KPMG
cutting through complexity

TELECOMMUNICATIONS

Mobile security: from risk to revenue

Creating opportunity from challenge

kpmg.com/mobilesecurity

KPMG INTERNATIONAL

Foreword

It has been just six years since the commercial introduction of the first smartphone and already it has become a ubiquitous and highly-valued personal and corporate tool. Indeed, from the corner coffee shop to online banking, from corporate email to business collaboration, mobile devices and services have rapidly integrated themselves into virtually every aspect of our lives.

The effect of mobility on traditional business models has been phenomenal. In Kenya, M-Pesa, a mobile payment system, now transfers roughly 10 percent of Kenya's GDP across mobile networks,[i] while in San Francisco and parts of the UK, motorists can now reserve vacant parking spaces in real-time with a mobile app connected to sensors embedded in parking bays.[ii]

But for telecom and technology companies, mobile means much more: it is an opportunity to create new business models, new services and new products that can enable this increasingly mobile world.

At the same time, the widespread adoption of mobile services, coupled with some recent high-profile security mishaps, have focused the attention of both consumers and corporate users on the potential risk that mobile poses to their privacy and security. Industry research consistently shows that security and trust are two of the top barriers to mobile adoption and innovation.

Clearly, telecom and technology companies – in partnership with their customers and corporate clients – will need to overcome these challenges quickly if mobile's current trajectory is to be maintained. But, as we highlight in this report, mobile security also provides telecom and technology companies with a significant opportunity to leverage their core skills to generate new revenue.

To develop this report, KPMG International partnered with Forrester Research to examine the market opportunities now emerging from the mobile security sector. Some, such as offering personal 'trust' services to consumers, are still nascent areas that will likely need to develop before significant revenues can be achieved. Others, such as device and application management services, are already in full bloom and showing strong returns for leading telecom and technology providers around the world.

We hope that this forward-looking report inspires telecom carriers, mobile operators, technology companies and service providers to rethink their approach to mobile security and find new ways to turn challenge into opportunity.

On behalf of KPMG's global network of Technology, Media & Telecommunications (TMT) experts, we encourage you to contact your local member firm to discuss your organization's approach to mobile security.

Sanjaya Krishna
Principal and Digital Risk Consulting Leader, KPMG in the US

Graeme Ross
Global Chair, Media & Telecommunications

Gary Matuszak
Global Chair, Technology, Media & Telecommunications

Contents

Executive summary

It seems everybody is concerned about mobile security. Consumers are worried that all of their personal data that now resides on their smartphones – contacts, bank account numbers, emails and so on – will fall prey to identity thieves and crooks. The risk for corporations is higher still as mobile devices become integrated into the office environment and start to be used to access sensitive company information, customer records and valuable intellectual property.

A complex environment

Mobile security is not a black and white issue; it is not simply a case of protected or at risk. Many complex issues compound the challenge and increase the rate of urgency.

For one, the recent trend towards encouraging employees to either bring or purchase their own device has not only brought masses of new devices on to the networks, but has also created significant security challenges for corporate IT departments who are already swamped trying to develop and integrate the many mobile solutions being demanded by the business.

In many markets, new spectrum releases will also catalyze the ecosystem into developing new applications and services which, in turn, will drive increased traffic through mobile networks and across mobile platforms. And as all this data whizzes around networks, security will once again be tested.

The security challenge

Trust will become the byword of the mobile era. Consumers will need to trust that their data and information is being kept securely when using mobile devices and services, while corporations will need to trust that their service providers, technology environments and employees are adhering to their security protocols.

As a result, demand for mobile security products and solutions is quickly picking up steam. Corporations – keen to unleash the productive benefits of mobile without taking on additional risk – are hungry for effective solutions, particularly those that can be outsourced or moved into the cloud.

Consumers have also proven willing to pay a premium for enhanced security and privacy on their mobile devices opening up a new market of opportunity for those that can successfully commercialize new consumer security solutions.

Turning risk into opportunity

While the mobile security field may still be somewhat nascent, there are already a number of telecom and technology organizations that are making strong businesses out of mobile security solutions and, at the same time, creating new and sustainable revenue streams for the future.

Based on research conducted by Forrester Research and the experience of the leaders within KPMG's GlobalTMT practice, we have identified a number of emerging opportunities for telecom and technology organizations to achieve growth from mobile security.

Telecom operators and carriers

- Deliver personal 'trust' services to consumers
- Develop consumer identity management services
- Provide device and application management services
- Mobilize security services.

Technology and service providers

- Develop location-based security services
- Deliver enterprise-integration-as-a-service
- Offer secure content services
- Deploy device and application virtualization technologies
- Create hardware-assisted security assurance technologies.

Securing the revenue potential

True, mobile security business models are only just emerging and the field will undoubtedly open up a host of new opportunities for telecom and technology companies in the future. But given the speed of the technology's adoption and the increased sensitivity of the traffic, we believe that industry leaders would be wise to start considering how they might transform their organizations to serve this new and growing market.

About this research

Working in partnership with Forrester Research, KPMG's Global TMT practice examined the current mobile security market and some of the key indicators of future success in the sector to identify and define new opportunities for telecoms and technology organizations. Analysis and commentary was provided by leaders from KPMG in the US, the UK, Germany and Australia.

This report is part of KPMG's wider initiative focused on exploring new opportunities emerging in mobile and complements the firm's *Mobile Evolution* series of bi-weekly articles which can be found online at kpmg.com/mobile.

A mobile world

A recent Forrester Research ForrSights Workforce survey found that 62% of employees who use a smartphone for work paid for the device themselves while 52% did the same with their tablets.

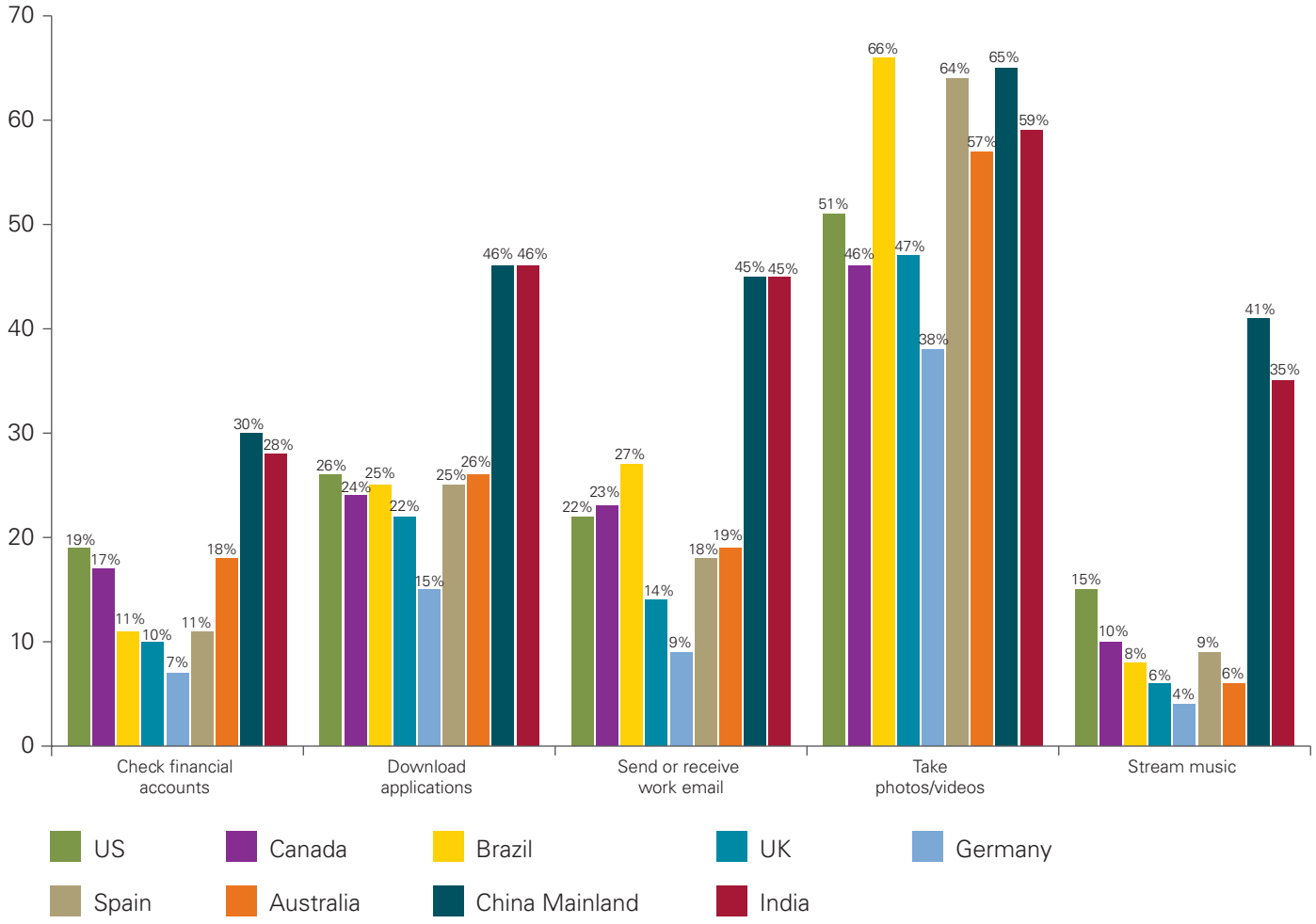
Driven by a workforce craving greater flexibility and technological agility, corporations around the world are increasingly integrating mobility into their workforce support and business applications.

Some, like the GSM (Global System for Mobile Communications) carrier in the UK who recently eliminated the use of desk phones in its offices, are reducing costs and increasing accessibility through mobile. Others, like the global bank that recently allowed its employees to access its customer relationship management (CRM) application on their mobile devices, are using mobile to transform their operating models and customer propositions. To respond to demands for greater flexibility, a growing number of workplaces are now also encouraging employees to bring their own devices to work.

For their part, consumers continue to pioneer the mobile space and – while personal communications still tops the list of how today's 'always connected' consumers spend their time on their devices – entertainment, personal finance and social networking have also moved up the list (see Figure 1).

Figure 1: Top consumer mobile activities around the world

Which of the following do you do on your primary mobile phone at least monthy?



Source: Forrester Research Global Technographics Online Benchmark Survey, Q2, Q3 2012. Base: US 53,427, Canada, 4,463, China Mainland 1,810, India 1,938, Australia 948, Brazil 1,818, UK 2,948, Germany 3,616, Spain 2,048 Online Adults (18+) who have at least one active cell phone.

The trend towards greater mobility seems set to continue with various government and regulatory bodies around the world freeing up spectrum for commercial use in an effort to foster greater mobile innovation and enhance the mobile economy.[iii] The net effect is that in the near future, on a global scale, mobile users will see more reliable, more readily available and more pervasive connectivity.

India recently launched spectrum auctions, while Germany has been auctioning spectrum since 2010. Australia auctioned further Spectrum in 2013, and the US will soon start whitespace auctions.

Security and privacy in the mobile ecosystem

> Unless your customers trust that you will not share their personal data – or their employees' data – with third parties or lose their data, there will simply not be a market.
>
> **Alfred Koch,** Director, KPMG in Germany

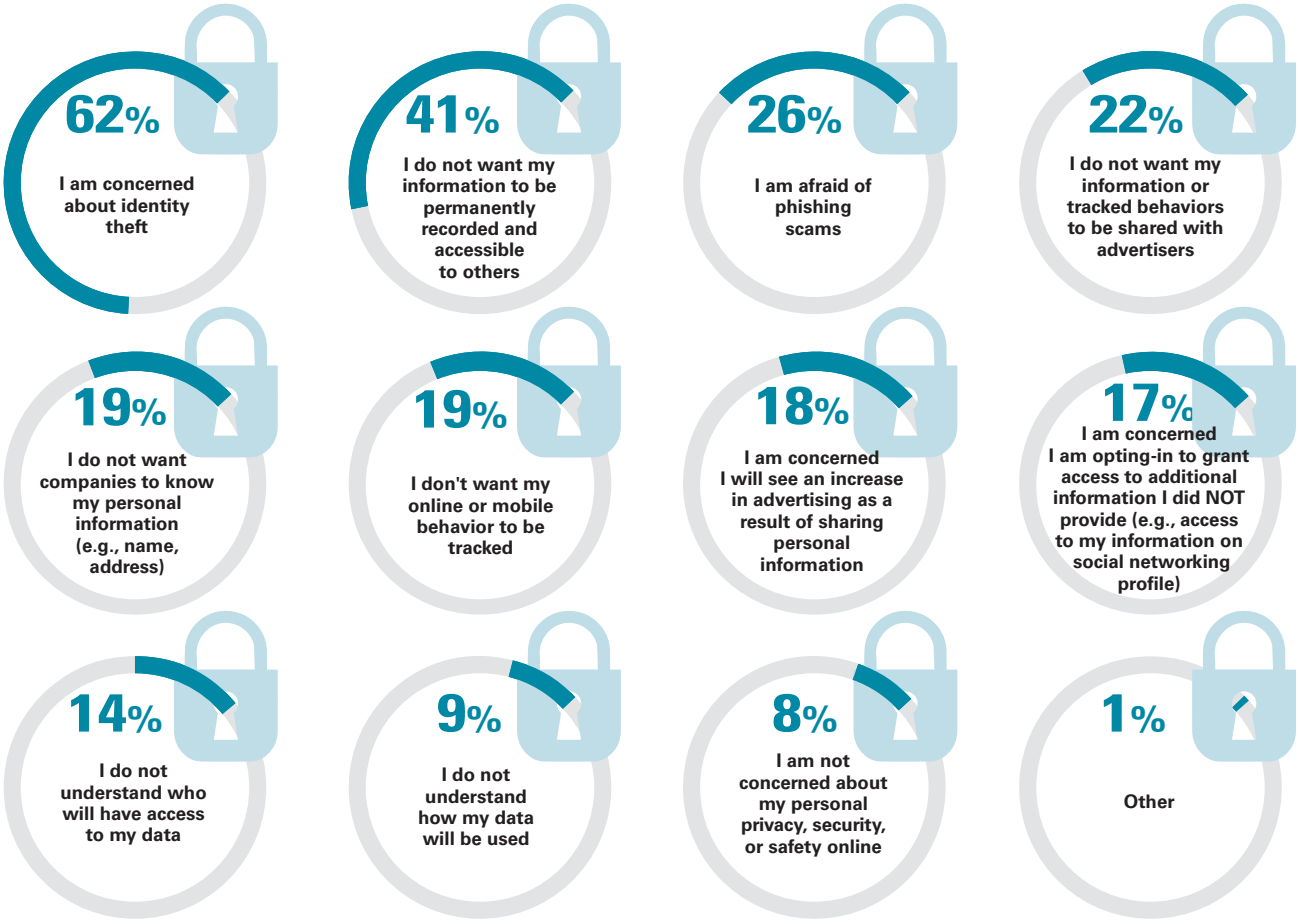
While the new era of the 'always connected' consumer certainly presents a myriad of opportunities for businesses, it has also created new threats. In particular, the reality of increased mobile penetration coupled with a changing mobile threat landscape and a fragmented mobile technology market has led to deep concerns about security and privacy risks that must be overcome for the ecosystem to thrive.

Building trust with consumers

Consumers are increasingly concerned about the security of their data and private information on their mobile devices. Indeed, according to a recent consumer report by KPMG International (*The rise of the digital multi-tasker*), users in many markets are increasingly willing to pay more for their mobile applications in order to ensure that their privacy is maintained. In Forrester's 2012 Technographics survey, 62 percent of North Americans said they were concerned about identity theft (see Figure 2).

Figure 2: Consumers are concerned about security and privacy for fear of identity theft

Why are you most concerned about your personal privacy, security, or safety when doing certain things online?

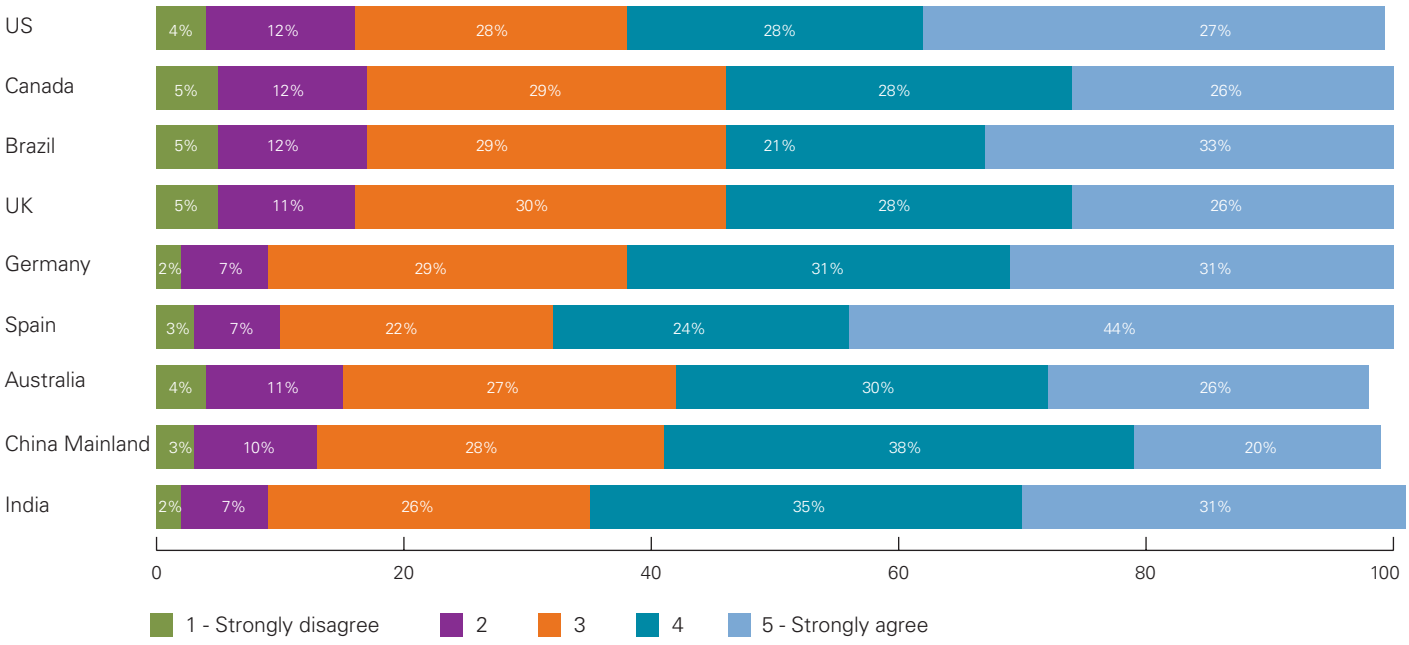


Source: Forrester Research North American Technographics Online Benchmark Survey (Part 2), Q3 2012 (US, Canada). Base: 30,549 United States Online Adults (18+).

Consumers have good reason to be concerned. A recent study of free mobile apps by Appthority found that 96 percent of all free apps in Apple App Store and Google Play share data with third parties and 76 percent of the top 50 most popular free apps are associated with risky or privacy-invasion behaviors.[iv] However, a recent study by Carnegie Mellon University found that while users may be concerned about mobile privacy, in general they are not very aware of what mobile apps are doing with their data.[v] And consumers expressed significant levels of concern about their privacy and security when accessing the Internet from their mobile phones, according to Forrester's Global Technographics consumer survey (see Figure 3).

> The fact that 'free apps' are able to triangulate their location and target ads based on personal preferences has shown the mobile consumer that the potential for abuse is high.
>
> **Greg Bell,**
> Information Protection and Business Resiliency Service Leader, KPMG in the US

Figure 3: Consumers are concerned about their privacy and security when accessing the Internet via their mobile phones



Source: Forrester Research Global Technographics Online Benchmark Survey, Q2, Q3 2012. Base: US 32,000, Canada, 2,751, China Mainland 1,711, India 1,688, Australia 603, Brazil 1,254, UK 1,164, Germany 1,662, Spain 1,111 Online Adults (18+) who use their cell phone to access the internet.

Figures may not add up to 100 due to rounding.

> Consumers are certainly starting to become aware of the implications of their decisions when it comes to protecting their privacy and security on mobile, even if they are not sure what to do about it.
>
> **Greg Bell,**
> Information Protection and Business Resiliency Service Leader, KPMG in the US

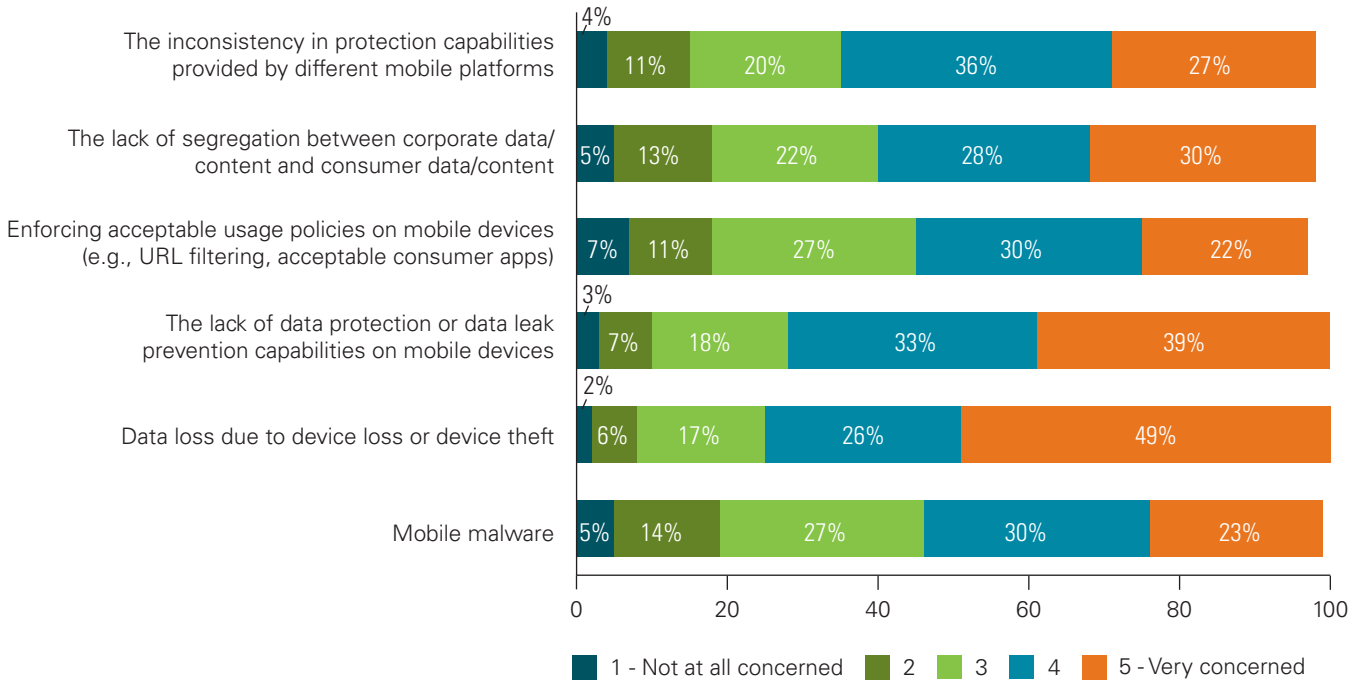
Building trust with customers and service providers is, therefore, critical. For technology and telecommunications companies, this means not only putting in place sufficient security and privacy safe guards, but also increasing communications and business transparency to help consumers understand what is happening with their personal data.

Overcoming the corporate security hurdle

In the business world – where corporate IT departments are already struggling to cope with the onslaught of mobile support requests – mobile security concerns remain top-of-mind. IT decision makers are particularly concerned about data loss due to device loss or theft[1] (see Figure 4) and, as a result, implementing or improving mobile security is the number one corporate mobile priority[2] (see Figure 5).

Figure 4: Top mobile security concerns for IT decision makers in North America and Europe

How concerned is your firm with the following for mobile security issues?



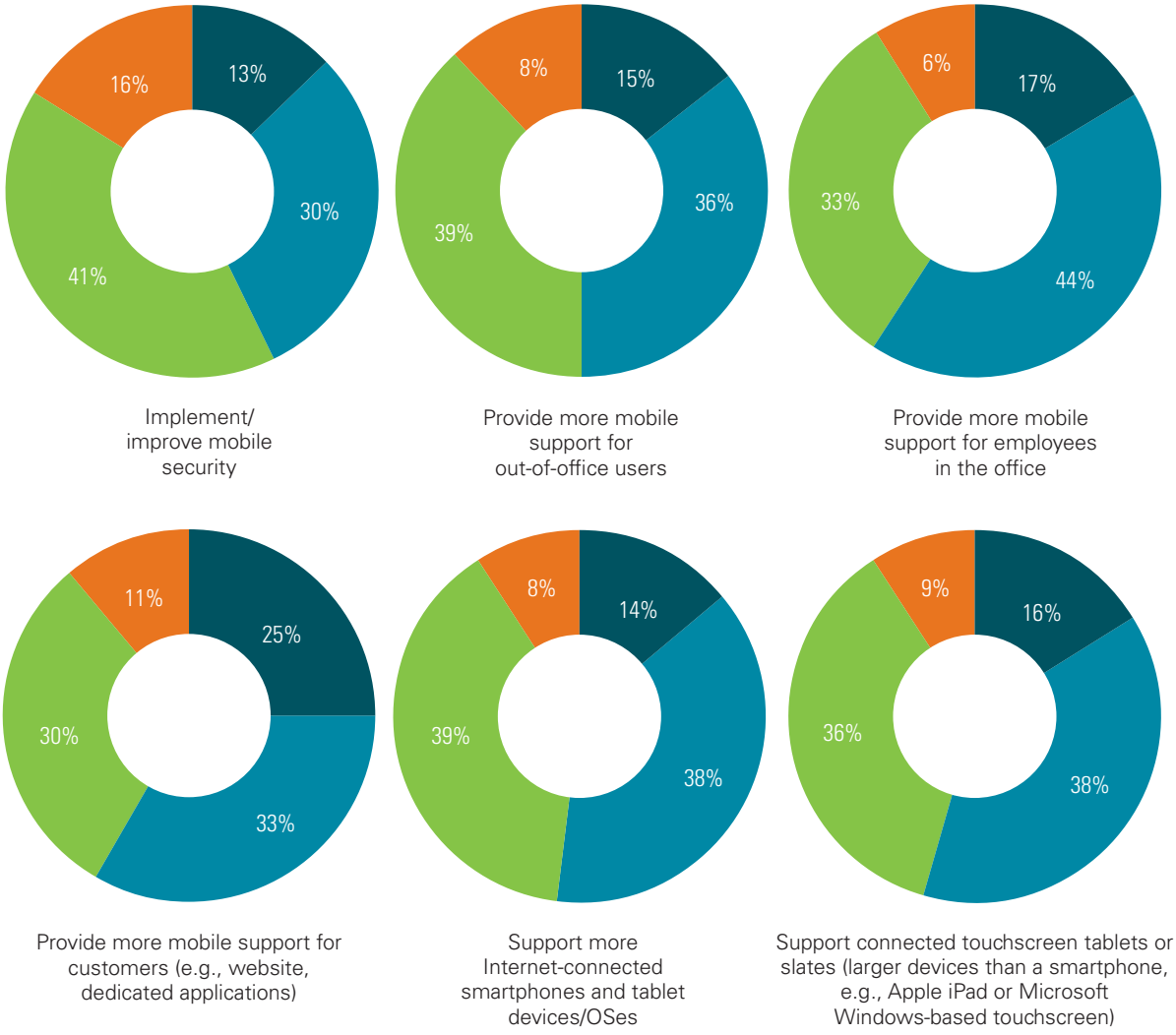
Source: Forrester Research ForrSights Security Survey, Q2, 2012. Base: 1508 North American and European IT decision makers.
Figures may not add up to 100 due to rounding.

IT security professionals are especially concerned about the possibility of mobile data loss (due to device theft or loss), the lack of data leak prevention capabilities on the mobile device and the lack of platform consistency in protection capabilities.[3]

[1] ForrSights Security Survey, Q2, 2012. Base: 1508 North American and European IT decision makers.
[2] ForrSights Networking and Telecommunications Survey, Q1, 2012. Base: 1535 North American and European IT decision makers.
[3] ForrSights Security Survey, Q2, 2012. Base: 1508 North American and European IT decision makers.

Figure 5: Top mobile priorities for IT decision makers in North America and Europe in the next 12 months

What are your firm's top mobile priorities during the next 12 months?



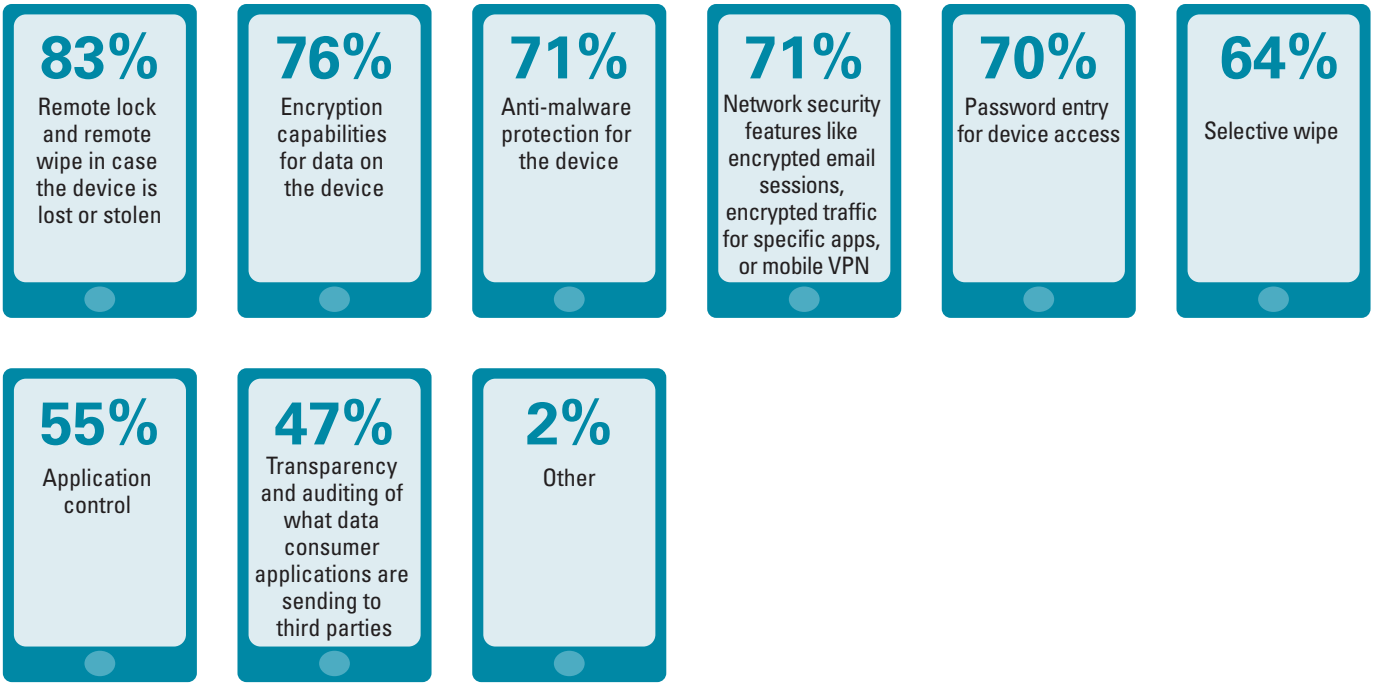
Source: Forrester Research ForrSights Networking and Telecommunications Survey, Q2, 2012. Base: 1535 North American and European IT decision makers. Figures may not add up to 100 due to rounding.

> Trying to enforce a consistent security policy while, at the same time, attempting to deliver a seamless user experience, is a difficult undertaking. But it's one that clearly needs to be addressed.
>
> **Sanjaya Krishna,**
> Principal and Digital Risk Consulting Leader, KPMG in the US

Viewed through the IT department's eyes, mobile security is focused on improving the organization's ability to control corporate content and data accessed through a mobile device, enforce corporate security policies, and defend against mobile threats. But as corporations move from a 'blackberry-only' world to a more multi-platform reality, many are being forced to deploy point solutions rather than a consistent data protection capability (see Figure 6) which, in turn, is adding to the complexity for corporate IT and security professionals.

Figure 6: Top mobile priorities for IT decision makers in North America and Europe

Which of the following security technologies and policies, if any, would alleviate your concerns?



Source: Forrester Research ForrSights Security Survey, Q2, 2012. Base: 1508 North American and European IT decision makers.

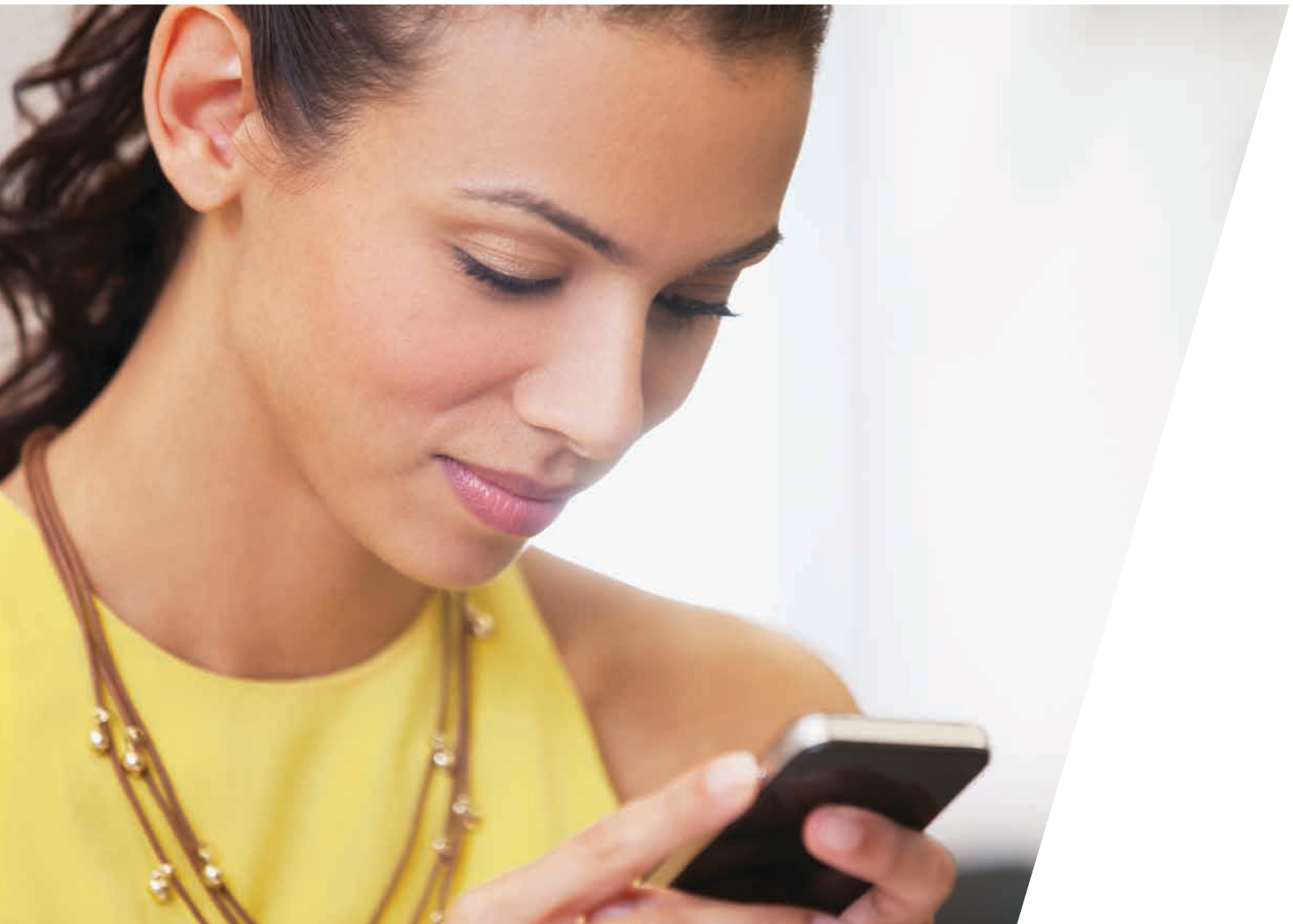
Opportunities for telecoms operators
The value is in services

> Mobile operators and carriers are already in a unique position to provide a broad range of mobile services but they will need to migrate to a user-oriented mindset and focus on the whole end-to-end customer experience.

Greg Bell,
Information Protection and Business Resiliency Service Leader, KPMG in the US

Clearly, more mobile traffic and more consumer services will lead to increased demand for mobile carriers and operators. AT&T, for example, has already seen its wireless data traffic grow an astounding 20,000 percent between 2007 and 2012, driven primarily by the use of smartphones.[vi]

But while more data volumes may mean increased revenues, it only reinforces the need for traditional operators to focus on the whole end-to-end customer experience. Given the trend towards more commoditized data volume businesses, it seems inevitable that – to survive in the longer term – operators will need to differentiate themselves and renew their businesses by offering smart services built on top of their data traffic, and delivering a superior experience to their customers. Security services, in particular, will be a key growth area for operators and carriers.



> The market desperately needs 'providers of trust' who can govern the interaction between consumers and the mobile environment to ensure transaction integrity, security and the protection of private information.
>
> **George Thompson,**
> Director,
> KPMG in the UK

Opportunity: Deliver personal 'trust' services to consumers

As consumers increasingly shift their critical personal tasks such as banking and commerce onto their mobile devices, issues such as identity protection, transaction integrity, security and liability rise to the surface. In particular, consumers report being worried about the potential for identity theft and misuse of their personal data.[4]

This provides a unique opportunity for carriers and operators that can provide targeted security services to their customers. For example:

- **Personal fraud watch and management:** This function helps the consumer identify potentially fraudulent transactions, alerts the consumer on frauds and can even help to rectify fraudulent charges. Unlike fraud detection functions employed by financial institutions, these services are designed to help individual consumers and as such are independent to specific service providers.
- **Consumer app risk management:** By providing this service, operators and carriers can help identify malicious and risky behaviors of mobile apps and help consumers manage their risks in the mobile world. For example, consumers need to know whether an app would leak their personal data to third parties, share their credentials with embedded advertising services, or worse, take over their mobile device.
- **Personal trust management:** This broad category of 'trust management' may include personal identity management, mobile usage monitoring, loyalty program management, privacy monitoring or even simply controlling which ads get displayed on the consumer's mobile phone. Personal trust management is a nascent market, but increased mobile penetration will quickly escalate customer demand for these services.

It is worth noting that these personal 'trust' services will ultimately benefit both consumers and businesses. Consider the case for tighter fraud management to a service provider like PayPal who processed roughly USD10 billion in mobile payments in 2012;[5] a drop of even a few percentage points in the fraud rate could mean hundreds of millions of recovered revenues.

> The market is starting to shift towards a preference for risk-based technologies that recognize that not everything needs to be encrypted, not everything needs to go through a VPN [Virtual private network]. The real challenge here is how to maintain the right level of information control but with a light touch.
>
> **Tim Miller,**
> Director,
> KPMG in Australia

[4] Forrester Research North American Technographics Online Benchmark Survey (Part 2), Q3 2012 (US, Canada). Base: 32,454 North American (US, Canada) Online Adults (18+).

[5] http://seekingalpha.com/article/882311-paypal-huge-mobile-payments-growth-remains-buried.

Opportunity: Develop consumer identity management services

In a quest to reduce operating costs and become more agile, many organizations are now looking for opportunities to outsource their customer identity management requirements to a third party consumer identity provider.

Mobile carriers and operators may have a strong vantage point for entering the market: they already know who the user is, where they live, which devices they carry and possibly even their financial information and real-time location, all important attributes of a strong user identity system. Telecoms may also find promising partnership opportunities with existing identity service providers (such as Equifax) to enhance the robustness of these services.

Identity services also benefit consumers; by managing consumer credentials, third party services providers – with permission – could tie that in real-time to devices allowing transaction information to be seamless to the users and ultimately provide a better user experience.

Opportunity: Provide device and application management services

As corporate customers continue to shift functions out of their business, carriers and operators may see growth potential in providing mobile and application management capabilities as part of the company's standard telecom services. This would essentially provide the benefits of consolidated telecom and mobile management billing with single-sourced support service and simplified vendor management.

By virtue of their position within the network, operators and carriers can also provide services such as traffic filtering and performance monitoring as well as services like app store management and secure cloud storage.

Many leading telecom players are gaining traction in this area: AT&T already offers device management, application development, security services and mobile application hosting; T-Systems (a subsidiary of Deutsche Telekom) offers device management, security and enterprise integration; while Mahindra IT & Business Services offers mobility solutions in areas like mobilization of SAP, Oracle, and BI installations.

Opportunity: Mobilize security services

While corporate security systems have traditionally been deployed on fixed infrastructure, the shift to mobile has made it clear that fixed infrastructure is increasingly ill-suited for a workforce that is constantly on the go. This leaves a valuable opportunity for carriers and operators to help organizations manage their security environment.

For example, carriers and operators could provide services that pre-scan apps in the app store and provide critical security assessments; or they could help operate corporate device security management servers to facilitate functions such as passwords, device tracking, encryption, lock and wipe. Moreover, if the management infrastructure were to be implemented in a carrier's cloud, clients could also achieve the benefits of operational elasticity and scalability.

> Several of my clients have experienced increased employee productivity by introducing mobile solutions. One bank has deployed their CRM system onto employees' mobile devices which has allowed them to be more responsive to customer needs.

George Thompson,
Director,
KPMG in the UK

> Becoming stateless with respect to customer identities is a distinct business transformation opportunity to reduce cost and scalability requirements in user onboarding, authentication and credential management.

Martin Sokalski,
Director,
KPMG in the US

AT&T: talking mobile data privacy and security

An interview with **Barry Johnson**, Senior Product Manager, AT&T Managed Mobile Security Services and **Michael Singer**, Assistant Vice President, AT&T Mobile, Cloud and Access Management Security.

Q: What do you think are some of the big opportunities for mobile carriers and operators when it comes to data privacy and security?

BJ: First off, we don't think that encryption on its own will cut it anymore. The key focus in 2011 was bringing personal devices on to corporate networks securely and most firms responded to the Bring Your Own Device (BYOD) shift by investing in endpoint security solutions. But we think that today's threat landscape has proved this tactic to be insufficient. Instead of just securing the device, it was data security that came to the forefront of attention.

We think that it's network-based security services that are really needed in this market. So while data protection on the endpoint has played a significant role to date, we believe that mobile carriers can go the extra mile to secure data by pushing security into their networks and being able to pinpoint malicious traffic quickly.

So, for example, providing VPNs with encrypted channels on the carrier side or creating 'data free zones' using virtual desktop infrastructure (VDI) encryption, or tokenization. By limiting where toxic data can be stored, companies can simplify the deployment of technology without worrying about potential data loss.

MS: We also see Mobile Device Management or MDM solutions playing a large role in data security and privacy and think that mobile carriers should be thinking about acquiring and offering these solutions.

But while MDM has been a hit on the corporate side, many organizations still realize that protecting devices with simple numeric PIN codes is not secure enough. Because of this, enterprises are looking at mobile carriers to provide or tie into caller ID, ANI, biometrics (facial recognition, fingerprint readers, voiceprint biometrics) as well as device fingerprinting solutions to protect both their devices and their back-end servers better.

Q: Where do you think the location-based security services market is going?

MS: While geo-locations services are still in a nascent creation phase, we think they will play a more comprehensive role in the future. The goal here is really to tie device location to mobile security policies to avoid data loss. The challenge in location-based services is that you are treading a fine line with respect to data privacy – the enterprise has to really soul-search about how to deal with privacy.

Q: What about secure content sandboxing and MDM integration.

BJ: In an age where most people carry multiple devices to stay connected to every aspect of their lives, encrypted containers are making it possible for one device to be used for both work and personal activities.

AT&T Toggle, for example, gives mobile professionals the option to use their smartphones and tablets for both business and personal use by separating and safeguarding business data into a specific work mode. Corporate IT departments can manage this work mode by protecting passwords, enabling and disabling business apps, locking and unlocking work mode and wiping work mode if the device is lost or stolen or when an employee leaves the organization.

IT departments will also want to make sure that, before they set up the container, the device is clean – so we have created a process to scan for any known threats and to conduct preliminary checks after which we can determine that the device is eligible to move on to the next stage.

Q: And what about device and application virtualization technologies?

MS: That's pretty exciting stuff. We've got a new LTE (long term evolution) technology that offers lower latency, and the processing time it takes to move data through your networks is faster. This, in turn, speeds up virtual connections from mobile devices to virtual desktops.

We've also got a Virtual Desktop Service that runs on a remote centralized platform within a state-of-the art AT&T Internet Data Center. As employees work locally, the programs and files they use are actually being processed and delivered from this remote cloud-based platform – and due to LTE speeds, data can be accessed and transmitted quickly.

Q: Is the mobile ecosystem really more vulnerable to security and privacy than the traditional web ecosystem?

BJ: We certainly think it is. AT&T actually sees WiFi 3G and 4G as the biggest threat to security and privacy today. In part, that's because many applications and web pages do not properly secure data, so when it travels across the network it can easily be intercepted and stolen. But it is also because many developers are focused on pushing out new products to capture new parts of the market rather than spending much time on privacy and security.

Third party app stores, sideloading, and the fragmented Android OS are also concerns because you cannot depend on the end-user to have their device fully patched and the IT department can't possibly control it all: users can – and will – bypass the VPN and install malware.

Global organizations may have an even larger problem. For example, encryption regulations differ significantly between countries which means that mobile handsets can often come with incompatible encryption algorithms. We think that by using in-line, transparent, and network-based security and data encryption, we can help deliver adequate and efficient data protection when moving data between geographically dispersed mobile devices and cloud SaaS applications.

We've often said that you cannot depend on the mobile operating system alone for security, but the mobile network should also provide security controls for sensitive data filtering, detecting and preventing mobile malware activity, and so on.

Q: Where does AT&T see the mobile security market going from here?

MS: Mobile technology is evolving quickly and now we are starting to see applications in everyday household items, cars and buildings which should enable us to do things that were not possible before: the refrigerator communicating with the car to remind the driver to pick up some milk on the way home, or maybe the building HVAC warning the user on their mobile device that it is time clean air ducts.

Essentially, billions or trillions of sensors will send data to processing centers – which may simply be applications already embedded into the cars and buildings – which will then generate a message on a mobile application for the user. The challenge, of course, is securing that data not only on the mobile device and processing center, but also in the car, the building, the house and the appliances.

Q: So what new capabilities do you think telecom players will need to make the most of this mobile opportunity?

BJ: A fundamental building block is having a network that will help secure and scale. If a mobile device is roaming or moving to a different carrier, and is swapping traffic from one carrier to the next, enforcing strong security policies to protect the customer is a must.

And while we think that a more portable, network-agnostic security approach will be the center of attention over the medium-term, we also believe that achieving this will require tighter coordination of development efforts between carriers and device manufacturers.

In the US, I think that the ISIS partnership has been a game changer, as have the current carrier agreements that allow customers to roam on all carrier networks, which improved the overall customer experience. Clearly, when the telecom industry works together it can lead to real benefits for customers.

Opportunities for technology providers
An innovation hothouse

> Assuming the governance requirements can be overcome, banks and other financial organizations will likely be very interested in getting their hands on an accurate location-based verification service to sharpen their existing fraud management systems.

Tim Miller,
Director,
KPMG in Australia

> Mobile Device Management, authentication services and app integration are all significant opportunities for technology companies.

Alfred Koch,
Director,
KPMG in Germany

Mobile is a veritable hothouse for technology innovation. There is now a fairly level playing field: small and nimble boutique firms that have an interesting technology alternative to offer can compete head-to-head with more established players.

And while the security and privacy market is still nascent and only yet forming, a number of innovative security technologies and services have been rapidly emerging on the stage, creating new opportunities for small players and traditional stalwarts alike.

Opportunity: Develop location-based security services

Adding real-time location information to security services offers security leaders greater context which, in turn, contributes to the robustness of decision making. But to make location-based security services work, technology providers will need to figure out how to process location and transactional information in real-time and in context of each other.

The task of getting different streams of data to work together in sync, while still preserving user privacy whenever necessary will also present a challenge to technology providers working in this space. But given that the industry is only just beginning to realize the potential of location-based security services, the area promises to be a strong growth market for those able to bring effective solutions to market.

Opportunity: Deliver enterprise-integration-as-a-service

With many IT departments struggling to keep pace with internal demand for new mobile applications, there is a growing need for technology service providers that are able to integrate mobile applications into enterprise back-end services through a standard set of APIs (application programming interface), SDK (software development kit) or app-wrapping service. Ultimately, this service allows individual app developers to build platforms that meet the needs of the internal clients without having to worry about integration challenges.

Enterprise-integration-as-a-service technologies are still in early stages – some are adopted as general purpose application development platforms while others are used more narrowly as a security mechanism and may be deployed with an MDM solution.

Opportunity: Offer secure content services

Many companies face a tremendous challenge trying to externalize their corporate content and data, especially when security is a concern. Often, the company's remote access infrastructure may not be set up to deal with mobile devices or accommodate a large volume of mobile traffic. This can lead to failed mobile experiments or delayed mobile expansion.

One effect of enterprise mobilization is faster adoption of cloud services; since cloud services would have dealt with the scalability and security issues already, it makes sense to move enterprise content into the cloud and let the cloud provider deal with capacity and security issues associated with mobile access. In particular, Forrester sees the emergence of 'secure enclave' content service providers that have the ability to offer separately hardened, separately certified, and vertically focused content services for confidential and critical business content.

Opportunity: Deploy device and application virtualization technologies

Companies looking to effectively segregate corporate content from personal data have few options today; they either implement a heavy weight container and do so at the peril of user experiences or opt not to manage corporate data at all.

Device or app virtualization technologies look to fill this gap by providing virtual segregation, deployment flexibility, and seamless user experience. In particular, device and app virtualization are attractive to organizations with stringent security requirements that still want to take advantage of enterprise mobility and BYOD, as well as to countries with strict privacy laws and regulations.

However – barring a major case of data loss related to BYOD in the market – workers will increasingly bring their own devices to work which, in turn, will increase the demand for virtualization technologies.

Opportunity: Create hardware-assisted security assurance technologies

Hardware-assisted security technologies on a mobile handset have thus far been limited to Secure Element and NFC (Near field communication) technologies, which do not lend well to securing general purpose applications.[vii] But as mobile payment and banking go mainstream, the demand for more security on mobile handsets is also rising.

Just as chip makers Qualcomm and NVIDIA are teaming up with ARM to offer TrustZone-based SecureOS for DRM (Digital rights management) operations and high-risk transactional applications, there is room for other hardware-based security innovations, such as general purpose secure co-processors, and those that support encryption and biometrics, to add trust and verifiability in the mobile transaction value chain.

> "BYOD certainly accentuates the security problem with mobile. You may have rules to delete data after certain period, but if you have no clue where it is – whether it is in the cloud or on devices – that is a big issue."
>
> **Sanjaya Krishna,**
> Principal and Digital Risk Consulting Leader, KPMG in the US

Sophos: taking advantage of new opportunities

An interview with **Gerhard Eschelbeck**, CTO and Senior Vice President of Sophos.

Q: Tell us about Sophos and the role that your organization plays in the mobile security ecosystem.

GE: Sophos is very focused on delivering complete security solutions for the mid-market enterprise. So we look at security at the network level, the end-point level, the mobile level and the enterprise level. Our ambition is to cover the whole security life-cycle for mobile by creating a product portfolio that matches the evolving security needs of our clients.

Q: What are the big mobile security challenges for the mid-market sector?

GE: The challenges for the mid-market are not all that different from those being experienced in larger organizations. The genesis of the security challenge started with the management challenge of integrating multiple mobile devices into the enterprise network. Indeed, as more and more organizations allow their employees to connect to the network on their own device – known as Bring Your Own Device (BYOD) – these complexities in security will become more acute.

One of the challenges with working in the mid-market is that each of our clients demonstrates different levels of mobile maturity and capability; some have five or six dedicated security personnel, while others have no dedicated security staff at all. What this means is that these organizations require a significant amount of partner support – particularly around security strategy and implementation – to fortify their infrastructure.

Q: How is the market transforming today?

GE: One of the biggest impacts on mobile security will come from multiple devices being connected to the network by individual users. I often ask executives how many devices they have that connect to the network. Some only have one or two, a growing number boast six or more. We're seeing a shift from what we considered a 'device-centric' security model where the focus was on securing individual tech assets, to now focus on 'user-centric' security models. What this means is that we are moving towards a more user-activated security solution and model versus an IT-activated model, and I think this is going to create unique issues for organizations large and small.

Q: What opportunities do you see emerging for mobile security providers in the future?

GE: Besides managing this 'user-centric' security model that will need to emerge, we see new opportunities emerging in almost every area that mobile touches. Connecting cars to the network – a trend that is already well underway – is creating new opportunities for mobile security providers. Similarly, so will the wider introduction of smart grids, mobile health and machine-to-machine communications and each of these new areas will create new opportunities for mobile security providers.

One area that we are placing both resources and investment in is the cloud. We think that mobile and cloud were simply made for each other, so we are developing a complete new security architecture for mid-market customers that is fully cloud-enabled.

Q: As a product-focused company, how are you working with partners to identify new models, client needs and trends?

GE: We have a very robust partner network that includes everyone from traditional resellers to MNOs (Mobile network operators) and systems integrators. It's really our partners that are on the ground providing that strategic input and direction on things like configurations and supportive policy development. But we also recognize that every client environment is different so we ensure that we maintain the right set of partnerships to meet our end-users' needs.

Q: Are you working with any telecom providers or MNOs?

GE: MNOs and telecom organizations are a key partner group for Sophos. On the one hand, we've been working with some of the world's largest telecom and MNOs (Mobile network operators) partners to embed some of our mobile security solutions into their own networks, to enhance their organizational security. But they have also been active in integrating our solutions – such as malware protection – into their own client solutions, meaning that a growing number of users are now using our solutions both in the office and outside of the enterprise.

Q: What advice would you give others in the mobile security market?

GE: Well, to corporate security leaders and executives, I would suggest that they do not underestimate the mobile security challenge. In the past three years alone, we've seen more than 100,000 new malware programs infect mobile devices and this number is growing exponentially. So for corporate clients, my advice would be that mobile security considerations be embedded into their IT architecture as quickly as possible.

For systems integrators, tech firms and telecom partners, I would suggest that the most important advance that we could make as a sector right now is to develop and adopt security standards. Systems integrators and MNOs, in particular, are in a position of strength to start pushing for standards and building out standard environments. The need to standardize should be pretty high on the priority list for our sector.

Five key takeaways

1. **Trust will always be king:** Building trust with customers – consumer or corporate – will be key to creating new opportunities in mobile security. But it will take more than a clean bill of health; players in this space will also need to be open and transparent with their customers in order to foster a stronger and more trusting relationship.

2. **Mobile security will always be a hot topic:** As mobile penetration skyrockets, the demand for greater security and privacy assurances on mobile devices and networks will reach fever-pitch. Those that are able to leverage their reputation and assets to create new and effective security products and services will gain a clear advantage in this market.

3. **Partnerships will be critical:** Like it or not, neither telecom nor technology companies can (at this point) deliver an end-to-end solution without developing mutual partnerships with clients, service providers and even each other. In many cases, the success of partnerships will depend on how they are structured and how the resulting customer data is shared.

4. **Opportunity lies in moving up the value chain:** For both telecom and technology companies, moving up the value chain will deliver new benefits and opportunities in the mobile world. Expansion into managed services, for example, or solutions integration, will provide tech and telecom providers with an opportunity to create sustainable new revenue streams.

5. **Success waits for no one:** Much like the technology itself, mobility-enabled business models are rapidly evolving and creating new opportunities in mobile security for those in the telecom and technology sectors. Success, however, will require not only a keen sense of the shifting marketplace and customer demands, but also a strong capability to develop and deploy new services at the speed at which the market demands.

Sources

[i] Refer to world bank statistics: http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/0,,contentMDK:22551641~pagePK:146736~piPK:146830~theSitePK:258644,00.html.

[ii] The app that can find parking spaces. http://www.dailymail.co.uk/news/article-2184174/The-app-parking-space-street-sensors-alert-drivers-bay.html.

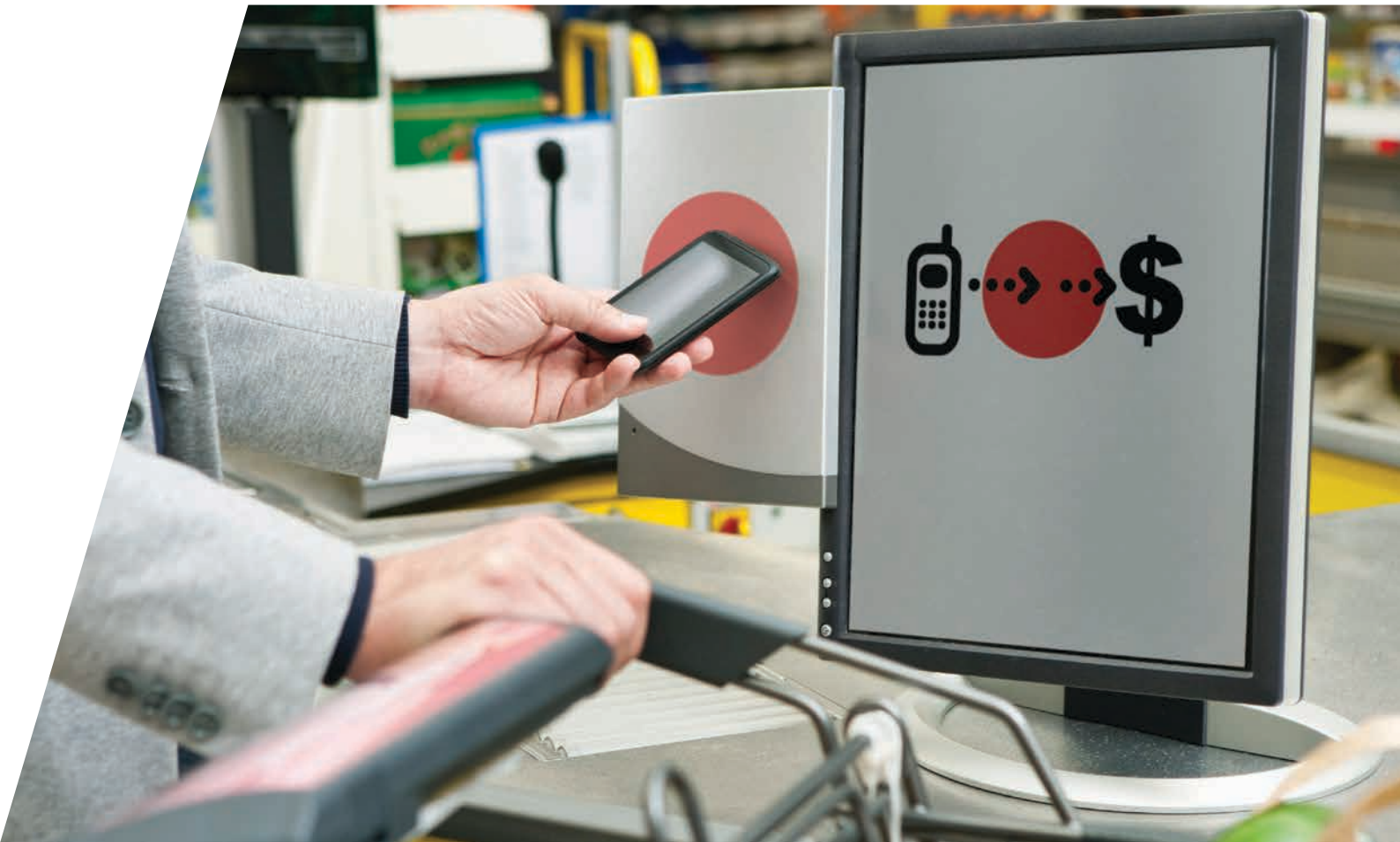
[iii] Interview with the Federal Communications Commission (FCC) Chairman at the 2012 Rutberg Wireless Influencer's conference.

[iv] For details, see Appthority's February 2013 app reputation study. Available at https://www.appthority.com/appreport.pdf.

[v] Jason Hong's study of Angry Birds and other apps revealed that few users are aware that the apps they are using are collecting or storing their location information. This work was mentioned in a NYT's article. http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html?_r=0.

[vi] Data volume report from AT&T annual report. Also reported in John Donovan's Blog entry: http://www.attinnovationspace.com/innovation/story/a7781181.

[vii] Secure Element can provide secure key storage, but is not suited to secure general purpose applications.



Acknowledgements

We would like to thank the following people for their valuable contributions to this report:

The Forrester Research team, in particular: Dan Klein, Demetrios Frangos, Chenxi Wang and Brad Kennedy.

Interviewees: Barry Johnson and Michael Singer at AT&T, and Gerhard Eschelbeck at Sophos.

The KPMG International project team: Joanna Wells, Natalie Cousens, David McAllister, Jennifer Samuel, Margaret Johnston, plus our external writer Peter Schram.

The KPMG contributors: sponsoring partner Sanjaya Krishna, plus Greg Bell, Martin Sokalski, George Thompson, Alfred Koch, Tim Miller and Tudor Aw.

KPMG contributors

Sanjaya Krishna
KPMG in the US
T: +1 212 954 6451
E: skrishna@kpmg.com

George Thompson
KPMG in the UK
T: +44 207 311 5117
E: george.thompson@kpmg.co.uk

Greg Bell
KPMG in the US
T: +1 404 222 7197
E: rgregbell@kpmg.com

Alfred Koch
KPMG in Germany
T: +49 211 475-7106
E: alfredkoch@kpmg.com

Martin Sokalski
KPMG in the US
T: +1 312 665 4937
E: msokalski@kpmg.com

Tim Miller
KPMG in Australia
T: +61 2 9455 9182
E: tjmiller@kpmg.com.au

Contact us

Gary Matuszak
Global Chair
Technology, Media & Telecommunications
T: +1 408 367 4757
E: gmatuszak@kpmg.com

Graeme Ross
Global Chair
Media & Telecommunications
T: +44 207 311 3372
E: graeme.ross@kpmg.co.uk

Malcolm Marshall
Global Information Protection and Business Resiliency Leader
T: +44 207 311 5456
E: malcolm.marshall@kpmg.co.uk

Media & Telecommunications Regional Contacts

Europe, Middle East & Africa

Joe Gallagher
T: +44 207 311 3044
E: joe.gallagher@kpmg.co.uk

Americas

Carl Geppert
T: +1 303 295 8827
E: cgeppert@kpmg.com

Asia Pacific

Peter Mercieca
T: +61 2 9455 9155
E: pmercieca@kpmg.com.au

Technology Regional Contacts

Europe, Middle East & Africa

Tudor Aw
T: +44 207 694 1265
E: tudor.aw@kpmg.co.uk

Americas

Gary Matuszak
T: +1 408 367 4757
E: gmatuszak@kpmg.com

Asia Pacific

Yoko Hatta
T: +81 36 22 98 350
E: yokohatta@kpmg.com

kpmg.com/socialmedia

kpmg.com/app

Available on the App Store

Designed by Evalueserve.
Publication name: Mobile security: from risk to revenue
Publication number: 130529
Publication date: September 2013