Mobile technology has revolutionized the way millions of people do their jobs. Employees now have unprecedented levels of flexibility, including the ability to work anytime from anywhere. Thanks to mobile collaboration apps, they also have the tools to work with colleagues, business partners and customers from around the world.

For enterprises, the resulting increase in employee productivity can translate into faster response time, more revenue and higher margins, outcomes that make mobile technology attractive to businesses of all sizes.

With this great opportunity comes a formidable challenge, especially for IT professionals. That’s because the key driver of mobile technology in the enterprise is consumerization—insistence by employees that they use the devices and apps of their own choice personally and professionally.

Consumerization is forcing enterprise IT to adopt a user-centric perspective, the exact opposite of IT’s longstanding practice of control and centralization. Enterprise professionals now must manage a multitude of mobile devices running on an increasing number of platforms and mobile operating systems. In addition, they must try to secure and manage enterprise data being accessed by and stored on numerous mobile devices.

Understanding your “mobile ecosystem” is key to comprehensive security.
Further, thousands of consumer mobile apps, including cloud storage apps such as Dropbox and Box, are being used by employees to access and store enterprise data. We’ve gone past BYOD (Bring Your Own Device), BYOC (Bring Your Own Cloud) and BYOA (Bring Your Own Apps) to BYOX (Bring Your Own Anything).

Consumers and enterprise workers aren’t the only ones leveraging mobile technology. The explosion of mobile devices and applications has attracted hackers, phishers and creators of malware, all trying to exploit network and device vulnerabilities to steal enterprise, personal and financial data as well as money.

The unique and rapidly evolving security considerations spawned by consumerization and the mobile revolution make it imperative that enterprise professionals adopt a clear-headed and coherent approach to mobile security. Not only does enterprise IT need the right security tools, it needs the strategic framework and policies that allow IT to effectively balance the freedom and flexibility mobile offers employees against the vital need to protect enterprise data and hardware assets.

**Conduct a security assessment**

So where should IT professionals begin when creating a mobile security strategy? Barry Johnson, a senior product manager for AT&T’s Managed Security Services, says enterprises trying to get a handle on mobile security must first focus—on everything.

“You’ve really got to look at the whole mobile ecosystem to start pulling together a cohesive, comprehensive mobile security strategy,” Johnson says. “You can’t just focus on one thing. You have to have a security posture around the devices, and that inevitably gets into operating systems and application usage. Then there are the internal enterprise applications or platforms that mobile devices are accessing along with how enterprise data is getting to and from those devices into the enterprise-hosted or cloud-hosted applications.”

The first tangible step in establishing a mobile security strategy is what Johnson calls a “posture assessment.”

“Have professionals come in and start a dialogue around where you are today from a security perspective for your mobile environment, as well as where you need to be,” he says. “That way you’re not just creating a tactical method; you’ve got a real strategy that you can build to over time.”

In this initial assessment phase, enterprises and the mobile security professionals they engage need to gain a clear picture of:

- The various mobile devices and OS platforms employees are using
- The types of applications employees use, including cloud storage apps
- Which enterprise data is being accessed by mobile workers

**The explosion of mobile devices and applications has attracted hackers, phishers and creators of malware, all trying to exploit network and device vulnerabilities to steal enterprise, personal and financial data as well as money.**

It’s also critical to determine why employees are using particular devices and apps. That’s because any effective enterprise mobile strategy must begin with the needs of the user and work back from there. In the consumerization age, employees no longer feel obligated to use the hardware and software tools provided by enterprises; they want what works for them. IT must provide enterprise mobile security within that context.

Once IT understands the current level and type of mobile use within the enterprise, it can devise security policies that empower employees while offering reasonable safeguards against data loss and device theft.

**To BYOX or Not to BYOX**

To be effective, mobile security policies must be designed around the type of mobile program enterprise decision makers choose. “The most fundamental question is whether you will provide devices to employees, contractors or partners,” says Johnson.

Enterprises that issue mobile devices to their workforce have some “flexibility around what sort of policies they’re going to dictate,” he says. And that’s because “the company owns that device and any data on it.”

Nonetheless, in such a “company-owned” mobile scenario, it’s important to spell out what rights the enterprise has and make sure these are communicated to employees. “Have an acknowledgment on file that the employee is using a company device and that any data they put on that device is susceptible to visibility to the corporation,” Johnson says.

Strictly company-owned mobile programs, though, are (or soon will be) in the minority. A Tech Republic survey from August 2013 shows that 62% of enterprises plan to support BYOX by the end of this year, up from the 44% already allowing BYOX at the time of the survey.

Not surprisingly, BYOX makes devising mobile security strategies and policies “infinitely more complicated,” Johnson says.
One reason BYOX increases complexity is the sheer number of platforms in use. New research from IDG shows that enterprises support and purchase devices—including smartphones, tablets and laptops—across an average of seven OS platforms. Effective mobile enterprise management (MEM) solutions can enable enterprise security professionals to support numerous types of devices running across multiple mobile OSes such as Android, iOS and Windows.

The major reason that BYOX complicates the development and implementation of mobile security policies is that enterprise data resides on a device owned by an employee rather than the business. This raises tricky questions about ownership and rights if policies aren’t clear (and clearly communicated) to enterprise BYOX workers.

“There has to be a clear delineation between the personal data and the business data,” he says.

There are two parts to this challenge: 1) Making sure employees understand their rights and responsibilities regarding the enterprise data residing on and accessed by their devices; and 2) Ensuring IT has the tools to manage enterprise data on employees’ mobile devices, as well as the devices themselves.

**Contain to control**

Whether an enterprise uses an off-the-shelf mobile device management solution or engages a managed services provider, the ability to create a mobile workspace (similar to containerization) separating personal and corporate data residing on an employee-owned device is paramount to fundamental mobile security in a BYOX environment. Users simply switch between their personal and work containers.

Providing a mobile workspace enables IT security to remotely wipe enterprise data on an employee’s personal mobile device in the event of loss, theft or termination, without deleting personal data. This option also allows IT security professionals to implement and enforce mobile access policies on the enterprise side of an employee’s device.

“'You have to enable security as seamlessly as you can within that workspace environment and tap into all those enterprise policies that inevitably have to be enforced,” Johnson says. “You can build policy to steer all enterprise-specific traffic to a focal point, so in essence you’re locking Dropbox type of activity out of the business environment. And from there you can build your traffic and application-level policies on your business traffic alone.”

Those policies should include procedures for authenticating both users and mobile devices attempting to access enterprise data and applications. In a mobile environment, single-factor password protection isn’t sufficient. Two-factor authentication is more secure, making network or device breaches less likely to occur. But it’s important that two-factor authentication and other security layers don’t hamper employee productivity or complicate access.

Finally, mobile devices should include anti-virus and anti-malware software that can scan the devices and memory cards for malicious applications and code to prevent enterprise networks and data from being contaminated.

**Securing data in the network**

While securing mobile devices—through passwords, authentication, containerization and application controls—is an essential part of enterprise mobile security, at some point data must move to and from the devices being used by employees. Enterprises can protect this data by enabling network access for mobile devices through a virtual private network (VPN) and encryption.

“Encryption is absolutely a necessary part of mobile security, both at the device level and while data is in motion,” Johnson says.

It’s also important for mobile security professionals to control which applications are allowed to access enterprise data.

“'Being able to block traffic at the application level is critical,” says Johnson. “Assuming you have some sort of container or mobile workspace environment, you can build policy to steer all enterprise-specific traffic to a focal point, so in essence you’re locking Dropbox type of activity out of the business environment.”

**Passing through the cloud**

The reality of modern network computing, however, is that enterprises increasingly rely on cloud-based storage, backup and application delivery as a way to reduce costs, enhance scalability and speed deployment.

**Two-factor authentication is more secure, making network or device breaches less likely to occur. But it’s important that two-factor authentication and other security layers don’t hamper employee productivity or complicate access.**
For small and mid-sized enterprises especially, a cloud-based mobile data and apps delivery can save money on hardware and software purchases and free up IT staff to focus on other things. Enterprises can generally pay for mobile apps delivered through the cloud on either a monthly or per-user basis, which reduces up-front costs and enhances flexibility.

Whether these clouds are public, private or some kind of hybrid, they represent potential security hazards for enterprise data.

Yet the advantages of combining mobile and cloud technologies are too compelling for enterprises to ignore. An August 2013 survey by Frost & Sullivan shows the percentage of businesses that use only on-premise servers to implement mobile apps fell to 27% from 36% in 2012. The survey also shows that 33% of enterprises use pure cloud-based mobile apps delivery, up from 30% in 2012, while hybrid on-premise/cloud mobile apps delivery increased to 40% from 34%.

That trend undoubtedly will continue, despite concerns about mobile data security. Enterprises that want to leverage their mobile apps through the cloud should use a holistic MEM solution that helps protect data from the network through the cloud and to the device while enforcing enterprise mobile policies such as device and user authentication.

**Getting users on board**

Mobile security professionals must establish and communicate clear rules and expectations regarding how employees secure their devices, which apps they use, and how they must access enterprise apps and external cloud services. Specifically, enterprise mobile security professionals should:

- Train employees on the security features of their mobile devices, particularly screen locks, encryption and procedures to follow if their device is lost or stolen.
- Spell out the enterprise’s policy regarding wiping data from missing or stolen devices.
- Create a list of whitelisted and blacklisted mobile and cloud apps.

Most importantly, an enterprise’s mobile and/or BYOX policy—no matter how carefully crafted or well-intentioned—is doomed to fail if it doesn’t work for employees. Workers who are proficient with their own iPhones, for example, will resent being forced to use company-issued BlackBerry devices with which they are unfamiliar because it will make them less productive, efficient and happy.

Consumerization and BYOX are driven by the needs of the user. If enterprises create restrictive policies regarding which devices and apps can be used for work, employees could become frustrated and either ignore the policies (creating more potential security problems) or simply be less productive because they’re not using the tools of their choice.

The goal should be to create a secure mobile environment that allows employees to use devices and apps “without feeling so ratcheted or locked down that they can’t do the things they need to do to get through the business day,” Johnson says.

**Summary**

Enterprises that want to implement a sound mobile security strategy should conduct a mobile security assessment with the help of managed security services consultants. Before developing specific mobile security strategies and policies, determine whether you want a pure BYOX, a “corporate-owned” or a hybrid environment.

- Create a mobile security strategy that protects data on the device, in transit, and from cloud services.
- Train and communicate with employees regarding mobile security policies, practices, rights and responsibilities.
- Perhaps most critically, enterprises should expect their mobile security policies to evolve over time as employees gravitate to new platforms, apps and devices (such as wearables).

“No security posture is going to remain static,” Johnson says. “It’s something that a managed security services provider or the customer security operations team needs to put in place and then remain flexible.”