SAMSUNG

White Paper:

Tactical to Strategic: A Guide to Assessing Your Enterprise Mobile Security

Introduction

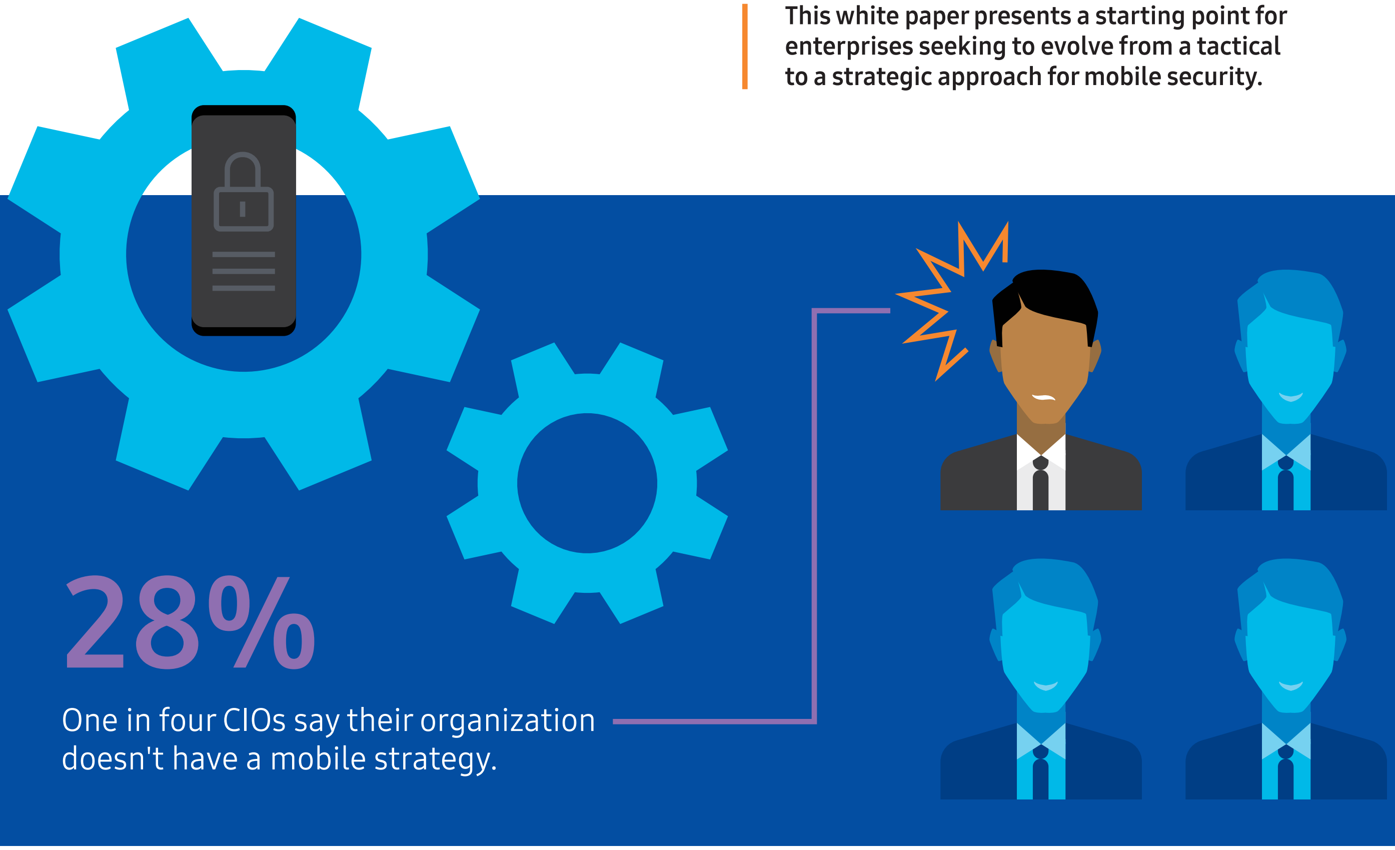
From BYOD to shadow IT to disparate homegrown or imported applications, many organizations are finding that mobile is happening, but no one is steering the ship. Companies that want to use mobile to create a competitive advantage need a mobile strategy tightly linked to business objectives while providing a risk management foundation that drives innovation.

According to a recent report by Robert Half Technology, one in four CIOs (28 percent) say their organization doesn't have a mobile strategy.[1] However, trying to dial back mobile because it's complicated isn't the answer. Employees have already proven they'll find workarounds to use the devices and apps of their choice. Instead, organizations need to accept that mobile usage will continue to grow and find a way to manage its pervasiveness and transform its role from tactical to strategic - and this includes making your organization's mobile security efforts more strategic as well.

A comprehensive mobile security assessment should evaluate mobile device management (MDM), mobile application management (MAM), and security and threat protection across the organization. It must consider not only the security effectiveness in these areas but how security protocols align with overarching business needs. An effective realignment requires both senior-level commitment and cross-enterprise collaboration.

There are a number of steps your organization should take in order to develop an effective mobile security roadmap that supports your organization's business goals.

This white paper presents a starting point for enterprises seeking to evolve from a tactical to a strategic approach for mobile security.



28%

One in four CIOs say their organization doesn't have a mobile strategy.

Step 1. Establish a Mobile Center of Excellence

A successful MCOE is able to stratify and understand what the business wants to achieve, and apply an appropriate security architecture that enables the business to accomplish its goals.

One of the first steps your organization can take to move mobile from a tactical to a strategic position is to develop a Mobile Center of Excellence (MCOE). When approached appropriately, an MCOE provides the leadership and the cross-enterprise activities necessary to align mobile initiatives and policies, including security, with the strategic goals of the business. When implemented well and linked to the business needs, a secure mobile environment can become an enabler of innovation and transformation. Additionally, because of the MCOE's cross-functional efforts, mobility becomes everyone's responsibility, not just IT's.

Best practices for building an MCOE that can achieve these goals include:

Defining the scope and charter of the MCOE:
At the outset, determine which aspects of mobile policy and strategy the MCOE will focus on and where the MCOE's authority to enact policy decisions begins and ends.

Securing executive sponsorship and financial levers:
Strong executive leadership is critical to an effective MCOE. Without support from the top of the organization, it will be difficult to gain the political power necessary to enact change. Similarly, the MCOE's influence on funding, whether as a direct control with its own funding or an approving step to demonstrate alignment with the mobile strategy, will establish the MCOE's ability to succeed in driving strategic mobile activities.

A security strategy is only successful if it provides a way for the organization to meet its business needs.

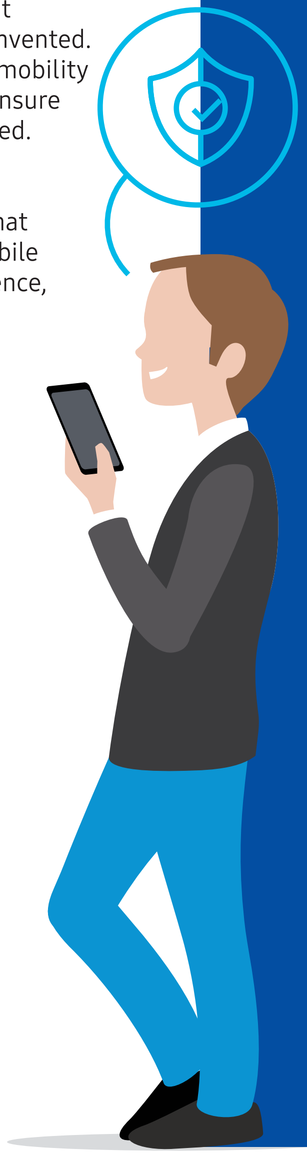
Establishing a partnership between LOBs and IT: Because mobility affects the entire organization, all departments need to play an active role in developing a mobile strategy. In particular, LOBs have unique insight into the areas of the business where mobile technologies could result in greater productivity or revenue in addition to opening new doors to innovation. Both membership in the MCOE and active participation from LOBs are needed.

Understanding end users' mobility needs: Security that doesn't meet end users' needs or that makes using devices overly complex will be circumvented. Gaining insight at a granular level into end users' mobility usage behavior, preferences and needs will help ensure that security protocols will work when implemented.

Focusing on security architecture: Organizations need an overarching architecture that defines the key contexts and requirements for mobile security, including addressing mobile user experience, security protocols, and app and BYOD guidelines.

Embedding a mobile security strategy within the organization's overall mobile strategy: A security strategy is only successful if it enables the organization to meet or exceed its business needs. Mobile strategies should look at how to use mobile to enhance productivity, innovate to generate new revenue streams and streamline collaboration. Layered on top of this, mobile security strategies should focus on managing risk while maintaining usability and operations to enable appropriate risk-taking in the business without sacrificing critical security.

A successful MCOE is able to arrange, classify and understand what the business wants to achieve, and apply an appropriate security architecture that enables the business to accomplish its goals. This requires making sure the technology is useful and enhances employees' jobs. And where mobile technologies interface with customers, there should be a strategic plan in place that addresses how to meet business objectives while keeping both customer data and corporate data secure.



The Samsung Enterprise Mobile Security Stack

Samsung's Knox platform and suite of mobility management tools provides a defense-grade foundation to take your mobile security to the next level.

The Knox Platform

Built into Samsung smartphones, tablets, and wearables at the manufacturing stage, the Knox platform consists of overlapping defense and security mechanisms that protect against intrusion, malware, and more malicious threats. Samsung Knox integrates closely with Android Work Profile and leading EMM solutions including Airwatch, BlackBerry and MobileIron.

Knox Configure

Remotely configure a large number of Samsung devices and tailor them to specific needs.

Knox Mobile Enrollment

A quick, automated way to enroll a large number of devices to your EMM for corporate use.

Knox Manage

An affordable, cloud-based EMM solution to manage your enterprise devices.

Knox Workspace

A managed, secure container to isolate business data and apps from personal ones.

Learn more: samsung.com/knox

Step 2. Establishing a Balance

Corporate data is being shared via mobile devices at an alarming rate. Not surprisingly, this data is at risk. In a survey by the Ponemon Institute, 67 percent of organizations said it was certain or likely that they had a data breach as a result of employees using their mobile devices to access sensitive and confidential company information.[2]

The survey also found large discrepancies between the data that IT claims employees have access to, and what employees say they can access via mobile devices. For example, 33 percent of employees say they have more access to confidential or classified documents, while only 8 percent of IT says that employees have this access.[3]

While the initial reaction to statistics like these may be to further lock down company data, this is a losing proposition, especially if one of the main drivers of mobility is to increase productivity. Organizations must balance security compliance and risk against employee productivity, privacy and trust. A key aspect of most enterprise mobile security solutions is using an MDM solution. However, Gartner predicts that 20 percent of BYOD programs will fail because IT is trying to implement MDM solutions that are too restrictive.[4]

Partnering With Lines of Business

To develop the right balance between securing data and enabling employee productivity and privacy, MCOEs should leverage their partnership with LOBs to create a mobile security strategy that simultaneously meets end users' and LOBs' needs. The strategy should include best practices such as the ability to provision devices, set passwords and take advantage of biometric authentication options, back up data and wipe devices when an employee leaves or a device is lost.

At the same time, the security protocols must be careful not to go too far and need to provide employees with confidence that the company will not impact their personal use in BYOD scenarios. For example, a containerized MDM solution that allows IT to selectively wipe corporate data while leaving personal data untouched provides an effective way to balance secure employee productivity and personal use of the device.

To build trust and compliance, IT should ask users to opt into mobile security policies, but be prepared to revoke or limit access for users who are unwilling to do so or are using devices that cannot be brought into compliance with company policies. They should also make sure that password and authentication protocols aren't too cumbersome, and that they maintain high security standards without limiting employee productivity. This means finding a balance between the length and complexity of passwords required, as well as retry and timeout standards, or leveraging easy-to-use, secure biometric authentication options. Ultimately, when mobile device management practices are well designed and based off of business needs, both the end users and the organization as a whole benefit.

Develop mobile security strategies that will protect your data.

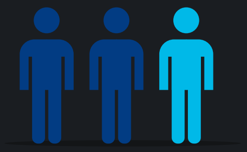
67% of organizations think they may have already experienced a data breach due to data being mobile or accessible from mobile devices.[2]

Communicate with employees how to manage confidential data on mobile devices.

33% of employees say they have more access to confidential or classified documents than they previously had.[3]

Manage and enable the reality, not the perception.

8% of IT teams think employees have access to confidential data, but the reality is that one-third of employees in your company are likely to already have access on their devices. [3]



Step 3. Manage Your Enterprise Apps

With the pervasiveness of mobile devices in the workplace, the number of applications that run on these devices is also spiraling upward.

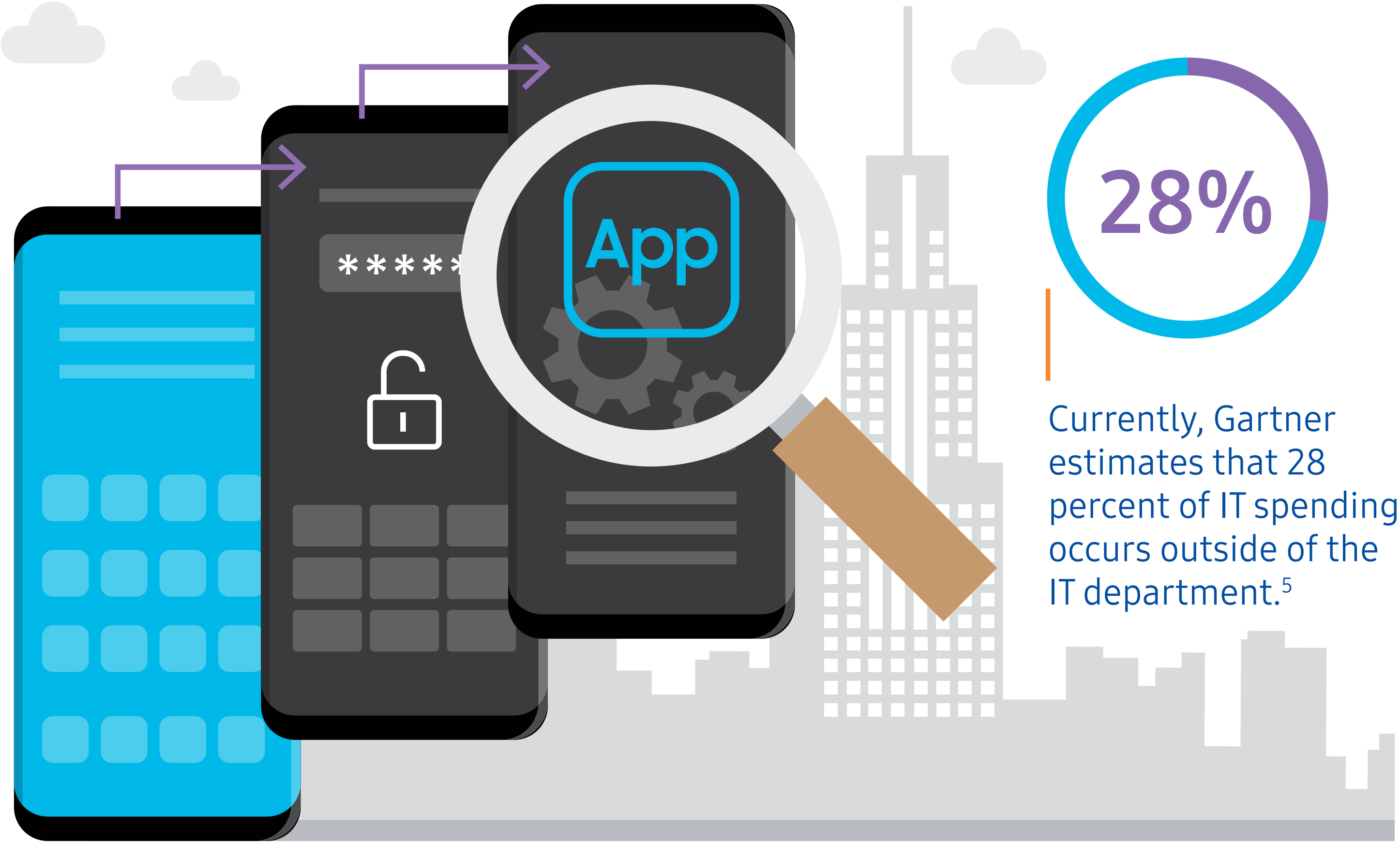
It's difficult for IT to find ways to deliver and manage these applications and protect confidential information, in part because employees and LOBs frequently circumvent the IT department when they deploy apps. Currently, Gartner estimates that 28 percent of IT spending occurs outside of the IT department.[5]

To achieve appropriate security measures while driving productivity and innovation, IT and LOBs need to partner, rather than circumvent each other. Containerization on mobile devices, which allows for the separation of personal data from business data, gives LOBs and their end users more confidence that they can use their personal devices productively for business without risking an encroachment on their privacy or personal data loss if a device is lost and needs to be wiped. At the same time, separating business and personal apps allows IT more control of the business environment and what applications can be accessed and utilized.

Even with containerization, in order for IT to effectively manage applications and protect critical data assets so that business needs are met and security is enhanced, MCOEs need to develop clear and consistent policies around mobile app development, management and distribution.

App Development

Whether addressed as part of an overall security architecture or part of its app management strategy, MCOEs need to determine which model they'll use for specific applications — native client, HTML5 or a hybrid approach. Along these same



Currently, Gartner estimates that 28 percent of IT spending occurs outside of the IT department.[5]

lines, app development policies need to address how the app life cycle, such as version control, code re-use and so on, will be managed in addition to building security into the software development lifecycle.

App Management

End users and LOBs will have strong preferences for specific apps that improve their productivity. But, given that Gartner predicted that by 2017, 75 percent of mobile security breaches will be the result of mobile application misconfiguration,[7] organizations can't take the risk of leaving app management up to end users. The key to an effective MCOE is to allow the use of apps that clearly offer business value, while securing the data the apps have access to.

This is tougher than it may sound, especially since many business applications need access to corporate resources and systems that sometimes interface with existing systems, such as CRM solutions. Whitelisting or blacklisting certain apps is one way to control what end users are allowed to access. Educating end users on using only applications that come from reputable sources, such as well curated app stores like Google Play and Apple's App Store, will also help minimize risk, as most infections on mobile devices come from third-party app stores.

For cloud-based applications, leveraging secure communications channels along with encrypting data at rest and enterprise-managed access controls can also add additional layers of security. Containerization, as discussed previously, is another way to help keep corporate data secure and separate from personal data, and all users should be required to have current anti-malware software installed on their devices. Finally, IT needs a way to update and manage apps over time to ensure they remain secure. Many MAM solutions on the market can help manage this process.

App Distribution

The most common way for users to add apps to their mobile devices is through an app store or another public app distributor. However, using the public marketplace provides little control for IT and can put sensitive data at risk. Alternatively, MCOEs can set up a different app delivery model that can still provide access to applications employees need, while creating a more secure environment.

Here's a comparison of private versus public app distribution models:

1. Private app store: Instead of using the public marketplace, IT can create its own app store. The advantage to this approach is that it allows IT to not only vet what applications are acceptable for download, but it makes regulating compliance, data, bulk purchasing and licensing simpler for them. The downside of this approach, though, is the high investment in resources required to maintain a private app store.

2. Public app store: Public app stores such as Google Play and Apple's App Store are familiar to most end users, easily accessible, and don't require resources to maintain. On the downside, with millions of applications available for download, IT maintains less control over what applications are accessed, and it can be difficult to publish certain enterprise apps through these public app stores. Additionally, while most apps in Google Play and Apple's App Store are secure and pose little risk, other third-party app stores can pose significantly higher risks. IT must be careful to educate employees about these risks.

Ultimately, determinations about how apps are developed and what management and application practices to put into place should be driven by overall business needs. MCOEs should set policies that take into consideration the risks that applications — particularly cloud-based apps — pose, the productivity and business value they provide, and end user input. Of course, the real key for all mobile applications is designing a user experience to support productivity, but this goes beyond the scope of our discussion here.

Step 4. Conduct a Mobile Security Assessment

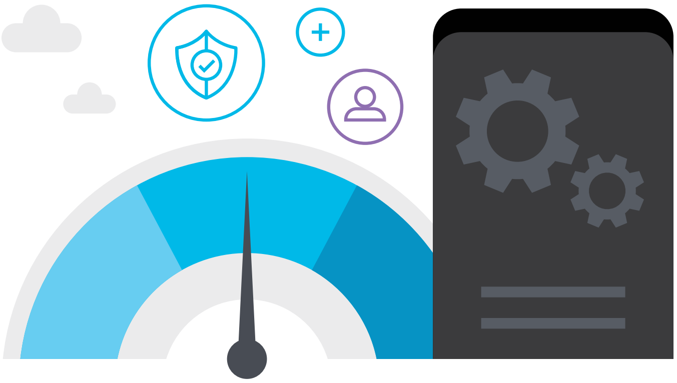
Mobile device security starts and ends with end users. They have the ability to install apps, reconfigure settings and back up their data (or not). Making sure they understand the risks and how their actions affect these risks is key.

The MCOE should next guide a mobile security assessment to comprehensively assess the maturity of the organization's mobile capabilities using a mobile security maturity model and framework that considers technology, processes and skills. The assessment should cover several specific topics including:

- Risk tolerance
- Vulnerability assessment
- Information risk assessment
- Threat vector identification
- Asset management

Risk tolerance is different for each organization. A small business will have different security needs and risk tolerance than a large financial institution or a healthcare organization with numerous regulatory mandates. Therefore, the first step is to determine an acceptable risk level when weighed against the broader benefits of mobility. With tolerance levels defined, the organization can then assess what preventative measures are acceptable and implement them accordingly.

Using a vulnerability assessment, organizations can determine where their biggest weaknesses lie — whether it's with end users, not having two-factor authentication or a lack of a BYOD policy. Once vulnerabilities are identified, organizations can then apply solutions that take into consideration their risk tolerance. For instance, if there's little risk tolerance around data loss, then two-factor authentication is a non-negotiable feature on employees' phones. On the other hand, if there's low-value data with little business impact of data leakage and a significant demand to improve productivity in the field, authentication steps and other security controls may be less onerous.



It's also important to assess where the vulnerabilities are occurring and what data is essential to protect. For example, a company may determine that new product designs and correspondence about the new product are highly confidential. But, on assessing the actual information risk, they may find that the detailed design files that seemed to be the greatest risk are in fact encrypted and rendered unreadable on a mobile device. The real risk then may be email and instant messenger threads discussing the product and its design that are being read and responded to on mobile devices — and this is where the company needs to focus their efforts to secure the intelligence on mobile devices.

As part of its security assessment, the MCOE should also identify threat vectors that create vulnerabilities or open the door to threats. Mobile device security starts and ends with end users. They have the ability to install apps, reconfigure settings and back up their data (or not). Making sure they understand the risks and how their actions affect these risks is key. The dialogue should be ongoing, as the risks and threats are as ever-changing as the technology itself.

Along these same lines, organizations should also enact measures to prevent device loss. All corporate devices should be tracked with inventory tools such as bar codes or QR codes. Another good prevention mechanism is to activate a "find my phone" application on end users' devices. These apps can use GPS tracking, lock phones or put phones in alert mode. Some even have the ability to use the phone camera to photograph anyone trying to access the phone.

At the end of the day, a mobile program that provides risk management from mobile threats hinges on a number of factors. These include involving end users in the security dialogue early on, ensuring that there's a solution in place for mobile device management and app and data management. Tools and processes are needed to help continually monitor and quickly analyze and react to threats.

Take Control of Security

As mobility continues to rise in the workplace, a head-in-the-sand approach simply won't work. Instead of letting mobile "happen," organizations need to take control.

But control must be holistic, comprehensive and add value to the business. This paper outlines the first four critical components of developing an effective mobile security strategy:

1. Establish an MCOE
2. Protect your business data
3. Manage your enterprise apps
4. Conduct a mobile security assessment

By putting together a clear mobile security roadmap, IT leaders allow their organizations to mitigate risk and drive greater innovation. Samsung's mobile expertise and industry-leading mobile security solutions can help in your to transition from tactical to strategic mobile management. Visit the pages listed below and contact our mobile consultants to find out how.

Learn more about Samsung's Mobile Security Solutions
samsung.com/knox

Learn more about Samsung Business Services
samsung.com/us/business-services

Footnotes

[1] Josh Brost, "1 in 4 CIOs Say Their Organization Doesn't Have a Mobile Strategy," Robert Half Technology, March 25, 2014, https://www.roberthalf.com/technology/blog/1-in-4-cios-say-their-organization-has-no-mobile-strategy.

[2] "The Economic Risk of Confidential Information on Mobile Devices in the Workplace," Ponemon Institute, Feb. 2016.

[3] Ibid.

[4] "Gartner Predicts 20% of BYOD Programs Will Fail in the Next Two Years," Unified Communication Strategies, Jan. 14, 2014, http://www.ucstrategies.com/unified-communications-newsroom/gartner-predicts-20-of-byod-programs-will-fail-in-the-next-two-years.aspx.

[5] "Bring Shadow IT Out of the Dark," EnterpriseTech, June 17, 2015, http://www.enterprisetech.com/2015/06/17/bring-shadow-it-out-of-the-dark-gartner-tells-tech/.

[6] Nick Earle, "Do You Know the Way to BalleyLickey? Shadow IT and the CIO Dilemma," Cisco, August 6, 2015, http://blogs.cisco.com/cloud/shadow-it-and-the-cio-dilemma.

[7] "Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration," Gartner, May 29, 2014, http://www.gartner.com/newsroom/id/2753017.