. Both have their vulnerabilities."

Mobile Security

FIELD: It is clear our respondents are concerned about data loss and malware. But what are their top security threats, and how do they need to begin to address them?

HARDY: Organizations need to understand that if the device is at risk, then the enterprise data may be at risk as well. Mobile malware may be used to collect user credentials that can be used to access web-based applications.

It is increasingly more common for the hackers to collect sensitive information on a mobile device and then use it for other attacks. Right now these platforms are less secure and make for a good target. After all, we've spent years securing laptops, and we now do a pretty good job at that.

Therefore, companies need to deploy a solution that identifies devices that contain malware, devices that have been jailbroken or rooted, or even devices that are running an OS version with known security issues. They need solutions that help them decide whether these devices are secure enough to be allowed to access their environments and help them limit their level of access. And these solutions need to take proactive steps to make these determinations.

Content and Collaboration

FIELD: What would you say is the current state of the art in ensuring that the content stays secure no matter where or how it's accessed?

HARDY: Organizations today are still working out how to best provide and secure access to content. They are having discussions such as, "Do we want to leverage a cloud solution like Box? Do we want to take advantage of Office 365 or Google Docs? Should users be able to take content and save it in a preferred location, even if that location is not supported by IT?"

Regardless of their decision, an enterprise mobility management solution needs to be able to play a big part in giving users a seamless experience to accessing that information and provide security around what they can and can't do with it. This includes supplying direct content functionality, as well as integration with the customer's choice of solution.

One of the things we talk about is making sure your end users have options. If you don't give them an option that you've approved like Box, they're going to go out and find another solution for sharing files. So, one step you can take to secure your content is to give them options because chances are if you recommend an option, they're going to use it. If you don't, they're going to find a way to get the job done, and it may be an option that is not as secure as you want.

"Protecting devices is a great place to start, but understand that it's just a starting point."

Application Security

FIELD: It struck me that organizations aren't particularly bullish on their application security practices when it comes to mobile, and at best it seems that they're either tending to just the basics of blacklisting and whitelisting, or they are paying lip service to software development lifecycle practices.

HARDY: Application security is one of the areas of the survey that I took a detailed look at right up front because in the past it was an area of weakness within organizations.

First, 42 percent of respondents say their application security is above average when compared to their peers, which led me to believe companies were doing pretty well. I then looked at what they said they were doing for application security and the top two items were what you mentioned: whitelisting and blacklisting of apps and incorporating secure software lifecycle development practices. These areas are a great start, but they aren't enough.

When I saw whitelisting and blacklisting of apps, my first thought was: Based on what criteria? How do you make the decision of what apps are on the blacklist versus the whitelist? And then my second was: Once you create this list, are you able to monitor and enforce this approach?

SDLC practices are another great start and should be part of everyone's app security strategy, but it's only as good as the most recent training information that your staff has and the ability to implement it.

Fraud

FIELD: Mobile is an increasingly attractive channel for fraudsters to enter organizations now. Given that as the reality, how do the targets need to better protect themselves?

HARDY: When you start focusing on the end users, there's only so much that the enterprise can do, and then it really falls on the end users to take some ownership. With over two billion smart devices in the world, the mobile platform makes for a very attractive target for fraudsters. When you compare laptops and smart devices, there are some significant differences in how they are sourced, deployed, monitored and managed. Mobile represents the first time where most users are bringing their own equipment. IT no longer owns the device. They don't put an image on the device and control the device like they did in the past.

When you think about OS upgrades on your laptop, you were never scrambling for the newest OS and rushing to download it. You worried about what it might break. With mobile, the newest OS is announced, and then there is a rush to download it. Within three weeks of iOS 9 being released, over 60 percent of the Apple devices in the market were

running it. And one of the kickers is once you upgrade a mobile OS, there is no backing out of it. If it introduces an issue, you're stuck with it.

Mobile is just so different than what we've done in the past, and there are several steps that end users can take. And they are very basic:

- Use passwords and opt for more complex passwords;
- Don't use the same password across mobile apps;
- Use auto-locking features so that when you set down your phone, it locks fairly quickly;
- Don't click on a link to download apps, and only download apps from a reputable app store;
- Update your apps. Oftentimes the updates contain security patches;
- Delete apps that you aren't using. If you're not updating them and you're not using them, delete them.

Then there are a few things that are slightly more involved, like:

- Don't tamper with the device. Security measures are built into that device, and jailbreaking it or rooting it weakens that security;
- Be aware of the risks of public Wi-Fi. Save your banking for when you're on a secure network. It's just too easy for somebody to spoof a Wi-Fi network or a hotspot and see your information.

"There is no question that mobile is transforming how we live our lives, how we do business. But the question is: What are the benefits, and are we able to measure them?"

2016 Agenda

FIELD: Organizations clearly have budget for new investments, but as you say they seem committed to investing in just more of the same. Where do you recommend that they prioritize their spending to get beyond the basics and really get beyond the table stakes?

HARDY: When we developed the IBM mobile security framework, we wanted to convey the message that mobile security really doesn't have a linear approach that needs to be followed. Although protecting devices consistently is the top concern we hear from our customers, they should go into mobile with a plan to address the full spectrum of threats. Instead of taking an area and trying to make it bulletproof, look at the full range of threats and think about how you're going to address each of them to some extent.

There is a theory of "good enough security," which says my security doesn't have to be 100 percent, but it needs to be good enough that the fraudsters look elsewhere for an easier target. If you've already deployed an EMM solution, think about other areas. Think about how you're going to combat fraud and how you'll detect a device that is risky. Think about access and identity management and what you can do to make sure that the person behind the device that is asking for access has the appropriate credentials.

Take a layered approach to security. Don't keep investing more and more in the same area. Look across the spectrum; think about how you're going to address the full breadth of threats and make some investment in each area. And if it's not possible to hit everything in 2016, at least have a plan that says, "We're going into this with our eyes wide open."

Put Survey Results to Work

FIELD: How do we ask the audience to take these results and put them to work? How do they act on what we've given them in this survey?

HARDY: With 99 percent of respondents saying some portion of their workforce is using mobile to perform their job, it's obvious that mobile needs to be part of the overall security strategy. We're still early in adopting mobile within the enterprise, but our respondents indicate there are productivity gains to be had.

So, think about how you're going to embrace mobile. Think about your mobile security strategy holistically. Our survey follows the idea of a mobile security framework, which provides a blueprint for protecting devices, securing content and collaboration, safeguarding applications and data, and managing access and fraud. Look at the survey, and use this model to think about how you'll address the full range of threats.

Your strategy should take a comprehensive approach that delivers solutions to all of the mobile security threats. Think about the threats, but don't think about the threats as point threats and address them with point solutions. Make sure the solutions you plan to deploy are integrated and scalable. And when I say scalable, I'm talking about growing with your security needs, as well as growing with the volume of devices and apps that you deploy.

Bottom line: Think about your mobile security strategy holistically and have a long-term plan for "How am I going to deploy mobile and secure it over time?" ■

Establishing the Baseline

The report opens by taking the pulse of respondent organizations on the ubiquity of mobility within their organizations today. This information lays the groundwork for later conclusions about how mobile has transformed these enterprises.

Some opening statistics to consider:

- 96 percent of organizations currently support smart phones, while 77 percent support tablets;
- 86 percent support Apple iOS products vs. Google Android (77 percent)

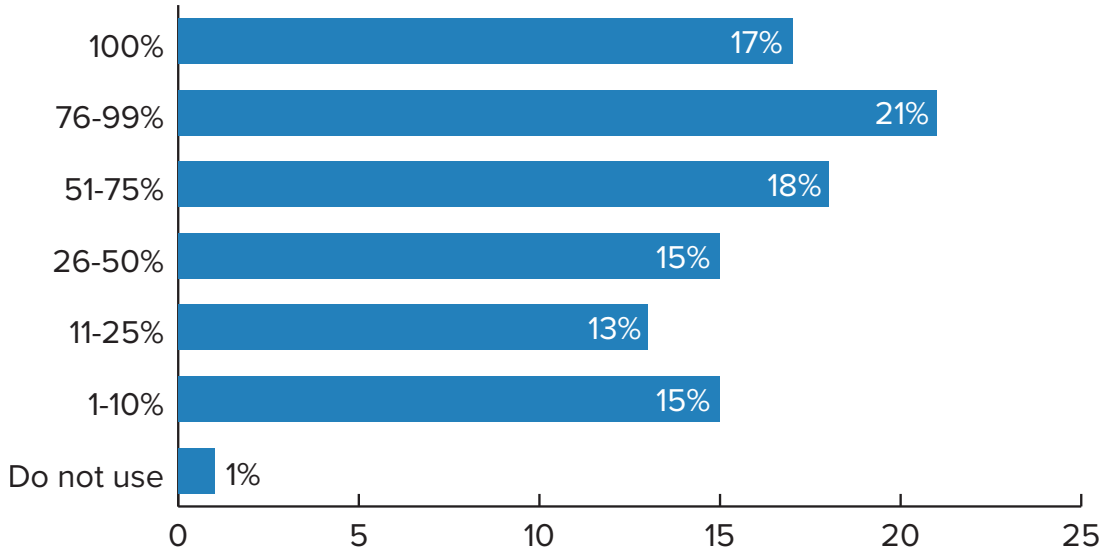
Read on for full baseline questions and results.

The only somewhat surprising note here is that 1 percent of organizations somewhere still do not have employees using mobile devices for work.

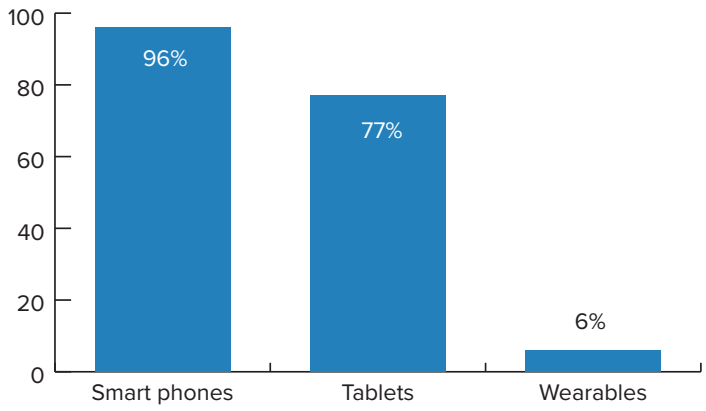
For the rest ... 38 percent of respondent organizations have more than three-quarters of their workforce on mobile devices, and another 33 percent place that figure at between one-quarter and three-fourths.

There is no question, then, about the expanding ubiquity of mobile devices in the workspace.

What percentage of your workforce uses mobile devices – specifically, smart phones and tablets – to perform their jobs today?



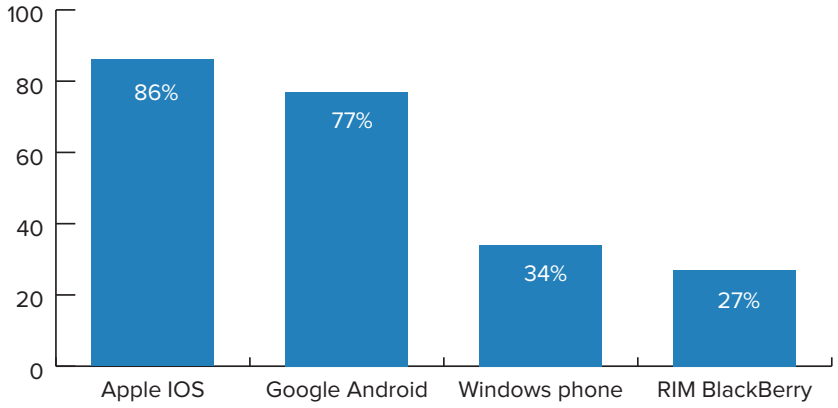
Which of these mobile form factors does your organization currently support? (select all that apply)



As for the types of mobile devices supported in the workspace, the vast majority are smart phones (96 percent), followed by tablets (77 percent). Wearables (6 percent) have not entirely caught on yet.

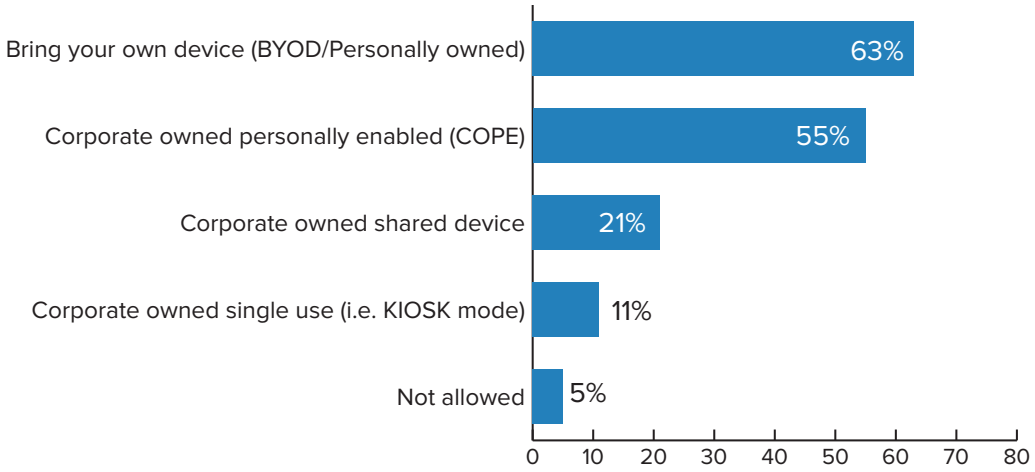
Apple iOS is supported by 86 percent of organizations, with Google Android placing second at 77 percent.

Which of these mobile platforms does your organization currently support? (select all that apply)



In past mobile surveys, Google Android devices were those of favor in the enterprise. But in this study, Apple iOS is supported by 86 percent of organizations, with Google Android placing second at 77 percent. The Windows phone has slipped by RIM BlackBerry for third place.

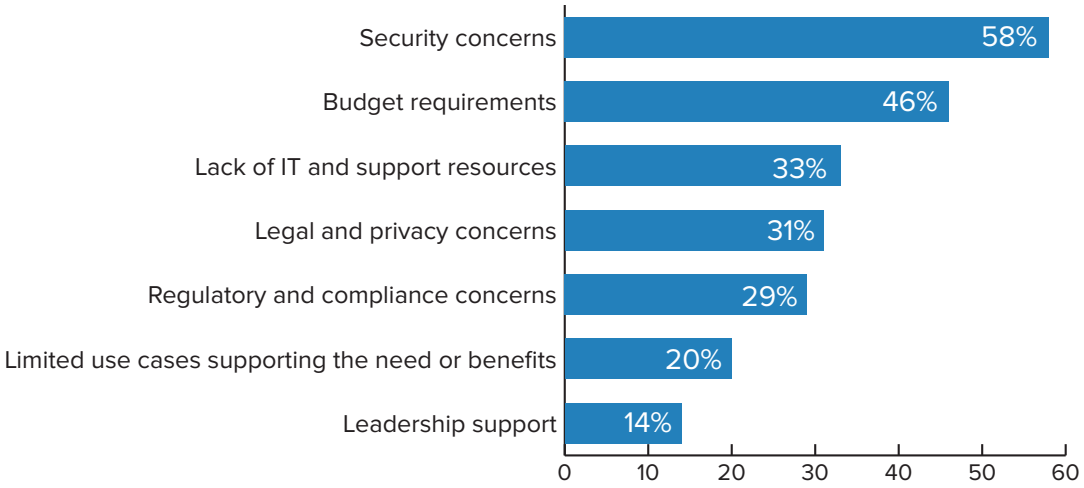
Which model has your organization chosen for deploying mobile devices? (select all that apply)



Can you remember when BYOD was even a debate within organizations? That conversation is for the most part over, and 63 percent of respondents say their enterprises support the bring-your-own model for deploying mobile devices.

There is no single answer for many organizations, of course, and so 55 percent of respondents also see the corporate-owned, personally-enabled model. Only 21 percent of respondents say their enterprises issue corporate-owned devices.

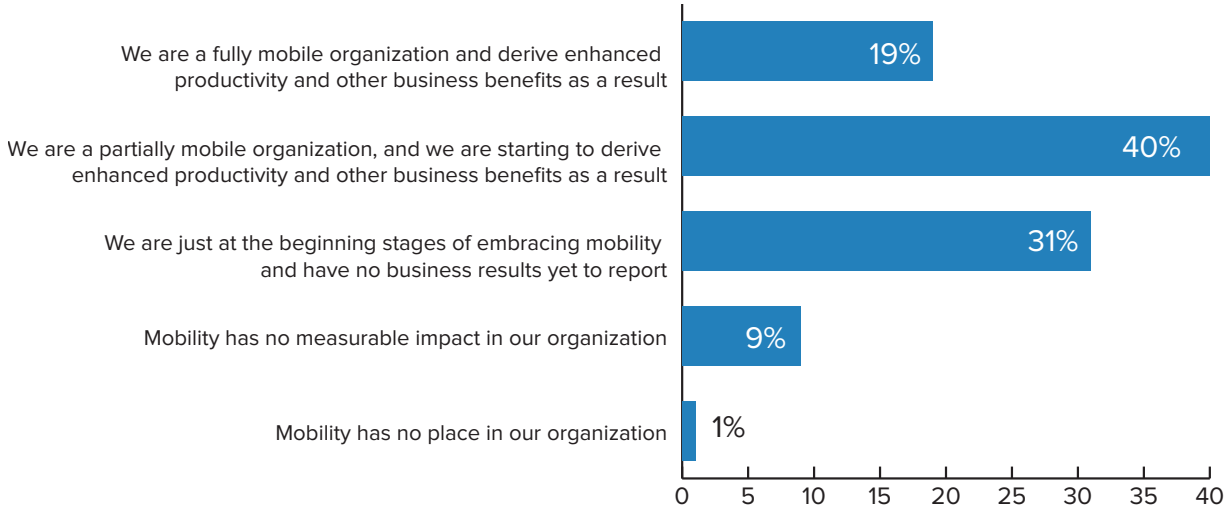
Which factors most inhibit your organization's full deployment of a mobile security strategy? (select all that apply)



And so, in an age of ubiquitous mobility, what factors still inhibit organizations from fully deploying a mobile security strategy? Security primarily, according to 58 percent of respondents.

Next on the list: budget (46 percent), lack of IT and support resources (33 percent) and legal/privacy concerns (31 percent).

How would you describe the scope and impact of mobility on your enterprise?



How mobile is "mobile?" The point of this study is to assess the degree to which organizations have been transformed by mobility. Step one is to determine the scope and impact of mobility. Toward that answer, 40 percent of respondents describe their enterprises as "partially mobile" and enjoying enhanced productivity and other business benefits.

Nineteen percent of respondents describe their enterprises as "fully mobile," while 31 percent say they are just at the beginning stages of embracing mobility.

Ten percent say either there is no measurable impact of mobility, or mobility has no place in their organization.

In the report's next section, responses will show the degree to which mobility has transformed enterprises.

Mobility may be near ubiquitous in some organizations, but that does not mean they are necessarily exhausting innovation from these devices.

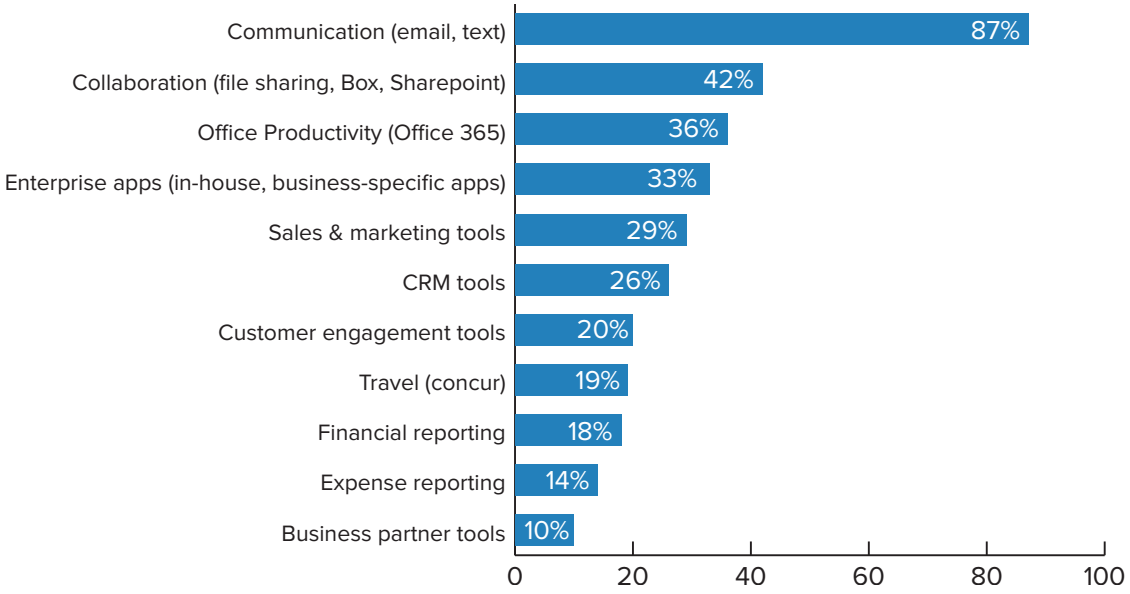
Mobile Transformation

It's one thing to ask respondents how mobility has transformed their organizations. The answers are likely to be subjective. But by asking specific questions, the responses provide a metric. That is the intent of this section of the report.

Some key statistics to consider upfront:

- 87 percent of respondents say communication apps are the top mobile apps they currently deploy.
- 92 percent of organizations are deploying these apps to employees; 31 percent to customers.

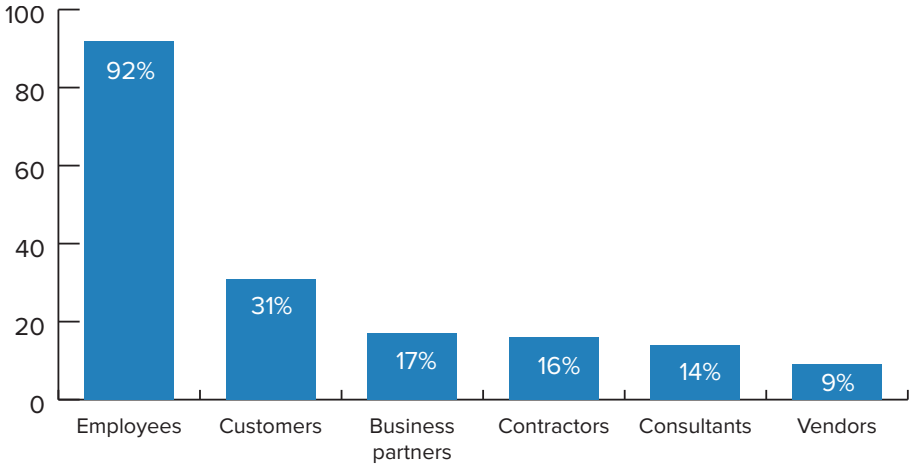
What kind of mobile apps does your organization currently deploy? (select all that apply)



Mobility may be near ubiquitous in some organizations, but that does not mean they are necessarily exhausting innovation from these devices.

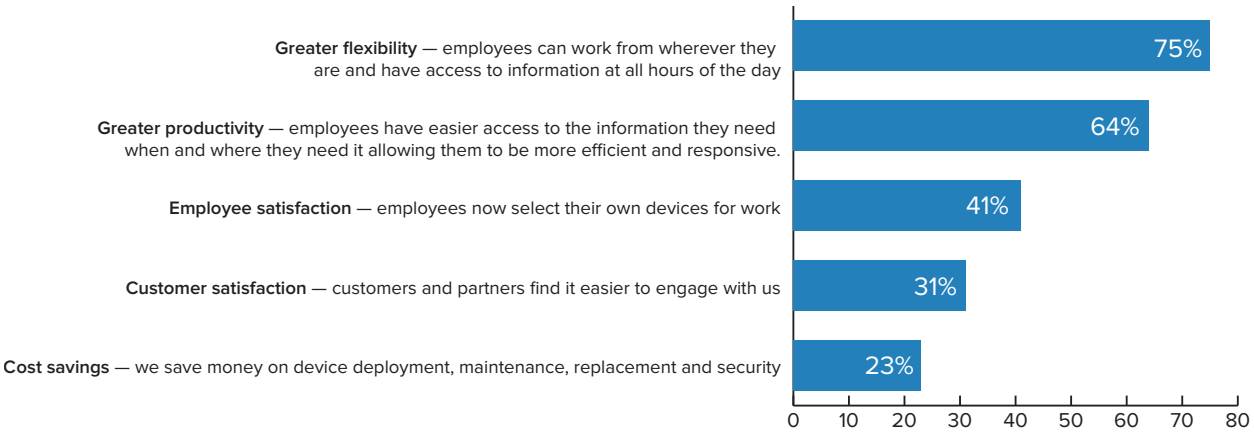
In fact, the most common mobile apps deployed are communication – email and text – by 87 percent of respondents. Next on the list, at 42 percent, is collaboration (file sharing), followed by office productivity (35 percent).

To whom are you deploying these mobile apps? (select all that apply)



For 92 percent of respondents, employees are the ones benefiting from these mobile apps. Thirty-one percent of organizations are deploying apps to customers, while 17 percent say they are deploying to business partners.

How has mobility transformed your organization? (select all that apply)

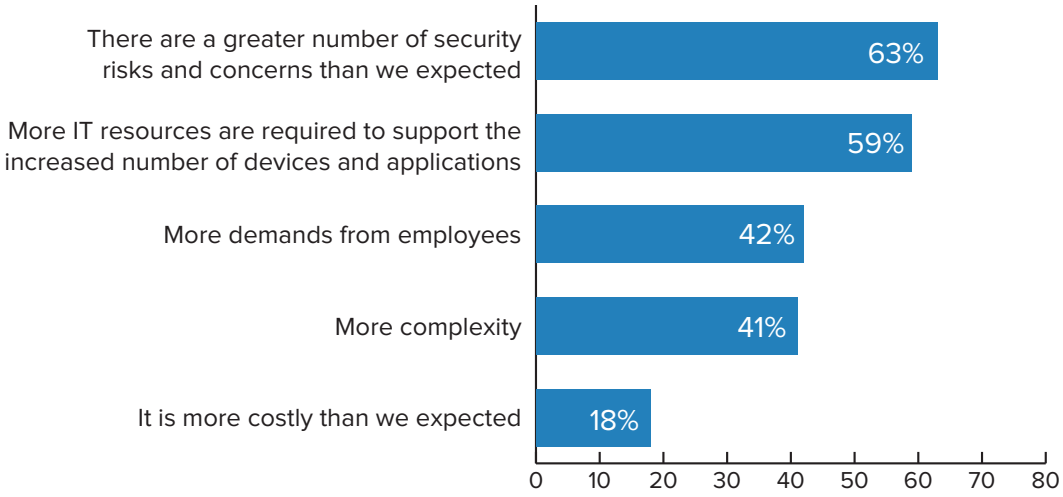


The big question: How has mobility transformed your organization?

For three-quarters of respondents, the answer is: Greater flexibility. Staffers now can work remotely and have access to all the information they need to do their jobs.

- For 64 percent, the answer is greater productivity.
- Forty-one percent cite employee satisfaction, while 31 percent claim customer satisfaction.
- Only 23 percent claim cost savings from mobility.

What specific challenges has mobility created for your enterprise? (select all that apply)



The inherent challenges of enterprise mobility are easy for respondents to list. And they begin with a greater number of security risks and concerns than expected, as cited by 63 percent of respondents.

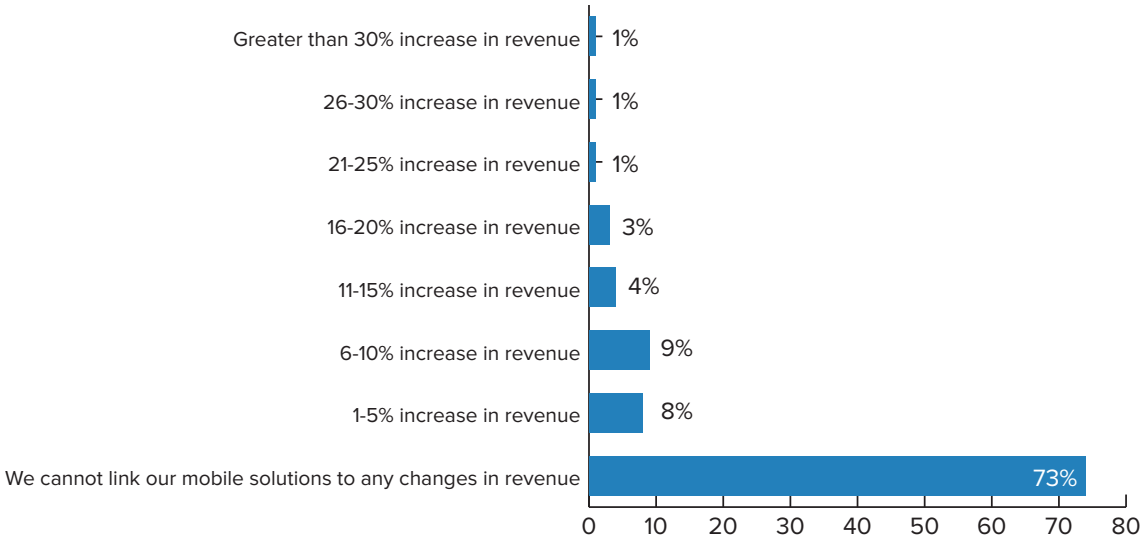
Fifty-nine percent say more IT resources are required to support the increased number of devices and applications.

Meanwhile, 42 percent see more demands from employees, while 41 percent cite an increase in complexity.

Since deploying mobile apps and access for my customers our organization has benefited in the following ways: (select all that apply)

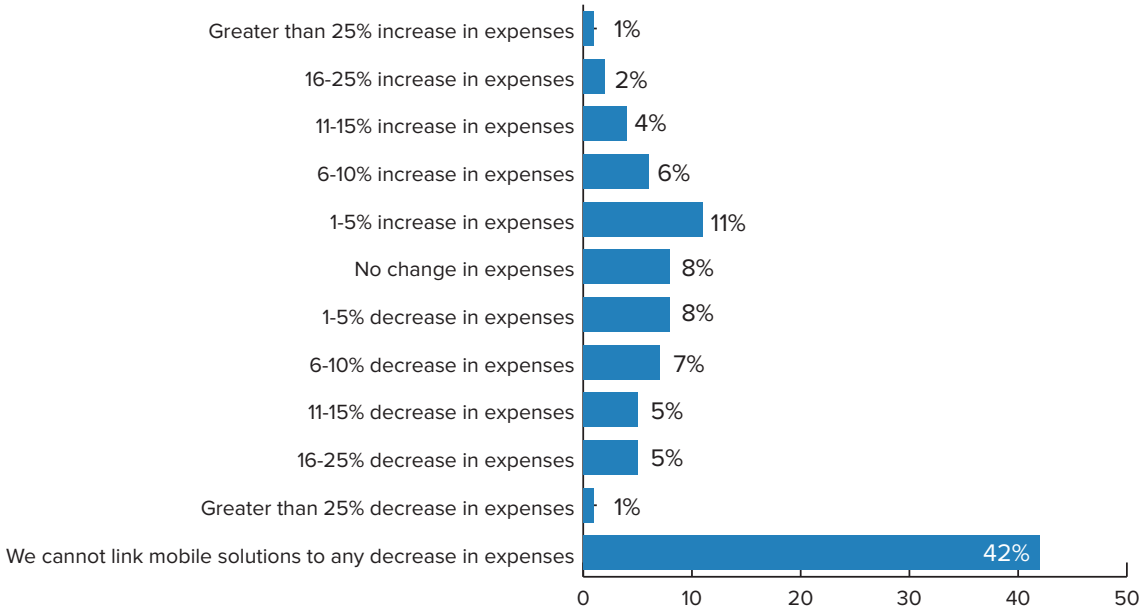
Talking specifically to organizations that have rolled out mobility to customers, respondents are asked to list benefits. Thirty-one percent say customer issues are now resolved in a shorter time frame. Meanwhile, about one-fifth claim three key benefits: a decrease in calls to customer service; an increase in self-service orders; and an improvement in customer feedback scores.

How has the deployment of mobile solutions impacted revenue?



But is there a bottom-line impact? Roughly one-quarter say they can link mobile deployment to anywhere from one to more than 30 percent increase in revenue.

How has the deployment of mobile solutions impacted expenses?



And 49 percent of respondents link mobile deployment to a decrease in expenses – anywhere from 1 percent to more than 25 percent.

In the next section, the report looks at some of the specific mobile security challenges that organizations face.

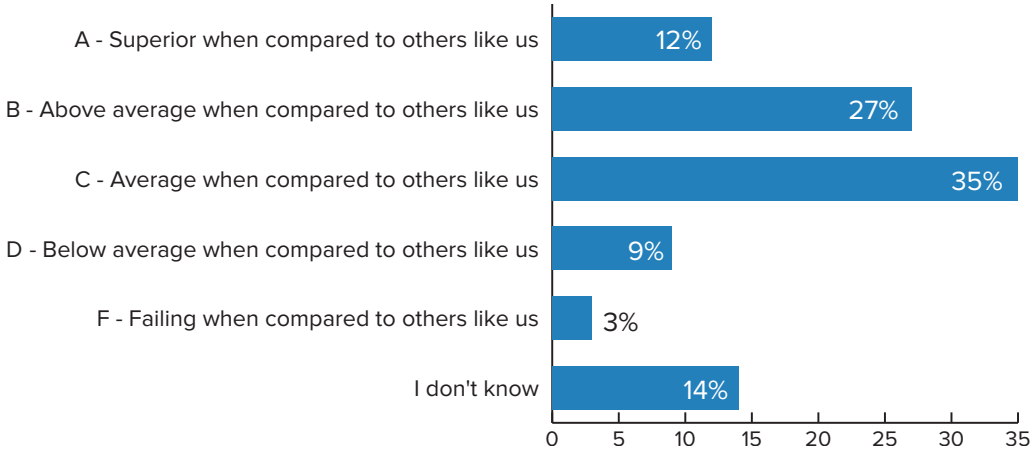
Roughly one-quarter say they can link mobile deployment to anywhere from one to more than 30 percent increase in revenue. And 49 percent...link mobile deployment to a decrease in expenses...from 1 percent to more than 25 percent.

Mobile Security

This section examines how organizations assess their current state of mobile security, as well as which controls they have deployed to improve their security posture. Among the key findings:

- 74 percent rate their current state of mobile security as average or above.
- Top mobile-related incidents in the past year:
  - » Data loss – 23 percent
  - » Malware detected on devices – 23 percent

How do you assess your organization's current state of mobile security in relation to other enterprises like yours?

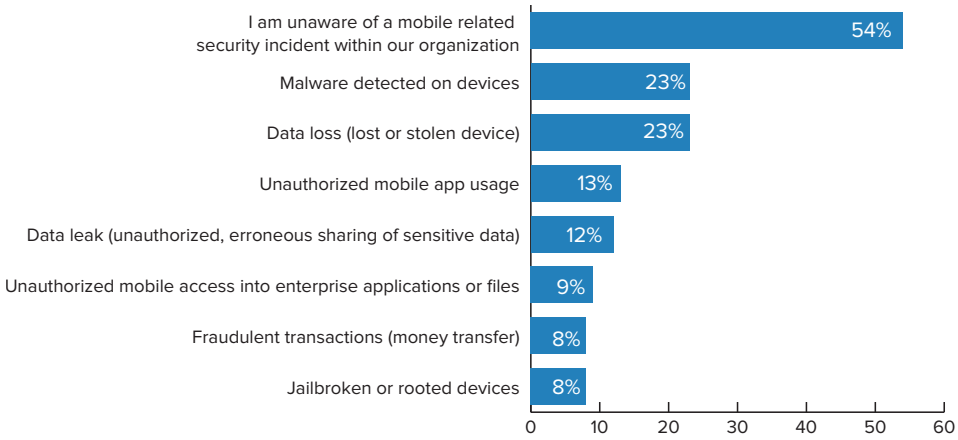


To start the security discussion, respondents are asked to benchmark against enterprises similar to their own. Upon doing so, 39 percent of respondents say their mobile security is above average or even superior.

Thirty-five percent consider their organizations average.

Only 12 percent rate themselves below average or failing, while the remainder don't know enough to make a fair assessment.

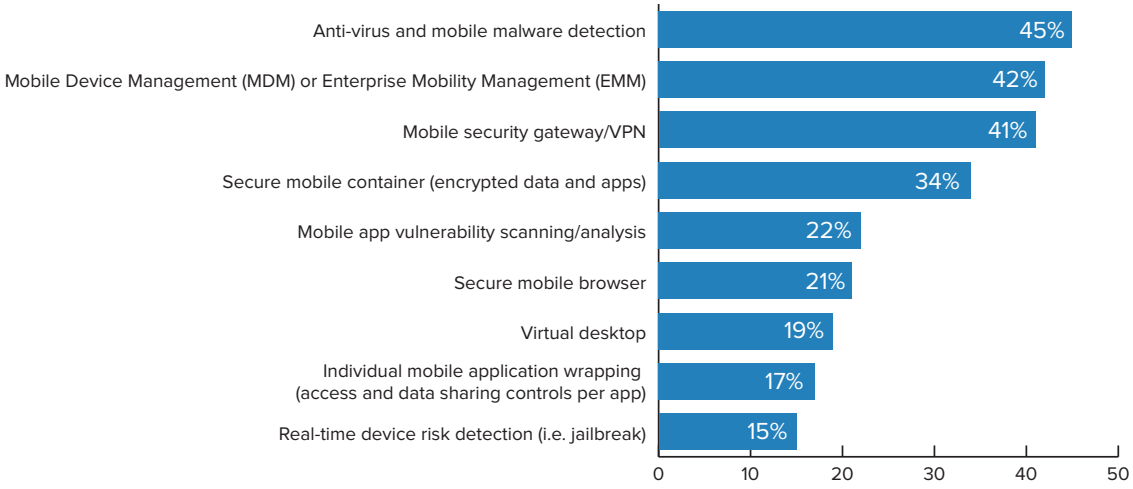
If your organization experienced a mobile-related security incident in the last year, what type of mobile security incident did you experience? (select all that apply)



More than half of respondents say they are unaware of any mobile-related security incidents impacting their organizations within the past year. Which doesn't mean such incidents didn't occur – simply that the respondents are not aware of them. Among those that do acknowledge such incidents, these are the most common:

- Data loss (lost or stolen device) – 23 percent
- Malware detected on devices – 23 percent
- Unauthorized mobile app usage – 13 percent

Which products/tools does your organization currently deploy for mobile security? (select all that apply)



It can be argued that mobile exploits continue to evolve in quantity and sophistication. But the controls leveraged for mobile security remain unchanged. Mobile device management and enterprise mobility management tools remain among the dominant controls. Forty-two percent of respondents say they currently deploy MDM/EMM, just slightly behind the 45 percent who deploy traditional antivirus and mobile malware detection tools.

Forty-one percent use mobile security gateways/VPNs, while 34 percent now use secure mobile containers for encrypted data and apps.

The next section moves beyond devices and delves into how organizations are providing secure content and collaboration via mobile.

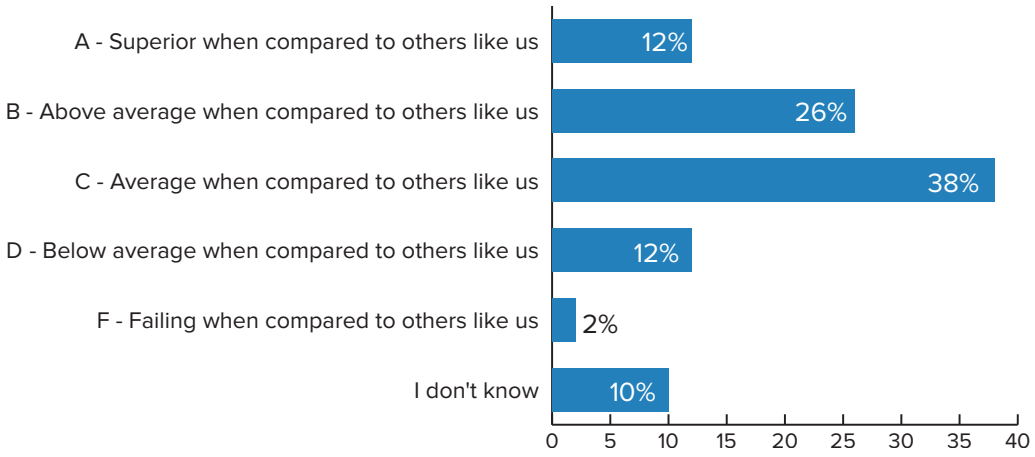
Secure Content and Collaboration

Just a couple of brief points covered within this subtopic:

- 38 percent of respondents assess their ability to secure content accessed/shared via mobile as above average or superior.

- Top means for securing content:
  - » Encrypted container – 40 percent
  - » Remote wipe – 40 percent

How do you assess your organization's current ability to secure content accessed and shared via mobile devices?



In recent years, enterprise security leaders have come to realize that mobile security is not so much about securing devices as it is about securing the content accessed via those devices.

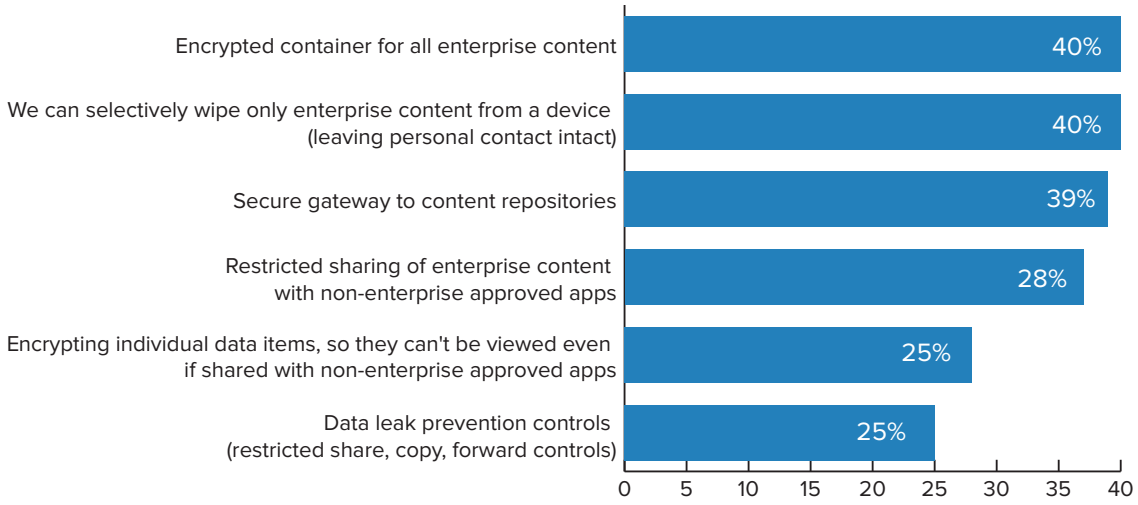
How are organizations faring at securing the content? It's a mixed bag:

- On one hand, 38 percent of respondents rate their organizations at above average or superior.

- But on the other, 38 percent also say they are just average when compared to similar organizations. Fourteen percent rate themselves below average or failing.

In recent years, enterprise security leaders have come to realize that mobile security is not so much about securing devices as it is about securing the content accessed via those devices.

Which capabilities does your organization employ to secure enterprise content accessed and shared via mobile devices? (select all that apply)



There clearly is no one way that organizations are securing content. It, again, is a mixed bag starting with encrypted containers and remote wipe, practiced by 40 percent of respondents. Other top controls:

- Secure gateways to content repositories – 39 percent
- Restricted sharing of enterprise content with non-approved apps – 37 percent
- Encrypting individual data items – 28 percent

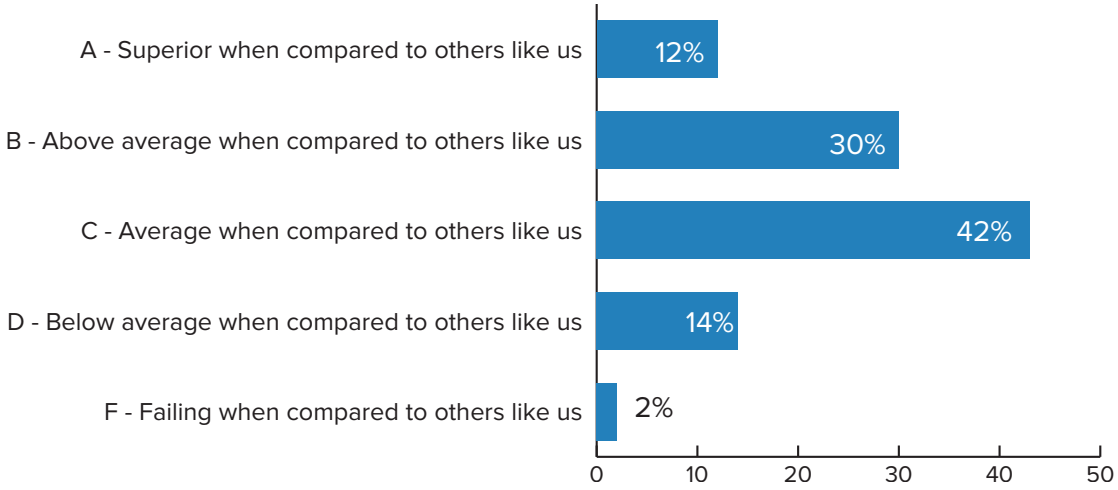
In the next section, the report focuses on application security.

Application Security

Top takeaways from questions focused on application security:

- 42 percent of respondents assess their organizations' mobile app security at above average or superior.
- Top means of enhancing app security: Whitelisting/blacklisting – 47 percent

How do you assess your organization's current mobile application security posture?



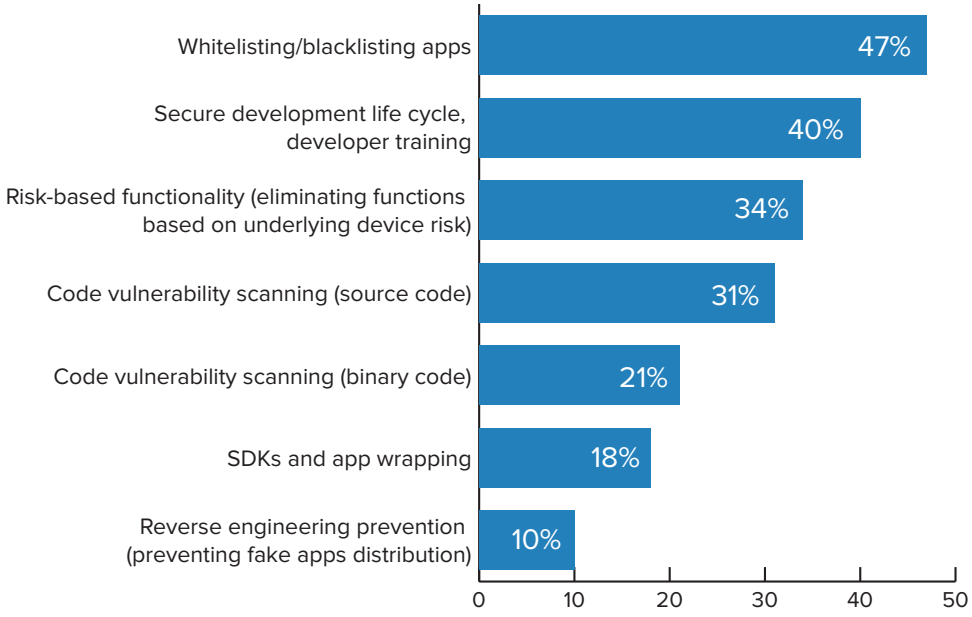
Similar to securing content, responses here are a fairly even mix. When asked to assess their organizations' mobile application security posture:

- 43 percent say they are average.
- Only 16 percent rate themselves as below average or failing.

The next response shows that organizations are not particularly progressive when it comes to mobile app security.

42 percent of respondents assess their organizations' mobile app security at above average or superior.

Which capabilities does your organization employ to enhance its application security posture? (select all that apply)



Of all the things enterprises could be doing to improve mobile app security, the most common ones they're employing are the basics:

- Whitelisting/blacklisting certain apps – 47 percent
- Secure software development lifecycle, developer training – 40 percent

Some of the more advanced means of application security have not taken root yet at most organizations, it seems.

In the next section, the results focus on managing access and preventing fraud.

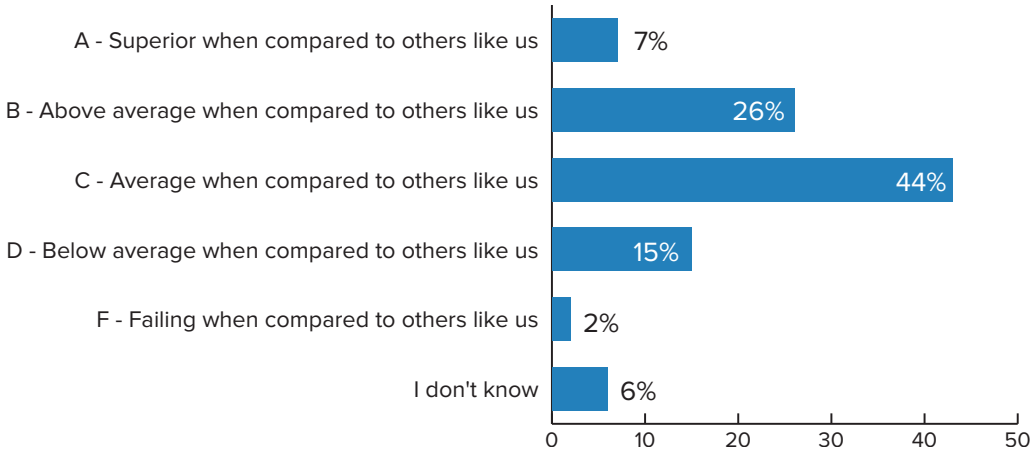
Manage Access and Fraud

Top points to bear in mind for context in this section:

- 33 percent rate their organization's ability to manage access and prevent fraud via mobility at above average or superior.

- Top forms of multifactor authentication:
  - » Single sign-on – 43 percent
  - » SMS one-time password – 37 percent

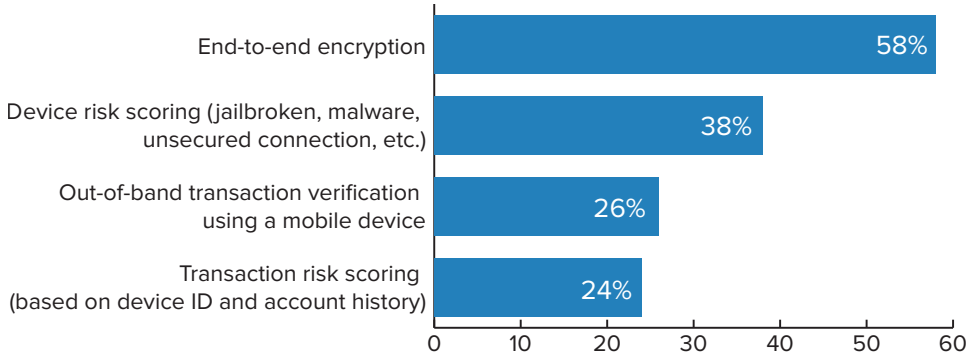
How do you assess your organization's current ability to manage access and prevent fraud via mobility?



Managing access to critical systems and preventing fraud via mobility are clearly a sore point with many organizations. Only 33 percent of respondents rate their abilities at above average or superior. Sixty-six percent rate themselves at average or below.

Managing access to critical systems and preventing fraud via mobility are clearly a sore point with many organizations. Only 33 percent of respondents rate their abilities at above average or superior.

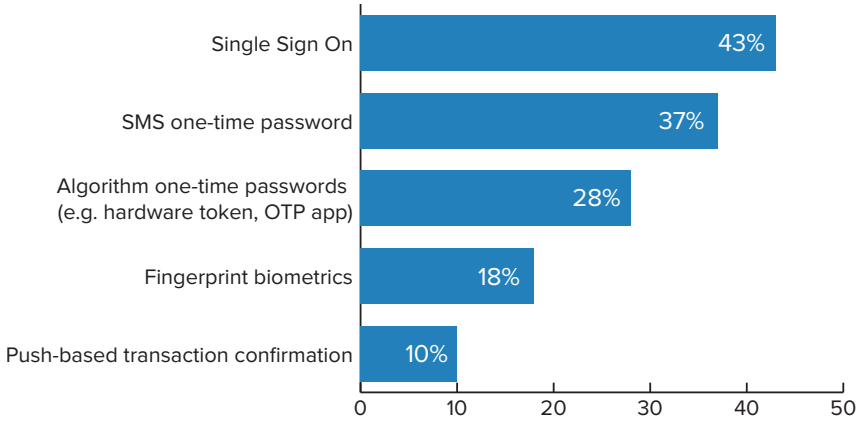
Which capabilities does your organization employ to secure mobile access and prevent fraud? (select all that apply)



It is encouraging to see nearly 60 percent of organizations employing end-to-end encryption as a means of securing mobile access and preventing fraud. Other key methods:

- Device risk scoring – 38 percent
- Out-of-band transaction verification – 26 percent

What type of multifactor authentication do you deploy for mobile users? (select all that apply)



Multifactor authentication commonly is employed for mobile users. The most popular methods:

- Single sign-on – 43 percent
- SMS one-time passwords – 37 percent
- Algorithm one-time passwords – 28 percent

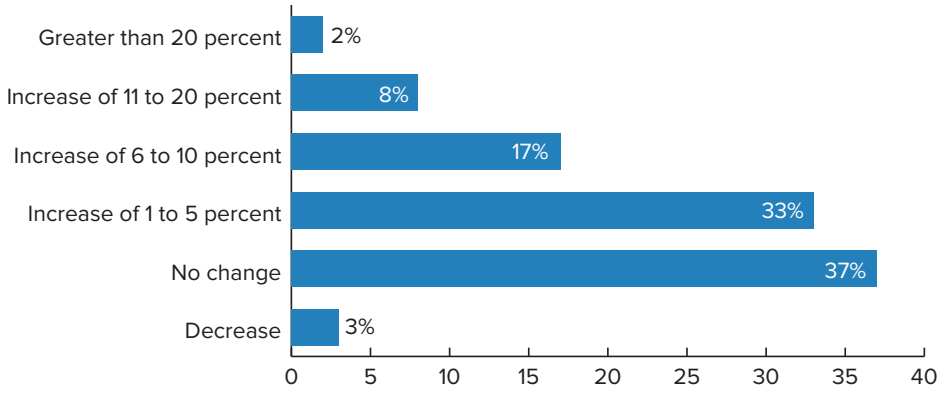
Next up: The 2016 mobile security agenda.

2016 Mobile Security Agenda

The most important points to know about resources available for mobile security in the year ahead:

- 60 percent of respondents expect a budget increase.
- Top projected investments:
  - » MDM or EMM – 38 percent
  - » Secure mobile container – 30 percent

How do you expect your budget dedicated to mobility to change in 2016?



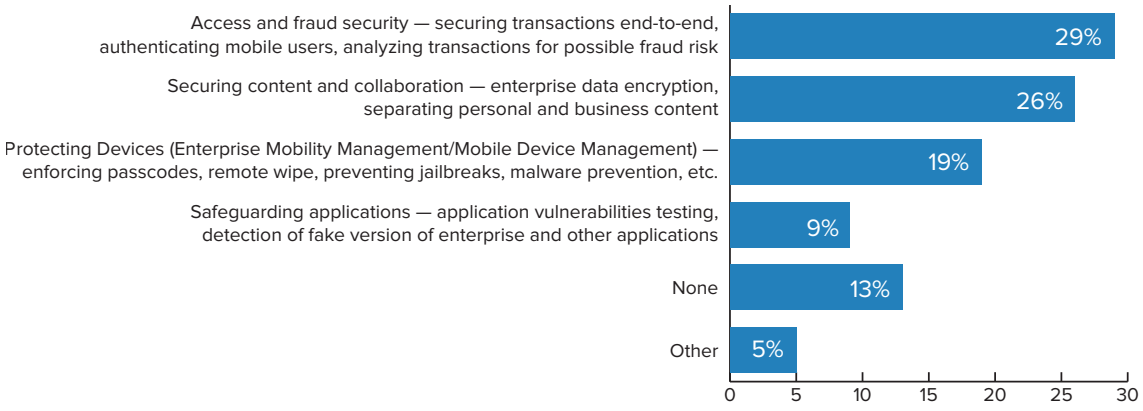
The important point is that only three percent of respondents envision a decrease in budget dedicated to mobility in 2016.

Which means 97 percent expect either level funding or an increase of anywhere from 1 to more than 20 percent. One-third expect increases of 1-5 percent.

Where will these funds be invested?

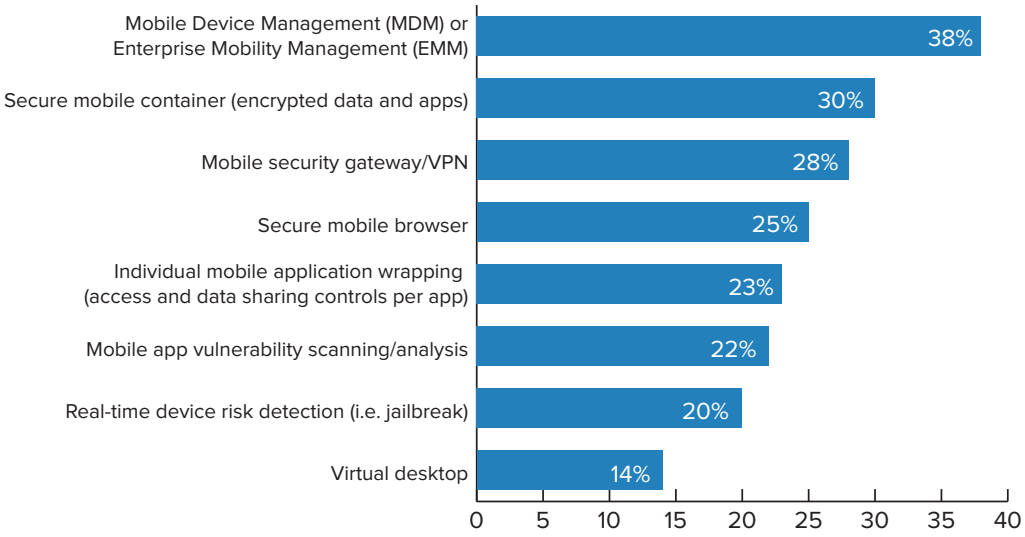
97 percent [of respondents] expect either level funding or an increase of anywhere from 1 to more than 20 percent. One-third expect increases of 1-5 percent.

Which of these mobility categories will be the main focus of your investments in 2016?



It's a close call. Twenty-nine percent of respondents say their main focus will be access and fraud security, while 26 percent will concentrate on securing content and collaboration.

Which specific products/tools does your organization plan to deploy to enhance mobile security in 2016? (select all that apply)



And as for specific tools to enhance mobile security, organizations say they are focused on more of what they already say they have:

- Mobile Device Management or Enterprise Mobility Management – 38 percent
- Secure mobile containers – 30 percent
- Mobile security gateways/VPN – 28 percent

In the next and final section, the report will present conclusions from the survey results, and then expert analysis – with an eye toward what the results mean, and how you can put them to work to improve your organization's mobile security.

Conclusions

Reflecting on the survey results provides the opportunity to take a broad view of enterprise mobility and realize how business transformation has begun. Nearly all enterprises now incorporate mobility in their work, and a majority now sees tangible business results from mobility. Organizations are seeing greater efficiencies and productivity from mobile workers.

But a majority of respondents also say that mobility comes with greater security risks and concerns than expected. These challenges have to be acknowledged and incorporated in mobile security plans for 2016 and beyond.

With the state of mobility – and mobile security – in mind, this survey report promotes these conclusions:

1. Business Transformation Has Just Begun

It is encouraging to see near mobile ubiquity in responding organizations. It no longer is a discussion of "if" when it comes to mobile. It's now firmly about "how." But for organizations to truly get beyond the mobility basics and transform how they conduct business, then they need to advance beyond simple messaging and content sharing on mobile devices. Currently, enterprises are focused mainly on extending communication apps to their employees. To get to the next stage, these organizations must extend mobility to customers and to partners, and they must envision innovative new ways to collaborate and conduct business. And as they scale up their business usage of mobility, organizations also must re-envision how they approach security.

2. Mobile Security: It's More Than Just Devices

To this point, enterprises largely have been focused on securing the smartphones and tablets they support, deploying new mobile device management and enterprise mobility management solutions. And these are important first steps. But it's time to acknowledge device security as just that – a first step. To truly advance along the mobile maturity scale, organizations must make greater investments in application security, content, collaboration and managing both access and fraud prevention.

3. More of the Same is Not a Strategy

The good news is that 97 percent of respondents expect to receive either the same or an increased budget for mobile security in the coming year. The bad news is: More than one-third of them expect to invest these resources in more of the same mobile device management and enterprise mobility management solutions they have been deploying. The point needs to be re-emphasized: The enterprise view of mobile security has to mature beyond mere device security. Organizations, then, need to start allocating more mindshare and funds to application security, content and collaboration, as well as managing access and fraud. Reinforcing what is already being done now will only freeze enterprises in a vulnerable state of arrested mobile maturity.

The road to true business transformation needs to be paved with enhanced mobile security. In the year ahead, enterprises have every opportunity to lay this critical foundational work.

Resources

Want to learn more about mobile security and how to fill the gaps?

Check out these content resources.

Apps attacking! Rogue devices! Business and personal worlds colliding! Are you missing all the warning signs? You and your business could have...mobilephobia! Unheard of just 10 years ago, mobilephobia is gripping security professionals around the world causing them to delay, stall and procrastinate from embracing and deploying a mobile security strategy. Don't despair, we have the cure!

Download the free e:guide "Curing the CISO's Most Common Mobile Security Fears"
https://ibm.biz/BdHdkD

Watch the on-demand webinar "Curing the CISO's Most Common Mobile Security Fears"
https://ibm.biz/BdHRz4

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401

sales@ismgcorp.com

BANK INFO SECURITY® CU INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com