iSMG
INFORMATION SECURITY
MEDIA GROUP

The State of Mobile Security Maturity

Findings from the ISMG Survey Sponsored by IBM

INSIDE:

- Complete Survey Results
- In-Depth Analysis
- Expert Commentary

Sponsored by

IBM®

From the Editor

2015: When Mobility Comes of Age

Tom Field
VP - Editorial
Information Security Media Group

We've been hearing for years now that mobile security threats are coming into their own, both in terms of volume and capacity to inflict harm.

And certainly we see plenty of evidence of evolving mobile malware strains and new exploits that focus on compromising mobile applications and data.

So, is it time for enterprise mobility to come of age? Is 2015 the year when organizations will move past their fundamental BYOD debates and start discussing more progressive mobile security topics?

That is the premise behind this Mobile Security Maturity Survey report. Inspired and sponsored by IBM, which has crafted a new Mobile Security Framework, this study focuses on the four key security pillars of IBM's structure: The device, content, applications and transactions.

With an eye toward the shape of mobile security in 2015, this study focuses on:

- Mobile Security Landscape – where are enterprises most vulnerable today?
- Maturity Level – at which stage of development are these organizations?
- 2015 Agenda – how will budgets grow, and where will priority investments be made?

It's a fascinating topic. Everyone is talking about mobile security, but not enough organizations are assessing and growing their mobile security maturity. Here's an opportunity to start that conversation and spark that growth.

Review the survey results and analysis, please, and share your reactions with me.

Best,

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

Table of Contents

Mobile Security Maturity Survey

Survey Results

Sponsored by

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Introduction

About the 2014 Mobile Security Maturity Survey

When you start the mobile security maturity discussion, you have to begin with the entry point – the device.

Even several years into the age of ubiquitous mobility, many large enterprises remain focused on securing mobile devices - and for good reasons. Lost or stolen devices remain the largest cause of mobile security incidents.

But the mobile security maturity level is increasing, as organizations now also turn their attention higher up the mobile food chain to content, application and transaction security.

And slowly, steadily the maturity level is increasing. This is the key takeaway of the 2014 Mobile Security Maturity Survey. Sponsored and guided by IBM, this study takes the mobile security pulse of large enterprises worldwide, helping them self-assess where they are on this emerging mobile security maturity scale, and giving us indications of where mobile security investments will be made in 2015.

IBM jumpstarted this survey with the development of its New Mobile Security Framework, which acknowledges the blurred line between personal and professional use of mobile devices, as well as the inherent risks enterprise mobility poses to data, applications and networks.

Among the topics addressed in this survey results webinar:

- **Mobile Security Baseline - An overview of today's mobile landscape, including device deployment and top threats;**
- **State of Mobile Security Maturity - How organizations self-assess their current level of device, content, application and transaction security;**
- **2015 Agenda - Specific technology investment targeted for the year ahead.**

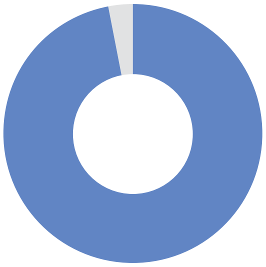
The survey was developed by the editorial staff of Information Security Media Group, guided by Yishay Yovel, Program Director, Mobile and Fraud Strategy, IBM Security Systems.

This survey was conducted online during the summer of 2014. More than 200 respondents participated in this international study. Key characteristics of the respondent base:

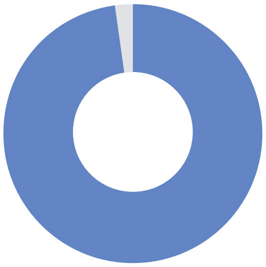
- Respondent organizations were limited to those with 500+ employees;
- 59 percent percent are from the U.S.;
- 35 percent have $1 billion+ in annual revenue.

Hard Numbers

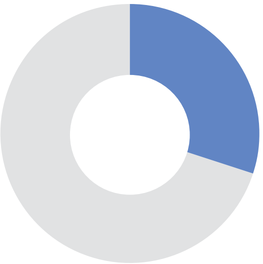
Among the statistics that jump out from the survey results:



97% say some portion of workforce uses mobile devices in their jobs today;



98% expect level or increased mobile security budgets in 2015;



30% say device management is their top investment priority.

Mobile Security Maturity Survey: IBM Perspective

By Yishay Yovel

At the beginning of 2014, IBM defined its Mobile Security Maturity Framework.

It is a holistic approach to securing the four pillars of enterprise mobility: the device, the enterprise content stored on it, the mobile applications used for employee productivity and the transactions generated by the device to enterprise resources. The framework incorporates the notion of BYOD, namely the blend of personal and enterprise use of the same device and how it impacts the security of sensitive enterprise data and resources.

In this study, we set to explore, with the help of ISMG, how enterprises view mobile security risks, what capabilities they are currently deploying vis-à-vis the four pillars of the framework and what their short-to-medium-term plans are to extend these capabilities. We called this "the path to mobile security maturity."

What we found indicates that enterprises are "halfway there."

Naturally, there is continuous focus on the foundational pillars: device and content security. Enterprises are still facing the risk of data loss from a stolen device, and the use of enterprise mobility management suites help address that scenario. We expect that in the next 18-24 months virtually all enterprises will have some form of an EMM deployed to ensure mobile devices - BYOD or corporate-owned - conform to their policies before allowing access to enterprise resources. And that such content can be selectively wiped out or protected if a device is lost or stolen.

Yishay Yovel

The next big challenge that our respondents are tackling is the development of secure enterprise applications. Here, the need to establish a secure application development lifecycle has been inherited from the existing paradigm of secure Web development. A subset of the respondents are using vulnerability scanning tools for their app source code, while a smaller subset does so for binaries (third-party or even public apps). Since mobile applications are a critical vehicle for accessing enterprise data, it is clear that ensuring these applications are vulnerability free is a critical capability for enterprise that want to realize the benefits of mobility while reducing exposure to malware and other attacks.

Finally, the transaction security layer is seeing less of a focus from our respondents. Transaction risk is related to all interactions between the mobile device and the backend system, accessing the network, login and access of data and services. In the context of customer access, some enterprises need to apply transactional risk mitigation for financial transactions. At this juncture, many enterprises deploy end-to-end encryption that is effective against man-in-the-middle attacks on transactional activity. To effectively protect transactions, enterprises will have to consider underlying device risk and user access patterns to determine the business exposure associated with specific sessions and interactions. This can help detect account takeover and fraudulent transactions before the enterprise data and customer assets are exposed.

Enterprises are still facing the risk of data loss from a stolen device, and the use of enterprise mobility management suites help address that scenario.

To summarize, it seems that our respondent are aware of the different requirements to secure their mobile initiatives and are on their way to building a comprehensive mobile security program. The IBM mobile security framework offers a viable roadmap for thinking and implementing such a program.

For more information visit: http://ibm.com/security/mobile/

Yishay Yovel is Program Director, Mobile and Fraud Strategy, IBM Security Systems.

The Mobile Security Baseline

In this section, we establish our mobile security baseline. What are the current investments and perceived vulnerabilities? Among the key points to consider:

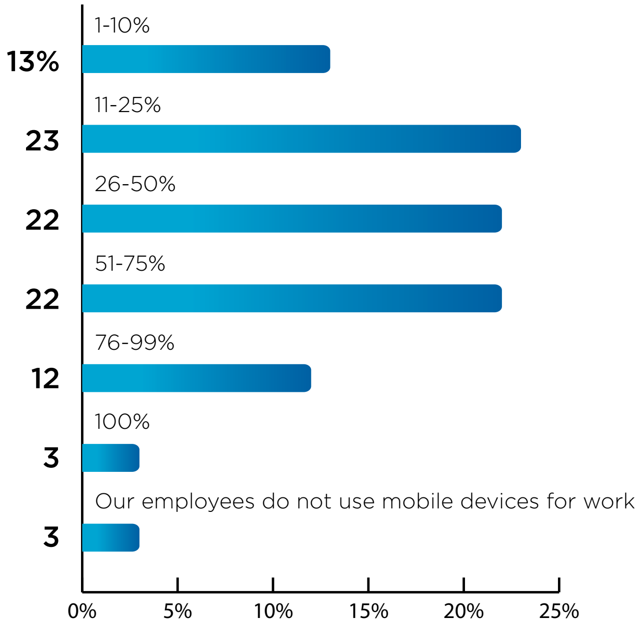
» 43 percent of respondents say device management is where security falls short;

» 32 percent says lost/stolen devices are leading cause of mobile security incidents.

Only three percent of organizations say their employees do not use mobile devices in their jobs today.

Key findings:

What percentage of your workforce relies on mobile devices to perform their jobs today?

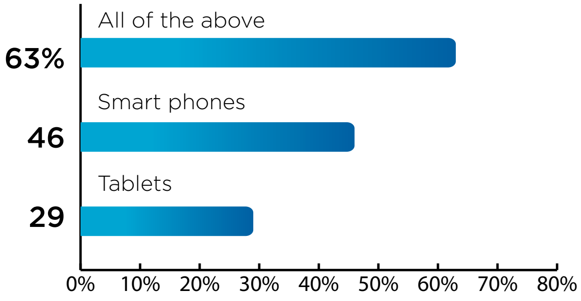


It's the smallest number that speaks loudest: only three percent of organizations say their employees do not use mobile devices in their jobs today. That is a strong statement when you realize that only a few years ago, we all were just coming to grips with the then-new term BYOD.

As the chart shows, at most organizations, 25 percent of employees or more rely on smart phones and tablets in their work, and we know that increasingly more critical work functions are passing through these devices, putting a heightened burden on security controls.

Subsequent survey findings show us more about the current mobile landscape.

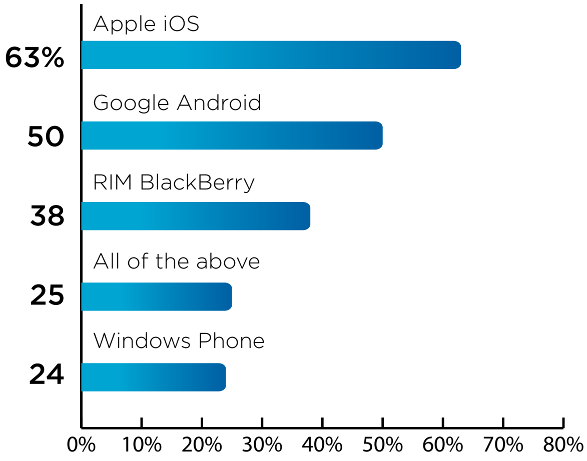
Which of these mobile form factors does your organization currently support?



How many mobile devices do any of us have close at hand at a given time? Two, three, four? Laptops, smart phones, tablets? We are increasingly multiple-device individuals, and our businesses reflect our diversity.

So, while smart phones might be the dominant device in the marketplace, with nearly half of respondents saying their organizations support them … 63 percent support the smart phone/tablet combination.

Which of these mobile platforms does your organization currently support?

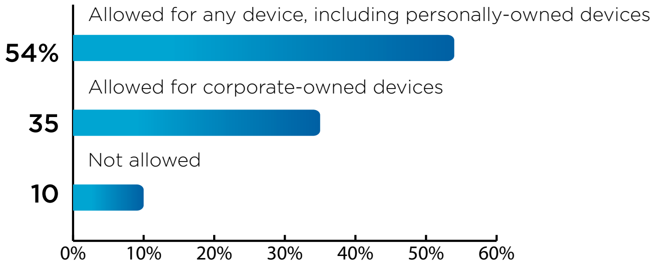


Google Android might rule the consumer market, but in the large enterprise it's Apple iOS that is king – and this question was asked before the latest upgrade to Apple devices and operating system.

Interesting to note: BlackBerry still retains significant marketshare, and the Windows phone has presence, too.

Most significant: A growing shift from single-platform shops. Whereas just a couple of years ago, many organizations were trying to enforce standardization on a single mobile platform, 25 percent of our respondents say they now support all platforms.

What is your stance on using mobile devices both for personal and business purposes?

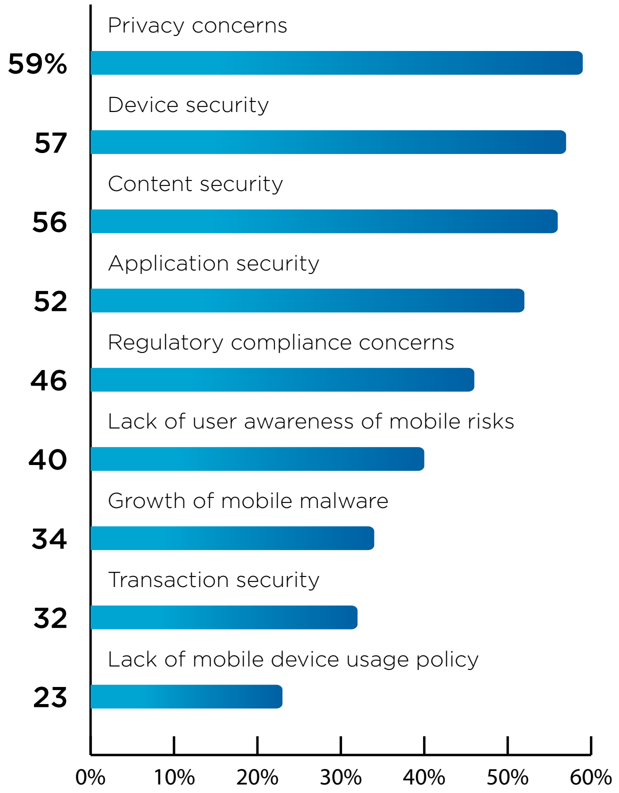


Here's where the mobile discussion gets personal: Do organizations allow employees to mix business with their personal activities?

Recognizing a losing battle – trying to maintain separation - 90 percent of respondents allow for some mix of personal and business on mobile devices. More than half open the doors altogether.

But a dwindling 10 percent still attempt to legislate strict boundaries that users, frankly, don't recognize or acknowledge.

Which factors most inhibit your organization's full deployment of a mobile workforce?

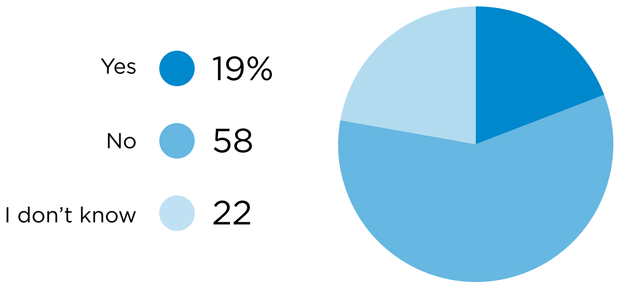


So, why don't all enterprises support a fully-equipped mobile workforce? What are the remaining barriers keeping these organizations from making the full leap?

The top three inhibitors are privacy, device security and content security – two of which are subtopics of this study. Organizations are clearly concerned about the risk of breach – and with good reason. In healthcare alone, lost/stolen mobile devices are the top form of breach to organizations.

How realistic is fear of breach, given organizations' recent experiences?

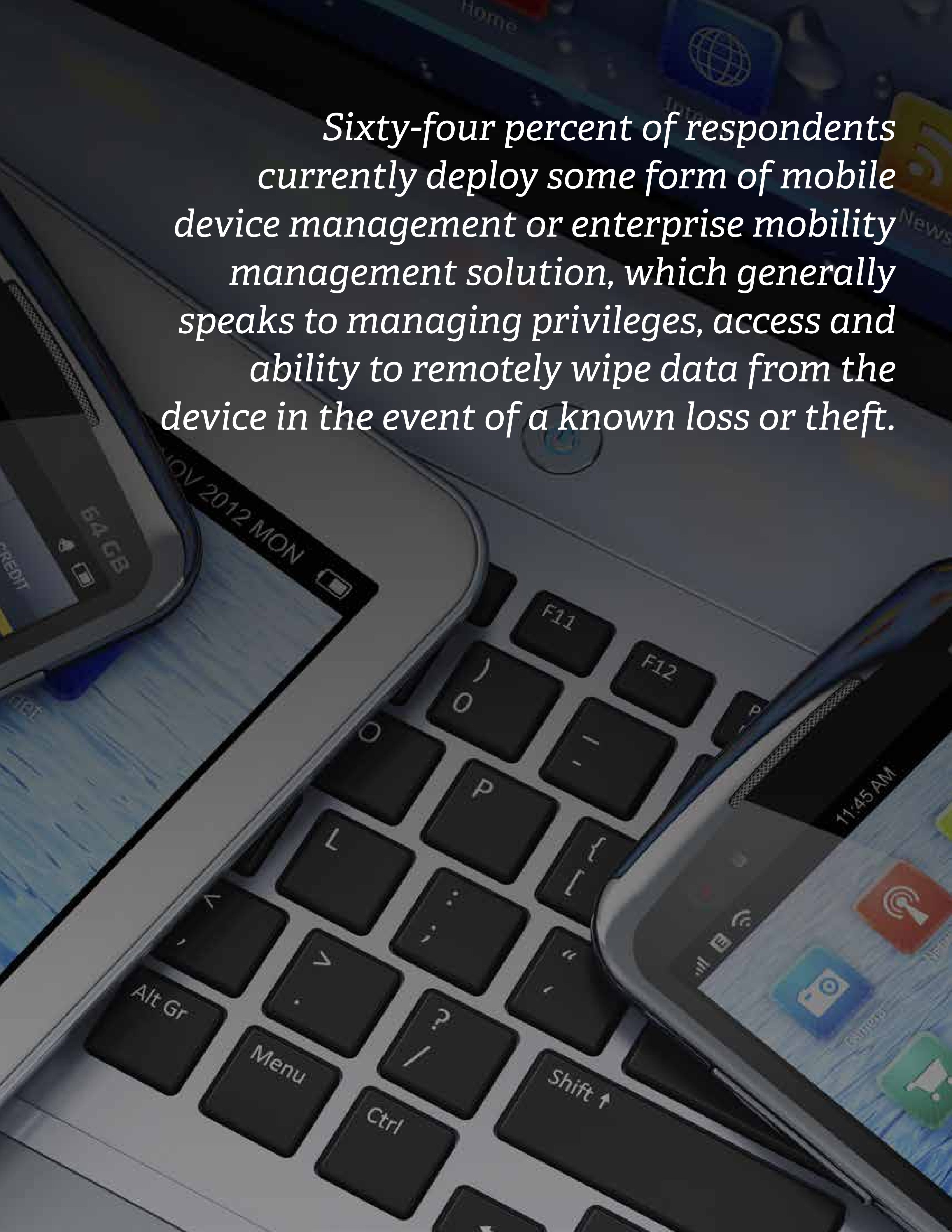
Has your organization experienced a mobile-related security incident in the past year?



Well, on one hand we have 58 percent of organizations saying they have not had a mobile security-related incident in the past year.

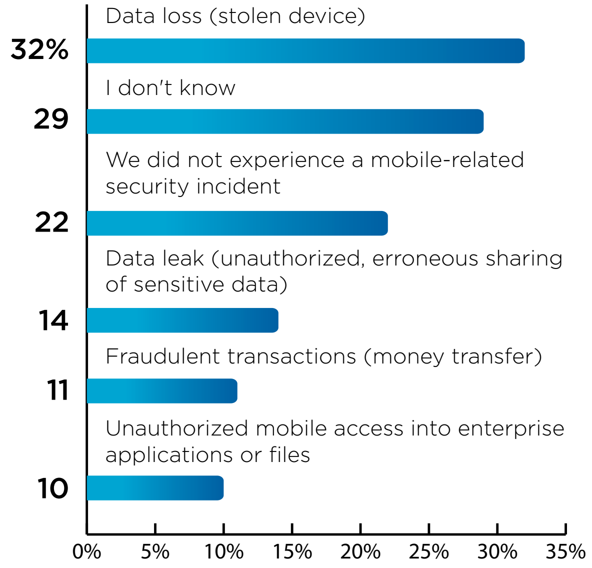
But nearly one-fifth have suffered such an incident, And nearly one-quarter say they do not know, which is a distressing statistic by itself.

For those that did suffer an incident, what was the cause?



Sixty-four percent of respondents currently deploy some form of mobile device management or enterprise mobility management solution, which generally speaks to managing privileges, access and ability to remotely wipe data from the device in the event of a known loss or theft.

What type of mobile security breach did your organization experience?

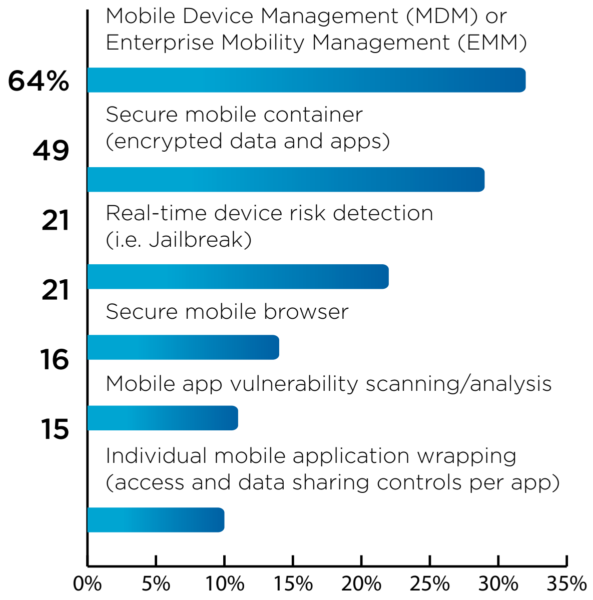


No surprise. Stolen devices head the list of factors behind these incidents – and by a large margin. This is consistent in industries such as healthcare that track and report breach incidents and causes.

Other significant causes: data leakage, unauthorized access to sensitive data; fraudulent transactions.

With incident stats in mind, let's turn to the current deployment of security controls in our surveyed enterprises.

Which products/tools does your organization currently deploy for mobile security?

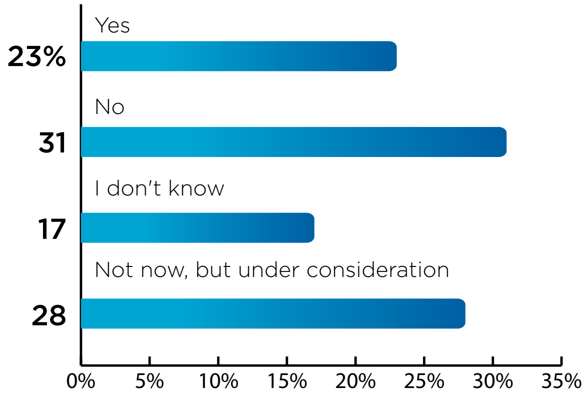


Once again, it comes back to the device.

Sixty-four percent of respondents currently deploy some form of mobile device management or enterprise mobility management solution, which generally speaks to managing privileges, access and ability to remotely wipe data from the device in the event of a known loss or theft.

Other controls that speak to more heightened levels of mobile maturity (read: beyond device security): secure mobile containers, protecting encrypted data and apps; and at least some level of secure mobile browsers and real-time device risk detection (to help protect against vulnerabilities caused by jailbroken devices).

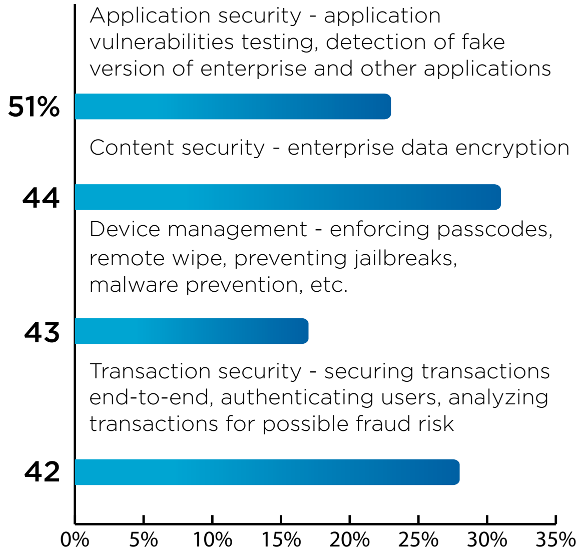
Do you deploy analytics tools to help detect mobile security threats and identify vulnerabilities?



Here we probe a bit for some more advanced security controls and find that most enterprises do not currently deploy these tools. Nearly one-quarter of respondents do, and more than one-quarter are at least considering this level of threat detection.

One final baseline question about mobile security:

Where do you believe your organization's mobile security controls fall short?



Looking at the fundamental elements of mobile security maturity, where do organizations believe they fall short?

Application security earns the top spot here, with more than half of respondents saying they don't measure up in areas such as vulnerabilities testing and detecting fake versions of enterprise apps.

Content security and transaction security also fall short – which is to be expected by organizations still focusing so heavily on securing their devices.

But even 43 percent of respondents say basic device security – malware prevention, remote wipe and enforcing passcodes – remains a significant challenge. This despite evidence that many organizations have, to this point, focused intently on this fundamental level of mobile security maturity.

Next we're going to explore responses to some more granular questions about the specific elements of mobile security.

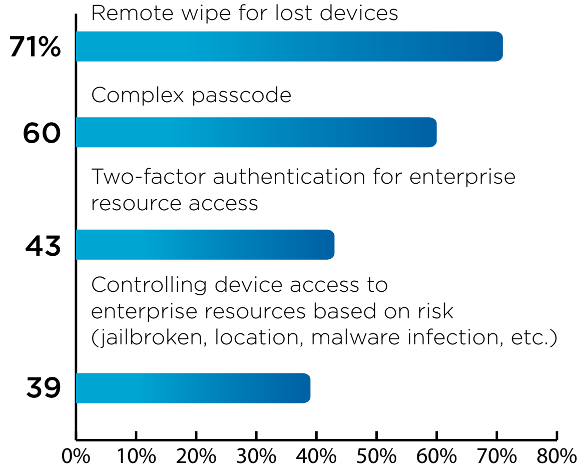
As we said from the outset, we view mobile maturity as a journey that begins with securing the device and ascends to the transaction.

Looking at the fundamental elements of mobile security maturity, where do organizations believe they fall short?

In crafting this survey, we honed a handful of specific questions to cut to the core of each of these security elements: device, content, applications and transactions.

Let's start with the device.

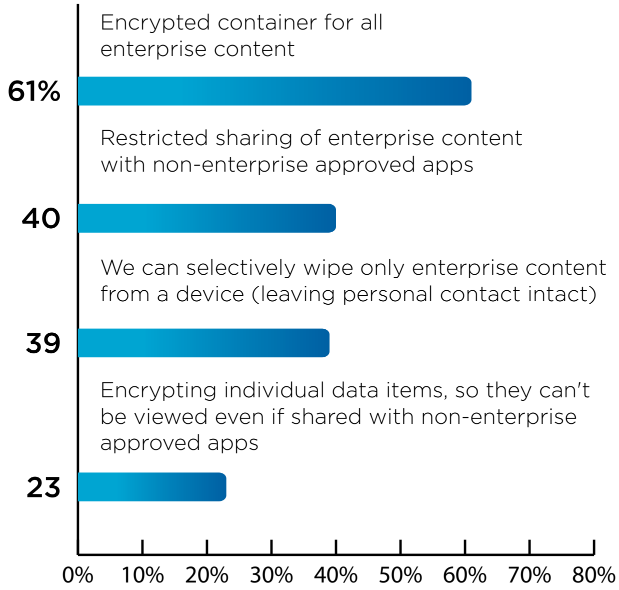
Which policies does your organization enforce to secure mobile device usage?



So much of device management comes back to policy, so we ask not just which policies enterprises post, but which ones they enforce. Clear winners: remote wipe for lost devices (which truly is tablestakes today) and complex passcode for users.

You see less emphasis on key security elements such as multifactor authentication and risk-based access to enterprise resources.

Which capabilities does your organization employ to secure enterprise content on a mobile device?



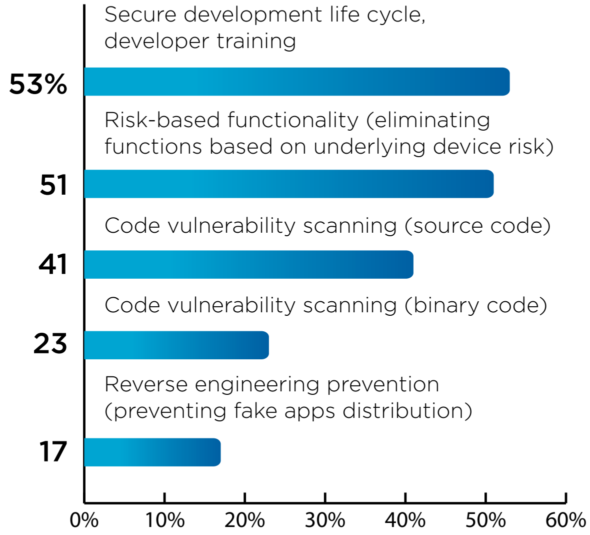
Turning to content security, we ask about the fundamental controls for securing data on the device.

Here we see 61 percent of respondents embracing the practice of a secure, encrypted container for all enterprise content (separating it from personal).

But again there's significant distance between the top response and the second – restricted sharing of enterprise content with non-approved apps, which earned only 40 percent of response.

The implication, which we'll explore in our analysis, is that content security is a growing concern within enterprises … but the actual practice is lagging.

Which capabilities does your organization employ to enhance its application security posture?



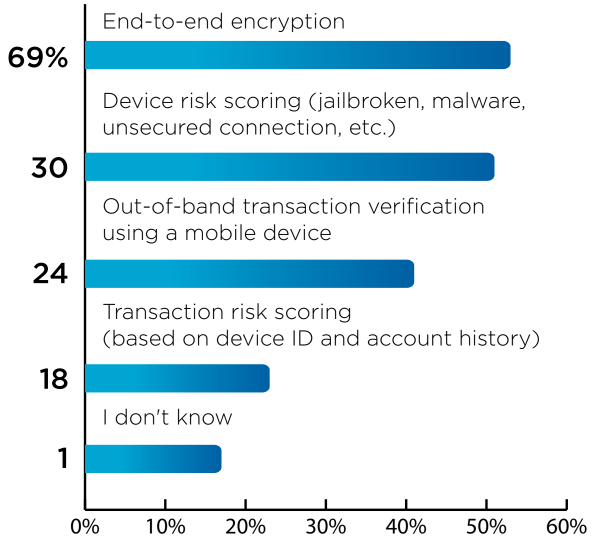
Application security is a hot topic in the marketplace, and many security leaders are embracing the notion that this discipline has matured at a far slower pace than have threats to enterprise apps.

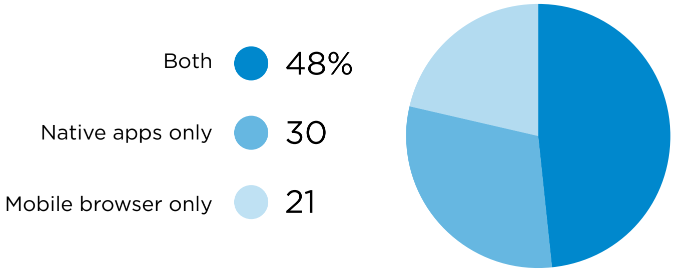
For too long, security has been a secondary consideration to the business need for speed –produce and deploy the app quickly.

It is encouraging, then, to see that 53 percent of respondents feel their organizations follow the secure software development lifecycle, and just under that amount practice risk-based functionality, eliminating functions based on the underlying device risk we discussed earlier.

Code vulnerability scanning gets slightly less priority, and fewer than one-fifth of respondents are doing any reverse-engineering prevention, barring fake apps from being distributed.

Which capabilities does your organization employ to secure mobile transactions?





Transaction security gets two questions in the survey.

In the first, we ask about fundamental capabilities and learn that 69 percent of respondents employ end-to-end encryption to protect mobile transactions. But other measures such as device risk scoring, out-of-band verification and transaction risk scoring gain far less traction.

Next, we ask about security deployed for native apps and mobile browsers. You can see the results: nearly half of respondents apply security to both; whole native apps earn 30 percent of the vote, and mobile browser wins 21 percent.
The message here is that while organizations clearly recognize the need for enhanced transaction security, the practice has not quite caught up to the need.

This is the level of maturity that must be tracked in the months ahead.

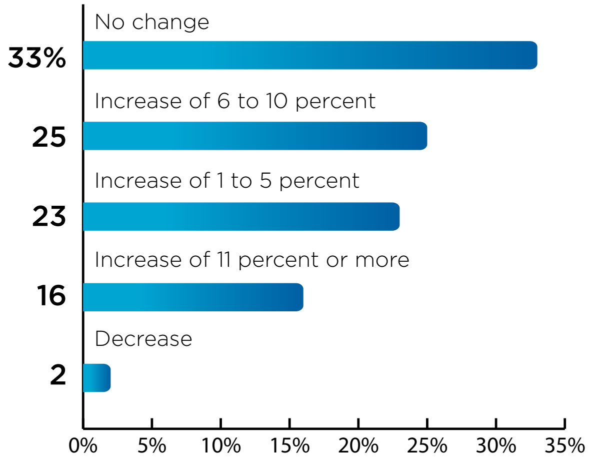
All told, about one-third of respondents expect level funding in 2015, but the rest believe they will see increases of anywhere from 1-5 percent, 6-10 percent or 11 percent-plus.

Here, having assessed the current state of mobile security and maturity, we take a look at 2015 – what is the expected budget, and what are the likely investments?

Good news here:

- **64 percent of respondents expect budget increase**
- **Top targets for investment:**
  - **48 percent MDM or EMM solution**
  - **37 percent Secure container**
  - **35 percent Real-time device risk detection**

How do you expect your budget dedicated to mobile security to change in the coming year?



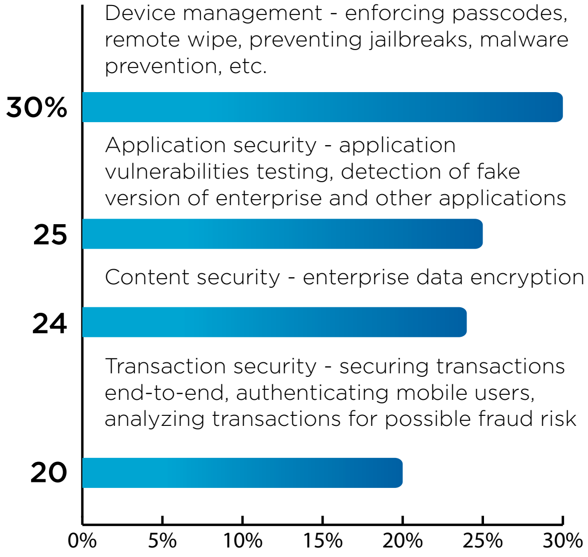
Starting with budgets, it's always a good year when the budget is expanding. And the mobile security budget looks expansive indeed.

Start with: only two percent of respondents expect a budget decrease in the coming year.

All told, about one-third of respondents expect level funding in 2015, but the rest believe they will see increases of anywhere from 1-5 percent, 6-10 percent or 11 percent +.

Given the resources, how will they be spent?

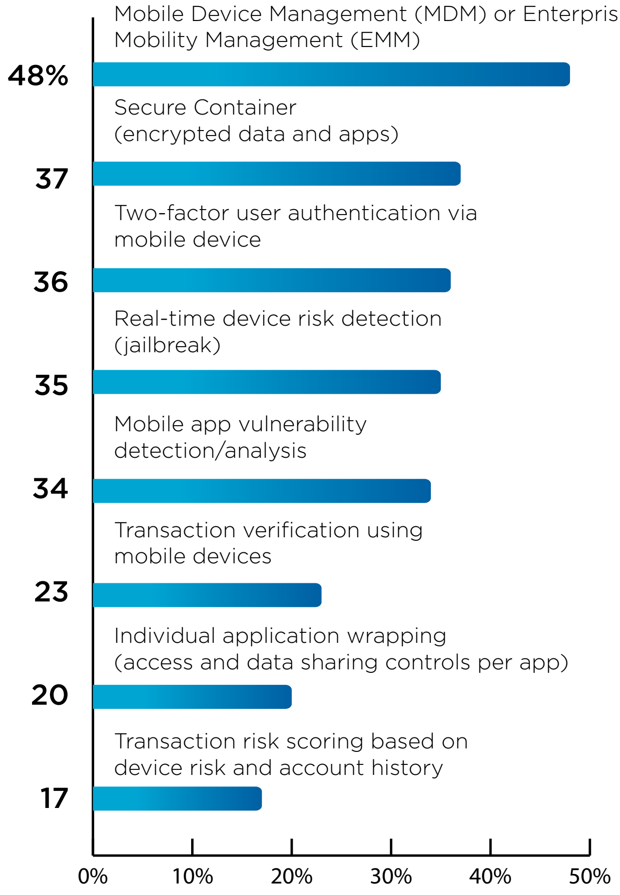
Which of these mobile security categories will be the main focus of your investments in 2015?



We'll look first at categories. Going back to our basic mobile security structure, we see that device management again is the dominant category, with 30 percent saying this is their main focus. Application security is second at 25 percent.

Next we look at specific security controls.

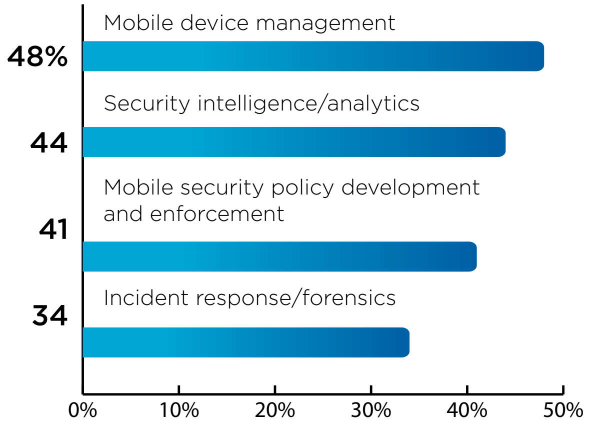
Which specific products/tools does your organization plan to deploy for mobile security in 2015?



Device and content security are the big winners when we look at planned investments. 48 percent of respondents are eyeing MDM and EMM solutions; 37 percent are planning on deploying containerization strategies; and 36 percent plan to deploy two-factor authentication using mobile devices.

Running a close fourth: 35 percent want to explore real-time device risk detection. And then there is mobile app vulnerability testing/analysis, which speaks to one of the key deficiencies we detected earlier.

What type of third-party mobile security services will your organization invest in during 2015?



Finally, we acknowledge that many organizations cannot go it alone when it comes to mobile security. So which types of third-party services do they plan to buy in the coming year?

Again, mobile device management is the clear winner with 48 percent of responses. But security intelligence/analytics and mobile security policy development score high, too.

The State of Mobile Security Maturity

We'll get into real survey analysis in our next section and a discussion with IBM's Yishay Yovel. But for now, let's recap a bit of what we've discussed and what we can conclude:

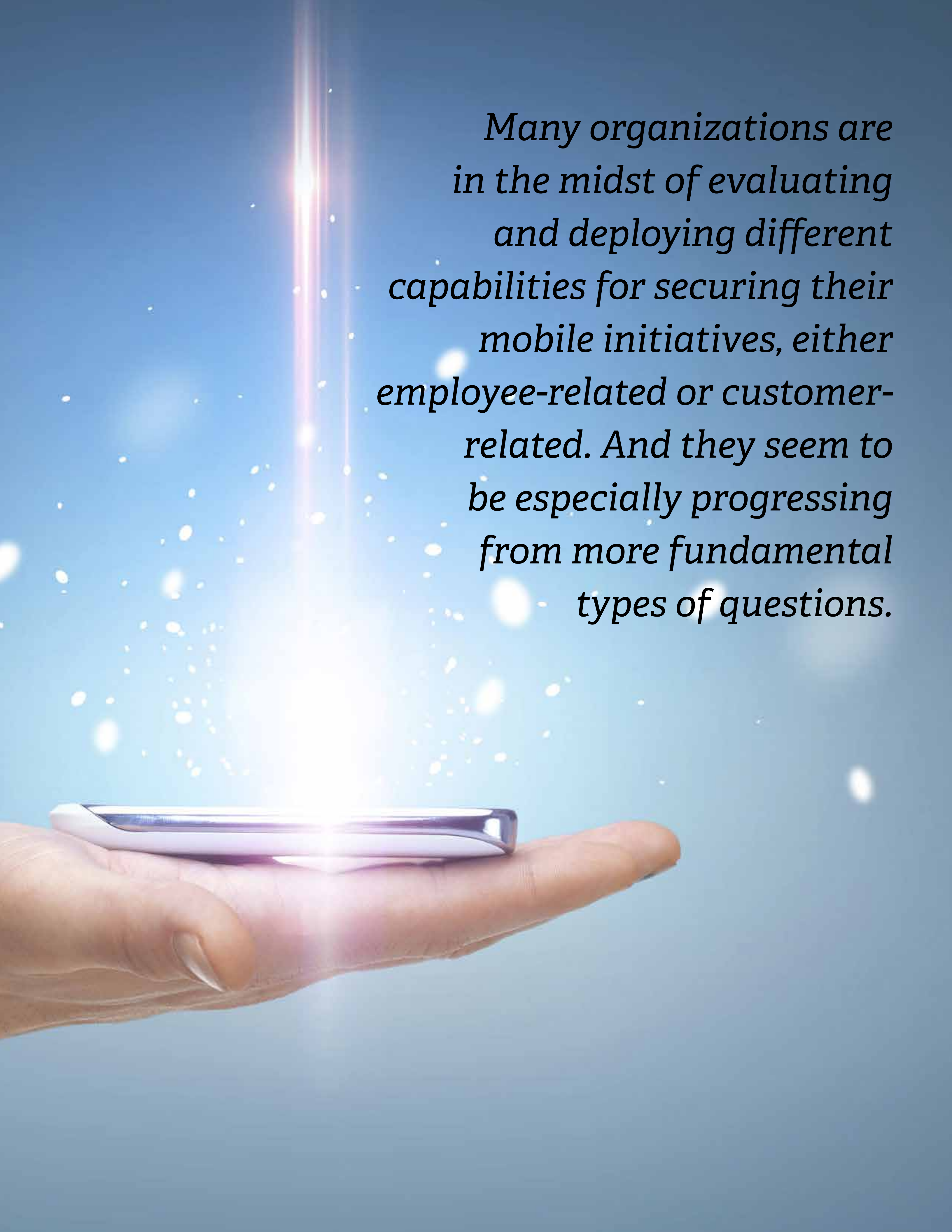
- **The Device is the Thing**
  Even as mobility becomes increasingly ubiquitous in the marketplace, enterprise security leaders still have a great focus on securing the mobile device, preventing loss or theft. This is the foundation of mobile security maturity, and many organizations are rooted here.

- **Content, Applications on the Rise**
  There is hope for ascension, though as organization' mobile strategies mature. They are increasingly paying greater attention to securing content and applications on their employees' mobile devices.

- **Transactions Transcend**
  Truly mature enterprises are following the market trend and focused now on securing the mobile transaction, which to this point is the height of mobile security maturity. And it's the level to which other organizations must aspire to attain in the months ahead.

But to grow this maturity, enterprises first must set their baseline and know where they are today. Then set appropriate goals, milestones and metrics.

In our next and final section, we discuss how to turn these survey results into action items.



Many organizations are in the midst of evaluating and deploying different capabilities for securing their mobile initiatives, either employee-related or customer-related. And they seem to be especially progressing from more fundamental types of questions.

IBM's Yishay Yovel on How to Turn Survey Insights Into Actions

So, now that we've learned about the state of mobile security maturity in large enterprises, what can we do about it?

Yishay Yovel of IBM has long focused on enterprise mobility, and he feels organizations have taken significant strides toward achieving true maturity. But the job is hardly over.

"We are halfway there," Yovel says. "There's definitely a concentration of focus on current investments in what we call the most foundational pillars -- securing the devices and the enterprise content on them. And then there is an emerging interest in getting more secured applications in place and finally securing transactions and access, which are more advanced capabilities."

In this excerpt of an interview with Tom Field, VP of Editorial at Information Security Media Group, Yovel discusses:

- The mobile security maturity model;
- What the survey results mean;
- How to improve mobile security and maturity in 2015.

Yovel directs IBM Security's mobile and fraud strategy. Yishay was previously the Vice President, Marketing for Trusteer, a financial fraud and advanced malware protection company, acquired by IBM in 2013. Yishay has over 20 years of experience in marketing, defining and deploying enterprise IT software solutions in the areas of security, storage, business continuity and mobile computing.

Survey Results: First Response

TOM FIELD: What is your gut reaction to the survey results, and what do you believe they say about the state of mobile security maturity?

Yishay Yovel

YISHAY YOVEL: I think that we are halfway there. This is how I would summarize it. It seems that many organizations are in the midst of evaluating and deploying different capabilities for securing their mobile initiatives, either employee-related or customer-related. And they seem to be especially progressing from more fundamental types of questions. They want to answer the device security [question] and start to look deeper into the different risks and threats that are involved in mobile security.

> *"There's definitely a concentration of focus on current investments in what we call the most foundational pillars."*

Stages of Maturity

FIELD: There were four key areas that we looked at in this study: Device security, application security, content security and transaction security. Looking at those four areas and the results that we got back, what do you see as the key messages?

YOVEL: There's definitely a concentration of focus on current investments in what we call the most foundational pillars. So, securing the devices and the enterprise content on them. And then there is an emerging interest in getting more secured applications in place, and finally securing transactions and access, which are more advanced capabilities.

This is something that we did expect to see. It seems that some enterprises are already getting into those advanced stages more, while others still kind of looking at first steps, etc.

FIELD: Now, we know that device security is the entry level. Do you see content being the next progression, then application and transaction as the pinnacle right now?

YOVEL: Yes. I think that in some ways, device and content security are bundled. It's typically packaged into the enterprise mobility management suites, and you get two for one, if you like.

But then addressing applications is more of a skillset and a capability that you have to develop in-house as you start looking at mobile application development pretty much the way you looked at the custom application development for web. Now we have to do the same thing for mobile, and it's presenting a unique set of requirements and capabilities. So, that's why it's more difficult, and that's why I look at it as the next pillar.

Transactions are even [more] different than that. It's looking at every individual transaction that you generate and assigning a risk to each one. This is very typical in the banking environment when you think about mobile banking, money transfers, etc., but it can actually span a transaction with any kind of enterprise resource, and you can look at those individually.

So, the progression I see is associated with granularity. You deal with the entire device, then you separate the personal and enterprise content, then you have to look at every individual application and understand the risk and vulnerabilities that it contains, and how to mitigate them. Ultimately, you have many transactions emanating from each application, and each one of them has to be analyzed.

So, as you progress in that framework, you become more and more granular in controlling the different assets, and the different interactions that you want to control to achieve optimal security. I think this is the path to mobile security maturity that we're thinking about for enterprises.

Device Security

FIELD: From your perspective, why did our respondents focus so much on device security, and what should they be doing next to progress?

YOVEL: There is some alignment in the survey between BYOD adoption and device security. So essentially, as an organization makes the leap into BYOD and it varies by industry, by organization, by size, even by the nature of the organization, the first thing you have to tackle is device security. Especially all the newcomers this year into BYOD adoption have to take care of that. Now, it may take time for them to deploy that capability, and then they have to roll it out in pieces. This is why we're still seeing a lot of concentration in device security.

Once BYOD adoption reaches saturation, which means everybody who wants to do it or will do it has done it, we will see a decline in the focus on device security.

The other thing is that if you think about the risk, the responders have pointed out that lost device, which actually implies lost enterprise data, is the biggest concern they have. They have to immediately implement device-level security controls to enable capabilities such as remote wipe, etc.

So, the concentration on this has to do with the fact the industry is still coming to terms with BYOD adoption. There is an obvious risk they have to manage, which addresses the device level, and this is why we still have

“Wiping the entire device is a very interesting capability, but if I wipe critical documents alongside your photos, you’re going to be very unhappy.”

this kind of concentration. The next thing that we’ll have to address is content security, which may be a relatively short leap for them to achieve. But ultimately to really realize some of these productivity benefits, custom enterprise applications are the things that enterprises that are forward-looking will have to look at. Putting together a secure application development lifecycle on day one is something that they have to look at next, even in parallel because it takes time to ramp up such a program. So, as they get more and more into mobility while they are addressing device concerns, I think they should be looking at application security too.

Application Security

FIELD: What do you feel that we learn from the respondents and their answers related to application security?

YOVEL: When we went granular on what people mean by application security, what they do … they definitely establish training, or they train their teams on secure application development. And, again, it’s a best practice they adopted from application development. But then they do things like source code scanning. So this is something you do before you deploy an application. You take the source code and get an expert analysis from a tool, like an IBM AppScan for example, that goes and looks at the mobile application code and detects vulnerabilities that can be exploited by hackers to basically compromise the application and access the data.

So, that’s one example. Another capability is binary code scanning. Why would you need that? Well, some enterprises want to vet third-party applications and even consumer applications to be allowed to run concurrently on the same device as an enterprise application would. So they would take those applications from the app store. They run the binaries to determine if they are vulnerable, and then they apply rules that if a particular application exists on a device, they will not allow certain enterprise applications to execute concurrently. Again, that’s a more advanced capability, but some enterprises do look at it, too.

Finally, there is a particular area called tamper-proofing. It basically means that if you deploy an application to the public in a public app store, for example, a mobile banking application, you want to protect it against reverse-engineering, because this is how hackers take it, change the codes to capture details such an ID and password, and then redeploy it on a third-party application store, essentially fooling the customers that they are using the genuine application when in fact they’re using fake, essentially malware.

We finally saw one thing that we do see even in our own business quite a lot, and this is something we call risk-aware application. Essentially adding a capability to an application to determine the underlying risk of the device that it’s running on. For example, is it jailbroken? Or has it [been infected by] malware or other type of risky applications? Again, this runtime analysis of the underlying device is essential for the application to adjust its functionality. For example, if the device is high-risk, I may not allow money transfer, but I will allow you to look at your balance. Those kind of risk-aware applications are a very popular concept, and it seems that at least some of the responders are looking at that capability too.

"Where I think we should be going is risk-based authentication of both log-in and transactions, where enterprises have to adopt mechanisms that will step up the verification process based on underlying device risk."

Content Security

FIELD: In terms of content security, what would you say we learned?

YOVEL: So, content security is essentially a binary problem. You have the personal content, which is your Facebook, LinkedIn and Twitter content. And then you have enterprise data. It could be documents. It could be Excel spreadsheets coming from back-end systems, from SharePoint, from other types of systems. What you want to achieve is to isolate the business content, the enterprise content, via encryption and via other forms of isolation, so that content doesn't get compromised.

So for example, the capabilities that some of our respondents are looking at include encryption, policies that restrict sharing, so you can't copy/paste data from an enterprise application to a personal application. Secure access to the back-end, so you can only access SharePoint via a VPN connection provided by different technologies in the enterprise mobility management space.

Finally, of course, you want to be able to remotely wipe the business data. That's very important. So wiping the entire device is a very interesting capability, but if I wipe critical documents alongside the photos, you're going to be very unhappy. So, some of the capabilities customers are looking at include selective wipe. They want to be able to make sure that they can wipe only the business data, not the personal data in case the device gets found.

Transaction Security

FIELD: What do you think the results tell us about transaction security?

YOVEL: So, that [transaction] security is the least adopted. I can think about it in two ways. One is that there are specific transactions that are very high value. They're financial in nature, so our responders in the financial services space are definitely looking into it much more than other enterprises. One of the capabilities there is risk scoring. So essentially, associating every transaction with the risk so they can determine what is the chance that it's fraudulent in the back-end.

In the more general sense, people initially are looking at end-to-end encryption to make sure that they're not susceptible to man-in-the-middle attacks and other types of threats of that nature. We are seeing capabilities in the market, including in the IBM portfolio, where we allow risk-based response or risk-based authentication to be used with transactions, which means as you execute a particular transaction based on the nature of the transaction and the underlying risks, mobile security technologies can take action.

For example, they ask you for a one-time password, or they want to do an extra step in validating who you are, and that's an important transaction security capability that enterprises should look at moving forward.

Where we should be going is risk-based authentication of both log-in and transactions, where enterprises have to adopt mechanisms that will step up the authentication or step up the verification process based on underlying device risk. So, for example, if you typically access your enterprise system from a particular area, let's say New York, and you have done that five minutes ago, and five minutes later there is an access to the same account from a place like Shanghai, or Africa … It means that there is a problem, that something here doesn't make sense, and this is typically where risk-based authentication kicks in.

Put Survey Results to Work

FIELD: How should organizations now act upon the survey results to improve their own mobile security maturity?

YOVEL: What we wanted to achieve in the survey is to create awareness for a roadmap for a good mobile security program. Essentially, what we want to do is to raise awareness that while you're focused on a particular area that is aligned with where you are in adoption of mobility and mobile security, you should be looking further downstream to look at the other areas and plan when you will address them, if you need to address them. What is your particular situation?

So if you go to http://IBM.com/security/mobile/, you can learn more about the framework that IBM has built. The survey shows that many enterprises are looking at all these different areas, and we think that all enterprises should look at them, and look at the capabilities that are required in each one of them, and then determine what is suitable for their own situation. It's a very good planning tool in order to follow that framework and make those decisions. It will make the path to mobile security maturity easier and more logical for many enterprises.

Mobile Security Resources

From IBM

IBM Security

Confidently protecting the mobile enterprise

As a mobile security leader, IBM Security has created a New Mobile Security Framework. This comprehensive approach to Mobile security enables trusted, higher-quality interactions at the device, content, application and transaction level. We have added to our framework, a unique layer of protection and visibility through IBM's Security Intelligence.

http://www-03.ibm.com/security/mobile/

From ISMG

Researchers Describe New Air-Gap Threat

Air-gapped networks promise data security by disconnecting PCs from the Internet. But malware-infected systems connected to air-gapped networks can be made to broadcast data via FM radio - using a PC's graphics card - to nearby smart phones, researchers warn.

http://www.inforisktoday.com/researchers-describe-new-air-gap-threat-a-7499

Breach Prevention: The Missing Link

As the workforce increasingly relies on mobile devices, corporate privacy and security policies aren't keeping pace. And that's leaving a large gap in organizations' breach prevention strategies.

http://www.inforisktoday.com/breach-prevention-missing-link-a-7369

7 Apple Breach Business Lessons

Is an iPhone or iPad, when tied to the Apple iCloud, secure enough for business use? Here are seven steps businesses must take to secure any mobile device - BYOD or otherwise - that's used to access or store sensitive corporate information.

http://www.inforisktoday.com/7-apple-breach-business-lessons-a-7271

How to Vet Third-Party Mobile Apps

As more organizations accommodate employees' demands to use mobile devices, ensuring the security of the applications on those smart phones and tablets has become critical.

http://www.inforisktoday.com/how-to-vet-third-party-mobile-apps-a-7224

WEBINAR

iSMG
INFORMATION SECURITY
MEDIA GROUP

The State of Mobile Security Maturity

Findings from the ISMG Survey Sponsored by IBM

Register for this session and gain first access to the results of the 2014 Mobile Security Maturity Survey, which includes insight on:

- Top mobile security threats;
- Gaps in how organizations secure devices, content, applications and transactions;
- Key mobile security investments for the coming year.

REGISTER NOW

http://www.bankinfosecurity.com/webinars/state-mobile-security-maturity-w-525

Sponsored by

IBM®

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

iSMG
INFORMATION SECURITY
MEDIA GROUP

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