Teamwork, a clear vision and the cloud helped CDW develop a strategy to manage the influx of personal mobile computing devices that coworkers were bringing to — and using in — the office.

(From left to right) Steve Staines, Michael Pflieger and Travis Chavous helped CDW craft a strategy to reaping the rewards and mitigating the risks of a diverse mobile environment.

When CDW leaders saw a surge of smartphones and tablets streaming into their offices, they mobilized professionals from across the organization to address it.

CIO and Senior Vice President of Operations Jon Stevens “was quick to realize that this proliferation of mobile devices wasn’t going to stop,” explains Travis Chavous, senior manager of IT service management for the national technology solutions and services provider. “His vision was
Many organizations continue to struggle with managing and securing their mobile environments. Fortunately, the challenge has gotten easier, thanks to a comprehensive new portfolio of solutions and services that span each phase of implementation.

Total Mobility Management from CDW encompasses a full suite of best practices, applications and on-demand services to integrate, control and simplify all aspects of mobility management. Total Mobility Management also benefits from real-world validation: CDW developed and uses the offering's policies and tools to keep its own mobile workers productive and secure.

**Plan the Strategy:** CDW account managers and solution architects work with each customer to create a mobility roadmap, develop data and device policies, formalize a security strategy and understand network requirements.

**Enable Procurement and Provisioning:** CDW experts help customers design bring-your-own-device programs and create a procurement portal through which end users can administer their data plans, choose their mobile devices, deploy their selections, activate their accounts, and configure their smartphones and tablets.

**Protect with Centralized Management:** Integrated security technologies and policies control access to the organization’s network and keep information safe. Total Mobility Management gives organizations the tools they need to control devices, applications, content and BYOD policies. These resources also can be used to manage device and data plan expenses, and to monitor mobile activities in real time.

**Support IT and End Users:** Help desk services, warranty services and a portal that enables end users to manage their own mobile needs ensure that anytime, anywhere communications stay productive and efficient.

**Empower Customization and Enhancements:** By providing resources for custom application development, a customized app store and support for virtualizing desktops and applications, Total Mobility Management allows organizations to tailor their mobile environments to their own unique needs and opportunities.

Learn more about Total Mobility Management at CDW.com/mobility or download CDW’s mobile policy checklist at CDW.com/checklist.
4. Scalability and Viability: The plan had to remain relevant even as the mobile market continues to evolve.

One factor that didn’t loom large in the discussions was return on investment (ROI). Chavous says CDW’s desire to manage and secure a mobile environment for its 6,800 employees in Vernon Hills, Ill., and 24 other locations in the United States and Canada overshadowed the payback considerations that traditionally guide large-scale IT projects.

Bring-your-own-device programs and mobility have become “driving forces in all organizations,” Chavous explains. “We had to address the situation we were facing, rather than focus on achieving a predetermined ROI.”

Embracing BYOD

The team next turned to such fundamental decisions as who would pay for the devices and data plans. Ultimately, the team decided that a one-size-fits-all approach wouldn’t work, so it created a multilayered model with various options based on an individual’s role within the company.

Senior executives would continue to receive devices and services paid for by the company. Other professionals whose jobs require anytime, anywhere access to peers and company resources would receive stipends of up to $200 to pay for mobile devices. A formula determines a maximum dollar amount for each device type.

The third tier, which covers the largest segment of CDW’s mobile workforce, is BYOD. Participants may use their personal smartphones and tablets at work if they agree to follow the company’s usage policies and download an app from CDW’s mobile device management (MDM) platform.

“If the user’s device has the MDM application running, we don’t care if it’s a corporate-sponsored device or a personal one,” says Michael Pfieger, CDW’s senior director of IT operations. “We’ll treat everyone the same.”

Those usage policies included the following specific measures to protect information and company assets:

- Mobile devices must encrypt data stored on the hardware.
- Users can't install software blacklisted by CDW.
- External connections to the company networks require two-factor authentication.
- After a user makes 10 unsuccessful attempts to enter a password, the device is automatically wiped clean.
- “Jailbroken” or “rooted” devices, which have been altered to override vendor controls, are banned.
- Devices automatically lock after a period of inactivity.

A Firm Foundation

Even the best policies won’t guarantee success if a company can’t effectively implement and enforce them. To add oversight to its mobile strategy, CDW needed an MDM solution that would ensure that each device complied with internal usage rules before mobile workers accessed corporate resources.

In 2010, at the height of the mobile device influx, members of CDW’s 240-person IT team began evaluating MDM options, paying particular attention to ease of implementation and whether the solutions would meet all of CDW’s mobile management and security requirements.

Equally important was finding a solution that could support the diverse combinations of devices and operating systems in CDW’s existing environment.

They found their answer in MaaS360 by Fiberlink, an easy-to-configure software as a service option that didn’t require the upfront investments in hardware and storage that on-premises applications demand. It jump-started CDW’s MDM capabilities — the initial setup took only a couple of hours to configure.
To prevent potential support headaches for IT staff, the mobility team chose a self-service route, one that would give end users the tools they’d need to configure their own devices and troubleshoot common performance problems. “It’s very hard to support so many different types of devices with so many versions of operating systems,” Pflieger explains. “It gets almost unbearable because there are so many flavors and combinations.”

CDW had other practical reasons for minimizing support responsibilities in a BYOD environment. “We realized that the more we touched people’s personal equipment, the more liability we would take on,” Chavous explains. “So we created the basic configuration parameters and then got out of the general support business. As a result, the proliferation of devices hasn’t generated a lot of additional call volume for the service desk.”

Leveraging capabilities within the MaaS360 solution, CDW created a portal through which users can download the initial settings that devices need to connect to the network. Employee-owned devices are quarantined until their users follow emailed instructions on how to authorize their devices to access organizational resources. If a device isn’t rooted or jailbroken, the user is permitted to install the MDM application, which configures security controls. Within 10 minutes, corporate email is accessible through the device. “We’ve gone from having IT be involved with about 95 percent of the initial configurations before MDM to less than five percent now,” Staines says.

Of course, self-service doesn’t mean the IT support staff isn’t available if a mobile worker later needs assistance. “We never leave anybody hanging,” Staines continues. “We will always make our best effort to help a coworker resolve a problem, whether we work on it or refer the issue to the carrier to diagnose it.”

A dedicated procurement and expense management system that the mobility team established allows colleagues to order from an internal catalog of mobile devices and accessories, upgrade their devices or make changes to existing services. Managers benefit because the system breaks down mobile expenses by department for accurate chargebacks. Proprietary algorithms even flag accounts for which available minutes far exceed what users require, allowing CDW to save money by revising those account holders’ service plans.

To be successful, CDW’s mobile management strategy also hinged on a more robust wireless network. Prior to 2010, CDW’s network infrastructure could accommodate less than one device per employee. “When we saw a wave of people bringing in their smartphones and tablets, plus people working on notebook computers throughout the day, we realized the wireless network was getting overwhelmed,” Pflieger explains.

To accommodate colleagues who now carry a full-on-the-go arsenal, the mobility team relocated existing access points and added more to optimize coverage areas. Originally, CDW had configured the network with one connection point per user; after the upgrade, that ratio jumped to three connections per person.

“We made certain that the wireless network could handle today’s demands — and has room to grow,” Staines says.

**Clock Agnostic**

With the right policies and infrastructure to support ubiquitous mobility now in place, the 29-year-old company is enjoying the benefits of a closely connected workforce. Staff members have reliable access to corporate email, information and applications whenever they need it, using whatever device is appropriate for the task at hand.

At the same time, CDW has mitigated the security risks that can derail mobile strategies. “Our business is never 9 to 5, so we say, ‘Information anytime, anywhere, on any device,’” Pflieger explains. “And now we’re confident that we’re doing it in a way that’s both manageable and secure.”