Three Best Practices to Help Enterprises Overcome BYOD Challenges

Nearly 80% of white-collar workers in the United States use a mobile device for work and approximately 95% of IT organizations allow use of employee-owned devices in some way. Piggybacking on its popularity in the private sector, federal and state government agencies are also keen on bringing BYOD into their operations as well.

However, the preference for using personal devices over company-issued assets creates a set of new challenges for IT managers and business leaders. Moving to a personal device-oriented environment means IT departments must rapidly adapt to an increasingly mobile workforce with new mobile-friendly infrastructure, while simultaneously taking great care to address the security of sensitive information—including data vital to national security.

This paper highlights key challenges facing IT administrators in a BYOD environment—and discusses three best practices for network preparation, ongoing support, and securing information to enable widespread adoption of personal device use, while enhancing data security.

Increased productivity, cost savings drive the BYOD trend

Enterprises at all levels must address the expectation of constant connectivity and communication of public sector employees, contractors, and end users. A well-planned BYOD strategy can benefit workers with increased mobility, better work-life balance, and more flexibility to work where and how they wish for optimal productivity.

BYOD confers many benefits on enterprise operations. It creates opportunities to get new technology into employees’ hands as quickly as possible and saves money because employees are bearing the costs of purchasing the technology. Most importantly, using personal devices for work reasons has become so popular among IT leaders that most believe BYOD is essential to the success of their companies.

To make BYOD a reality in organizations and serve the needs of a diverse workforce, business leaders must consider and plan appropriately for an array of distinct responsibilities. In particular, IT administrators must understand how to manage a significant increase in network traffic, monitor and manage a diverse set of devices and applications, and consistently apply accessibility and security policies seamlessly and accurately across users and devices.
Best Practice 1: Plan Ahead
An airtight plan—written and agreed upon at all levels of the organization—is essential to a successful transition to a BYOD environment. Enterprises seeking to allow employees to use their own devices to improve productivity and mobility will undoubtedly worry that devices may not be secure, that workers may be distracted by applications rather than using the devices for work activities, and that IT administrators will be overwhelmed by supporting unmanaged devices.

The first step in addressing these concerns—or when considering any BYOD expansion—is developing a comprehensive BYOD policy. More than simply gaining acceptance and approval from top administrators down to end users, an effective BYOD policy reaches across the organization's operations and provides prescribed protocols for enforcement.

A well-conceived policy considers the needs of users from various lines of business and explicitly lists the types of devices that will be supported by the IT department. Prior to allowing any personal devices onto a network, IT managers should strategize how to achieve and maintain real-time visibility into network operations to accelerate troubleshooting or preempt network interruptions caused by unauthorized devices.

BYOD policies for enterprise must address new risk elements BYOD introduces to a company’s operations, map them to regulatory compliance challenges, and lay out procedures for mitigating each element. Policies should identify what data is actually being accessed, what—if any—intellectual property or classified information is vulnerable to unauthorized access, and the potential impact were that data to be exposed.

With clearly defined risk factors, IT managers can take numerous steps to reduce threats such as standardizing inspections and sweeps before allowing any device on the network, or by isolating essential applications and data from the rest of the device. Similarly, formalizing guidelines for strong password controls, inactivity timeouts, screen locks and failed password lockouts can be combined with authorization procedures to further strengthen local device security.

In addition to manual authorization, enterprises—especially those managing information such as medical records, personal identification records, or classified data—might elect to encrypt data or deploy solutions that automate the application of view-only access and enable other security measures like locking or wiping a device in case it’s lost or otherwise compromised.

Best Practice 2: Conduct Network Audits
While securing information and devices is the primary concern for administrators, users tend to be more interested in network accessibility and performance from their personal devices. Conducting a thorough network assessment is a critical task in supporting BYOD.

An audit can help administrators answer questions about how many and what kinds of devices can currently be supported and identify bandwidth or coverage limitations. An assessment is also an ideal opportunity to take inventory of a company’s essential hardware like wireless access points, controllers, and network management consoles.
One of the most important outcomes of a network audit or assessment is an understanding of how new devices will affect network density. The wave of personal and office-issued notebooks, tablets, and smartphones hitting a network can significantly impact the existing wireless infrastructure’s performance and security.

In the past, expanding a network simply meant increasing coverage with more access points on or around the business campus. With today’s knowledge worker owning three network-connected devices that can increase bandwidth demands by as much as 300%, it is imperative to create high-density wireless deployments capable of allowing dozens—even hundreds—of users to get online at the same time without degradation of performance.

As such, IT managers should prepare to upgrade or add hardware and software to accommodate the increases in both on- and off-campus network demand. At the same time, dedicated human resources may be increased to effectively manage deployment and troubleshooting. Assembling a list of available technologies and partner service providers capable of meeting specific network needs will streamline the deployment and the support process in the future.

In addition to adding resources, the increased amount of wireless devices flooding the network requires IT managers to consider how they can configure existing assets to better manage and optimize performance. For example, while there are no standards for the implementation of Wi-Fi radios into mobile devices, a well-rounded BYOD plan will segment use across multiple bands (5GHz and 2.4GHz) and leverage wireless access points and routers that support both dual-band and dual-WAN operation to protect against performance degradation or outages.

**Best Practice 3: Automate and Accelerate Security**

The most intensely scrutinized aspect of BYOD for enterprises is the security and safety of high-value information and intellectual property. Protecting information as it’s sent between parties and while it resides on user devices is a critical challenge for IT managers.
Employees and contractors need the ability to communicate without worrying whether their messages will be intercepted or accessed by unauthorized individuals. IT managers can help ease those worries with robust peer-to-peer encrypted communications that guarantees all data such as video, text, and file transfers are private and safeguarded. However, given the time-consuming nature and complexity of learning or developing encryption modules, business leaders should decide, based on the BYOD policy, whether to deploy an on-premise or cloud-based service. Many will elect to use a cloud-based encryption service to save time and energy.

In addition to cloud-based encryption services, Mobile Device Management (MDM) and Mobile Application Management (MAM) solutions provide automated tools for standardizing data security protocols and applications. For example, while many devices have built-in encryption capabilities for basic level protection, IT administrators can use an MDM to ensure that only devices that support data encryption and have it enabled can access the network and corporate content.

Gaining a global perspective on a network’s operations and current status is essential to optimizing security. MDMs provide tools for monitoring and managing mobile devices from a network console and on the device itself. An effective MDM enables managers to configure device policies according to the BYOD plan and deploy them over the air to approved devices.

Preferred solutions will also automatically scan newly installed apps for malware, quarantine infected devices, protect users against phishing attacks or accessing potentially malicious websites, and allow remote partial and full data wipes on lost or stolen devices. IT managers can use MDMs to streamline configuration and enforcement of BYOD access policies by setting compliance criteria for platform and device groups. Devices and platforms can be segmented by job function, security clearance, or virtually any other consideration.

Using an MDM can help ensure that only devices meeting minimum standards and requirements can access the network or select files. MDMs also allow administrators to perform regular compliance checks for enhanced security.

Similarly, MAM solutions help IT managers assert control over the kinds of applications users download via the agency’s network. MAMs allow managers to determine which applications are acceptable on the network and securely deploy them to individual devices or work groups. A complete MAM solution provides the ability to centrally manage application updates, remove mobile applications, monitor application performance and usage, and remotely wipe data from managed applications from a single dashboard.

**Cisco solutions pave the way for wider BYOD adoption in enterprise**

38 percent of companies expect to stop providing devices to workers by 2016, according to a global survey of CIOs by Gartner, Inc.’s Executive Programs – an indication that BYOD in the enterprise will continue to grow. Cisco solutions help make the transition smoother, more secure, and more cost-effective for companies eager to bring BYOD into their environments.

Cisco offers an all-inclusive suite of BYOD products and services including systems management, high-density Wi-Fi, MDM, and third-party MAM integration. Unified components of a Cisco network offer the security and simplified management government organizations need to effectively employ a BYOD strategy including device-based security policies, built-in network access controls (NAC), and MDM.

With Cisco, IT managers and business leaders can gain deep-dive insights into network operations through real-time monitoring of an organization’s devices. The centralized dashboard shows useful metrics, including client hardware/software version information and even the recent location of any device on the network.

More importantly, Cisco solutions help IT managers assert control over the network at a granular level. Like many MDM/MAM solutions that offer over-the-air policy enforcement, Cisco device managers allow device-specific policies to be automatically applied to restrict, quarantine, or lock and erase user-owned devices. However, Cisco solutions also immediately recognize iOS, Android, Windows, and Mac devices, providing for the application of more restrictive policies across device types, specific user groups, or unknown devices.

In addition to tight security measures, Cisco BYOD solutions also help solve the problem of network traffic density. Wi-Fi configurations featuring wireless access points with high-performance processing capabilities, automatic radio frequency (RF) optimization to filter interference, and data delivery rates of up to 1.75Gbps help network managers provide consistent performance despite increased traffic.

As a global leader in collaboration and connectivity solutions, Cisco is helping usher in the era of BYOD in the public and private sector. With cutting-edge security measures, centralized system management of both on-premise and cloud-based deployments, and application program interface (API) support for a range of third-party MDM/MAM solutions, IT managers and business leaders now have answers to the most pressing BYOD questions.

**World-Class Planning and Support from a Global Leader**

Choosing the right hardware and software and strategizing an effective BYOD policy can be a daunting task. For many IT leaders, implementing a BYOD program from scratch is their first foray into that market. While ripe with opportunities to increase productivity and lower costs, BYOD is also rife with risk that can adversely impact an IT manager, his or her department, and the company as a whole.
Objectively assessing an organization's needs and a time-consuming, accurate inventory of available technologies are essential to a successful BYOD deployment, but often beyond the scope or capabilities of IT departments with limited or restricted resources. Instead, many CIOs and IT administrators find it prudent to seek expert guidance and advice from external sources. AVI-SPL is a global leader in the design, implementation, and support of cutting-edge systems and environments that enable enhanced communications and collaboration.

The company provides professional services, support, and training for organizations globally, with particular expertise in mobile infrastructure and security. AVI-SPL uses each of its partners' solutions at AVI-SPL offices across North America, using its own operations as a proving ground for innovative communication and collaboration solutions.

AVI-SPL has established a reputation for its innovative approach to unifying technologies and delivering high-performance, cost-effective solutions for clients. AVI-SPL works closely with employees at various levels of an organization's IT department and core operations to help clients gain better insight to the scope, requirements, costs, and ways to safely accelerate deployment of their mobile presence and BYOD programs.

To learn more about AVI-SPL's services and expertise, visit www.avispl.com.

**About AVI-SPL**

AVI-SPL has a team of experts with the experience needed to meet the most technically advanced needs of our clients. We can help you design, build, and support the systems and environments that enable your video communication and collaboration. Our engineers are certified to ensure they have the skills and knowledge necessary to manage projects of all scopes.

AVI-SPL works with Cisco to provide solutions for different markets, including healthcare, education, hospitality, and many more. From integration and fabrication through installation, documentation, training, and support, the team at AVI-SPL is equipped to be your partner every step of the way.

We're ready to help you better understand how video collaboration can fit into your organization. To learn more about video collaboration solutions for midmarket companies, contact us at (866) 559-8197 or visit www.avispl.com.

**About Cisco**

Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government, and home communications. Cisco hardware, software, and service offerings are used to create the Internet solutions that make these networks possible, giving individuals, companies, and countries easy access to information anywhere, at any time. Cisco has pioneered the use of the Internet in its own business practice and offers consulting services based on its experience to help other organizations around the world.

Learn more about Cisco on avispl.com/cisco.

**References**

- Cisco IBSG Horizons Study. Survey of 600 enterprise IT leaders from 18 industries. Conducted 2012.
- Ibid