Embracing the Benefits of 'BYOD'

The growing trend of 'Bring Your Own Device' brings great benefits to companies that embrace it

By David Sniderman

Today's Environment

Although you may not be aware of it, your company is likely in the midst of the fast-rising BYOD (Bring Your Own Device) groundswell. The way we use today's technology is blurring the line between corporate and personal computing – often the device closest at hand is the device used. To put it simply, employees want a device that fits *their* lifestyle, not a corporate standard.

Should you welcome the use of personally owned devices at work? Or fortify your security to block personal device access to corporate resources?

The financial benefits of BYOD can be significant. Employees often cover the cost of their devices and monthly data service and early adopters are usually quite adept at solving their own technical issues, reducing your technology and support overhead.

But allowing broad access to a variety of devices can expose your organization to security, compliance and loss of intellectual property risks, while attempts to support the panoply of devices users bring to the table can minimize any financial savings.

Point B's Perspective

For most organizations, we recommend embracing and planning for the productive use of BYOD. Taking a proactive stance can give you greater control while building goodwill with your tech-savvy employees.

These influencers will become allies in rolling out the program when the time comes. The key is to define a clear BYOD strategy, with straightforward and enforceable policies, and deploy technology to help you manage them. Employees must understand the boundaries and their responsibilities. With all the pieces in place, organizational productivity can increase in concert with security and compliance.

Here are four steps to consider when adopting BYOD.

Assess your security status quo, and your first step.

Start by evaluating your present security, compliance, and data management practices. Over the years, many technology advances -- flash drives, portable hard drives, personal cloud storage and even personal webmail -- have posed security challenges similar to BYOD. If you had a playbook for dealing with those risks, dust it off and update it to address new BYOD risks. If you haven't defined specific policies for those technologies, now's the time to address them too.

BYOD laptops should run anti-malware and anti-virus software—ideally, the same versions used on company-provided devices. But smartphones and tablets may not support the same security standards. In this case, limit risk by restricting access to applications, data, or both.

Identify the services that will yield the biggest benefits while posing the lowest risk and start your BYOD

Embracing the Benefits of 'BYOD'

program there. A common first frontier is BYOD access to corporate calendars and email -- functionality that can yield huge productivity gains with limited support and a manageable security risk.

Lengthen your stride, but keep it secure.

Think and plan carefully before allowing access to the next layer of business applications. The 'deeper' the BYOD access, the greater the risk and support issues. Determine which job functions will truly benefit and whether the gains outweigh the risks. How sensitive is the data being exposed? Is the as-is application usable on a tablet or phone? After considering all the factors, select a technology and policy solution that balances risks and rewards.

Refine your security strategy. At what layer will you control access or will you use a hybrid approach?

- **Data layer:** Users can access a restricted set of data, but from *any* application
- **Application layer:** Users are assigned specific application permissions, which limit data access
- **Network layer:** Access rules limit users to specific servers by name, group, or communication protocol

Once you've defined your data permissions, consider whether you should prevent data from ever leaving your premises. Virtual Desktop Infrastructure and Application Virtualization (e.g. Citrix) tools run applications on a server within your data center, returning only screen images (not data) to the user's device. Data Loss Prevention (DLP) software looks at the content of the data itself and blocks transmission of specific types, such as social security numbers.

Lastly, consider custom applications to address both usability and security on consumer devices. Though more costly, a purpose-built app can tailor the user interface to specific mobile needs, improving functionality and productivity on small form-factor phones and tablets, while restricting the data displayed.

Set the bar. Spread the word.

Once you have a BYOD strategy, translate it into a clear, concise policies and standards of conduct that are easy for users to understand and follow. Define "acceptable use" and establish the conditions for gaining corporate access, such as minimum system requirements, responsibilities for technical support and fees, corporate remote wipe permissions, and device security. Transparency is key; communicate your policies broadly.

Consider work/life balance (and the law.)

Be mindful of how your BYOD strategy and policies may affect work/life balance. Providing 24/7 access to work email may imply to some employees that they must always be responsive, even after work. In some instances, companies have been required by law to compensate hourly employees if they're responding to email after-hours. For this reason, some companies restrict BYOD access to salaried employees only.

It's important to remind people to take a break and enjoy their personal life. Research shows that 'always on' work connectivity is actually counterproductive.

The Bottom Line

Unless there are legal or regulatory prohibitions specific to your industry, embrace BYOD for those who want it and use it as an opportunity to evaluate security and data management practices. Set clear, consistent policies and create an infrastructure that makes it easy to stay within those bounds. A thoughtful, proactive BYOD approach allows users access to the services they need on the devices they want, while fostering creativity, productivity, and morale, all of which will improve *your* bottom line.