BRIEFING SHEET

Channel Partners™

Managed Mobility Is Secure & Cost-Effective Mobility

If your mobility program consists of unfettered mobile data usage and IT passing out expensive smartphones — or letting any user-owned device access your network — you are spending too much and putting sensitive information at risk. Investments in mobility management and telecom expense optimization may save money and protect your brand from a damaging ransomware attack, even a data loss that requires public disclosure.

MARKET MOVEMENT: Limiting mobile programs isn't a viable plan. Your peers in the United States and abroad are investing: Worldwide spending on mobility-related hardware, software and services is forecast to exceed $1.6 trillion in 2018, according to IDC's new **Worldwide Semiannual Mobility Spending Guide**, on the way to surpassing $1.7 trillion by 2021. For comparison, the entire 2016 GDP of Canada was $1.53 trillion.

BUSINESS BENEFIT: A more productive, secure, connected workforce is the goal of all mobility programs. Which model to choose?

BYOD: Employees may use any device to access the company's apps, email and data. Employers may provide a monthly subsidy.

Pros: Employees purchase their own devices, so they tend to be more careful with the hardware. They are using a device they're familiar with, which minimizes support calls, and if they watch hours of YouTube videos on their own data plan, that's on them.

Cons: BYOD brings security and data management challenges. There must be enforceable policies around the handling of company data and that requires some sort of enterprise mobility management tool. The business does not own the phone number, so a salesperson who moves to a competitor takes those contacts with them. There are ways around this that your adviser can explain.

COMPANY-OWNED: The employer purchases and issues the device and pays for call, text and data usage.

Pros: You have control and can mandate tight security and affordable data and voice plans, as well as set terms and conditions around use. You can track employees, capture email and text messages, and retain ownership of information placed on the device. This is often the best choice in regulated industries.

Cons: Employees may question why their employer needs that amount of information and raise privacy complaints. If an employee uses an excessive amount of data or loses a device, that cost is on you.

TECHNOLOGY ELEMENTS: A mobility management program may include MDM (mobile device management), EMM (enterprise mobility management) or MAM (mobile application management), as well as telecom expense management and specialized endpoint security products or services. Your trusted adviser can recommend the right mix for your business.

With modern mobility management tools, your IT team or a partner may set up secure containers for personal and corporate use. If a device is lost, you can wipe all business data and enforce rules for web browsing, passwords and authentication, as well as accessing corporate data such as email and documents. You can also control what applications may be downloaded.

Telecom expense management systems can now optimize cellular plans just as they help control wired line costs, possibly resulting in significant savings.

If you are in a regulated industry or have employees carrying sensitive data on their phones, ask your adviser about specialized endpoint security tools.

5 Gotchas to Avoid:

Ignoring security: Ransomware is getting into networks via mobile devices. These attacks rose more than 400 percent in 2017 over 2018. Good mobile management should include a rule regarding what apps may be downloaded — Trend Micro found 30,000 more malicious applications published on Google Play in 2017 than in 2016, and Apple's App Store has also been infiltrated.

Spending too much on hardware: Deciding among devices, upgrade tempo, leasing programs, locked or unlocked and payment plans can be extremely confusing. A trusted adviser can compare dozens of options from multiple manufacturers to get you the best fit and price.

Leaving out laptops and tablets: The term "mobile device" no longer simply means smartphones. For some companies, iPads or Surface tablets are displacing laptops for certain employees. The right mobility management platform delivers the tools to keep tabs on a company's potentially mixed and massive fleet of devices.

Not leveraging the cloud: Mobile employees expect the same user experience from their business apps, whether they're running on smartphones or desktops. This is where Office 365 and other software-as-a-service comes in.

Not upsizing your underlying infrastructure: In many offices, the network wasn't built to handle the high-volume traffic of a mobile workforce, which might have doubled or even tripled the number of devices a typical employee uses at work. Ask your adviser what effect external traffic from, say, a field employee accessing data from one of your critical databases will have on the network.