Software

Why BYOD?

Build your case and lay the foundation for a successful BYOD strategy

The bring-your-own-device (BYOD) movement is gaining steam. Across a wide range of industries, organizations recognize that allowing employees and contractors to use their own laptops, tablets and smartphones for work can deliver significant benefits to workers and the business. For employees, BYOD (or BYOPC) can help enhance work flexibility and increase satisfaction. Meanwhile, organizations can optimize IT resources and benefit from more productive workers who are more likely to work anytime, anywhere.

With comprehensive mobile enablement capabilities available to help streamline a full range of administrative functions, now is a good time to implement or expand your BYO program. By employing best practices along with the right tools, you can support an evolving mobile enablement strategy that delivers secure anytime, anywhere access to information from a wide variety of devices while controlling administrative complexity.

Before embarking on a BYO program, consider both the advantages and potential challenges. Then take into account the full range of user, IT and business requirements in selecting a BYO solution. With the right approach, you can maximize the benefits of BYO without sacrificing IT control.

Why transition to BYO?

A well-implemented BYO program can enhance worker flexibility, productivity and responsiveness. Employees can use mobile devices and other client systems to conduct a full range of work-related projects whether they are away from their desks, with customers, traveling or at home. As a result, they can be more responsive to customers, suppliers, partners and colleagues.

Allowing workers to use personally owned laptops, tablets and smartphones can also boost employee satisfaction (*see figure*). Workers feel more comfortable working with familiar devices, applications and operating systems. They also can avoid having to carry multiple devices and switching between personal and work systems. Many employees also enjoy the flexibility of responding to work requests outside of working hours — they feel more productive and have more control over their work.

The timing is right

Employees are playing a key role in driving organizations toward BYO programs. In the past, the enterprise IT group led the adoption of new technologies. Today, technical knowledge is no longer purely the domain of the IT group. There are tech-savvy employees in every department across the enterprise. These employees are familiar with the latest consumer technologies, and they believe there are significant benefits in using those technologies for work. They are also more invested in their own devices, which means they tend to take better care of them and keep them updated with the latest OS.

BYOD benefits can be worth the risk

Mobility enablement programs such as BYOD can deliver a multitude of benefits for organizations, including improved productivity, better IT efficiency and enhanced employee satisfaction.[1]

Shifting demographics are also affecting this employee-led push to new technology. An increasing number of today's employees are "millennials" — people who were born in the last two decades of the twentieth century. Millennials are part of the first generation to grow up with computer technology everywhere. These workers are comfortable with technology and highly digitally connected. They also expect to use the latest technologies at work, just as they do in their personal lives. As carriers introduce shorter-term lease programs, millennials will want to upgrade to new devices with cutting-edge capabilities more frequently.

A BYO program should be part of a larger strategy to attract and retain the most talented millennial workers. Of course, millennial employees are not alone in wanting greater flexibility at work. To effectively compete in the marketplace and attract and retain high-quality employees, you need ways to accommodate all of these tech-savvy people. Leverage BYO policies to gain employee acceptance and buy-in for a large-scale digital transformation of the enterprise.

Develop the right BYO strategy

Before implementing a new BYO program, be sure it makes sense for your organization. Establish a solid business case, weighing potential benefits versus costs, capabilities and security/legal risks. Is a BYO program a pressing need with potential transformative benefits for your organization? Or is it simply a "nice-to-have" program that would impact only a select group of employees?

Bring together teams from human resources, legal and IT to define the goals of the program. Address policy issues such as which devices and operating systems you will support, how you will handle employee privacy concerns, what criteria you will use to establish eligibility, and how you will retrieve and wipe corporate data in case of device loss or theft.

Once you've established your business case and decided to move forward, develop a BYO strategy that meets your organization's unique requirements. In broader terms, a BYO program can be as simple as allowing employees to use their smartphones to access company email, contact and calendar information.

Establish a solid business case, weighing potential benefits versus costs, capabilities and security/ legal risks.

Evaluate employee roles as a first step in identifying the right approach to a BYO program and the employees who will be eligible for the program.

Or it can be as complex as enabling employees to log into the company's enterprise business systems or other technology platforms. Since your mobility needs may change over time, choose solutions that work now as well as into the future, regardless of any shift in your mobility or business strategy.

Clearly communicate to employees the details of the plan, including policies, terms and rights of the participants. Outline how your IT group plans to manage personal devices and explain the steps IT will take to protect corporate data and applications on those devices. Ask for employee feedback and input, and then show them how their feedback will be used in the actual plan and policies. Increasing BYO transparency helps build trust between employees and company leadership.

Evaluate user roles

Evaluate employee roles as a first step in identifying the right approach to a BYO program and the employees who will be eligible for the program. Group users into broad categories that consider the kind of work they do on a daily basis — for example, field sales, contract workers, call center operators or software developers.

Weigh both the potential benefits and risks of allowing each category of user to use personally owned devices. For example, while you might reduce costs by allowing contract workers to use their own laptops, you will have to implement safeguards to ensure that those workers are unable to keep corporate information on their personal systems through a remote wipe of enterprise data and apps, or continue to access corporate networks after their contract expires.

Consider all mobile worker types and functions before deploying solutions. Recognize that while some groups of employees have a strong BYO requirement, other groups might not necessarily be well suited to a BYO model. For example, some workers need to access enterprise systems only during their shifts. Or a daytime employee might share his or her workstation with a nighttime employee. Allowing one of those workers to use a personal device would not bring any real benefit to the employee or company and could introduce security risks since consumer devices are not purpose-built for enterprise-level threats.

If a corporate asset, such as a laptop, is used to access mission-critical business applications and data, you'll typically control that asset more tightly and subject it to more restrictive usage policies. Likewise, organizations in some industries need to comply with confidentiality regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or more general security practice regulations such as the Sarbanes-Oxley Act. In these cases, you'll need to determine compliance is possible with a personally owned system or device.

Assess security issues

As organizations consider implementing BYO programs, security is often a top concern. Before allowing employees to use their personally owned devices for work, consider all the possible security issues a BYO program could create. Identify your requirements for security solutions and define policies that can help you maintain tight security, such as access to corporate networks and applications.

To avoid the loss of corporate information and maintain compliance with privacy regulations, you could set a policy that limits the type of corporate information that employees can store on their personal devices. In addition, consider prohibiting the use of cloud storage solutions or USB drives, or implement encryption of corporate data for cloud or USB-drive storage. Implement a security solution that includes remote wipe capabilities so you can remove corporate data from a personally owned device if the device is lost or stolen, or employment is terminated.

Recognize that you need to set distinct policies according to user roles, functions and technology requirements. For example, you might enable access to different systems for a salesperson who primarily uses a smartphone to communicate with customers than for a marketing manager who uses a laptop to collaborate on numerous internal documents and work with multiple teams around the world. To minimize risks, set policies that offer access only to what employees require, nothing more.

Control complexity with a single, consistent solution

Administrative complexity is often another top concern for companies considering a BYO program. You need ways to provide enterprise resources (including enterprise software, remote access capabilities and other tools), manage those resources and implement tight security without having to support a myriad of platforms.

To reduce administrative complexity, adopt a single, consistent solution across all the platforms and types of devices that employees use for work, including laptops, tablets and smartphones. With a consistent solution, administrators can avoid managing multiple consoles, processes and vendor relationships. A single secure enterprise workspace solution is also easier to support than the multiple variants of native email, calendar, contacts, alternative browsers and cloud storage options.

Adopt a single, consistent solution across all the platforms and types of devices that employees use for work, including laptops, tablets and smartphones.

Using a single, consistent solution also benefits employees. In many cases, employees use more than one personally owned device for work. Employees might use smartphones and tablets while traveling, but also use personally owned laptops while working from home or the office. They want the same experience no matter what type of device they are using — a reliable way to connect with the company network; a consistent email, calendar and browser experience; and the same productivity software.

Maximize user flexibility

While maintaining security and controlling administrative complexity are paramount, you also need to give employees the flexibility and simplicity they require. Your employees won't adopt a BYO solution unless it is easy to use and allows them to work when and where they want. Complex, inflexible solutions might also drive employees to use work-arounds that jeopardize security. Before committing to a BYO program, recognize that you need to balance these user demands to maximize the benefits of BYO and avoid potential problems.

Prepare the foundation for BYO

Implement a comprehensive mobile enablement solution with Dell Enterprise Mobility Management (EMM). Built with industry-leading technology, Dell EMM allows you to secure and manage desktops, laptops and mobile devices — plus enterprise workspaces running on those systems. It gives you the flexibility to support your BYO strategy, with capabilities for a full range of devices, operating systems, apps, user types and use cases.

Help ensure security: Dell EMM provides an encrypted, secure enterprise workspace for personally owned laptops, tablets and smartphones. The workspace enables secure remote access while separating personal data and applications from enterprise data and applications, keeping them from commingling. To bolster security, Dell EMM lets your IT group manage enterprise apps and content, set policies and remotely wipe enterprise data from the secure workspace.

Enforcement of data-loss protection (DLP) policies — including copy/paste restrictions, drag/drop restrictions, data-sharing restrictions, password protection, data encryption and auto lock/wipe functions — helps keep enterprise data secure and isolated from an employee's personal space.

Control complexity: Dell EMM helps control complexity by providing a single, consistent solution that can be implemented across a wide range of device types and platforms and managed with a central console. Whether you choose to manage an entire device or simply a secure workspace on a device, Dell EMM provides full management capabilities that include setting policies, enforcing encryption, providing secure remote access, pushing applications and managing patches — in addition to typical reporting and maintenance. You don't lose management functionality, regardless of what you're managing (a device or secure workspace) or what mobile strategy you use (providing corporate-owned devices or BYO). In addition, Dell EMM provides extensive management of systems, mobile devices, applications, content, encryption and policies.

Foster productivity: Dell EMM provides the software and tools that employees need to access required resources and be productive anytime, anywhere — even offline.

Two components of Dell EMM provide secure workspaces on different types of devices:

- Dell Desktop Workspace supports laptops and enables your IT group to create and deliver a Windows corporate image with all necessary applications.
- Dell Mobile Workspace supports smartphones or tablets, has a modern interface and is easily downloaded from the popular consumer app stores. Mobile Workspace includes built-in email, calendar, contacts, secure mobile browser and secure local file manager applications.

Increase flexibility: Because of the flexibility of the solution and the licensing offered, Dell EMM supports the various ways you might offer BYO — whether you allow employees to choose if they want to bring and use their personal devices, or if you enforce a policy. Regardless of how users participate with your BYO program, they gain a self-service portal that lets them get set up and request support as needed.

Ready when you are

Employees have a strong desire to use personal devices for work, and employers gain increased productivity in return for supporting BYOD. With the right strategy and solution, you can implement a BYO program that benefits employees and your organization. With Dell EMM, you can deliver a comprehensive, consistent solution that helps ensure tight security, controls administrative complexity and meets employee expectations.

Learn more

Dell Enterprise Mobility Management (EMM):
Dell.com/EMM

Dell Desktop Workspace:
http://software.dell.com/products/desktop-workspace

Dell Mobile Workspace:
http://software.dell.com/products/mobile-workspace/

Dell Mobility Solutions:
dellmobilitysolutions.com

Contact a Dell expert:
https://marketing.dell.com/mobility-solutions

Dell EMM allows you to secure and manage desktops, laptops and mobile devices — plus enterprise workspaces running on those systems.

[1] *Vanson Bourne, "BYOD: Putting Users First Produces Biggest Gains, Fewest Setbacks," a survey commissioned by Dell, January 2013, http://en.community.dell.com/dell-blogs/software/b/software/archive/2013/02/11/survey-commissioned-by-dell-on-byod-putting-users-first-produces-biggest-gains-fewest-setbacks.aspx*

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology — delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.

June 2014