CYBER SECURITY EXCHANGE | US

# Is BYOD (Bring Your Own Device) Worth the Risk?

As technology continues to advance and BYOD (Bring Your Own Device) workplaces become more and more commonplace, IT leaders everywhere are faced with a critical dilemma: Do we embrace the more productive mobile workplace at the expense of security, or do we sacrifice productivity for peace of mind?

It's a tough question indeed. The embrace of mobile devices and BYOD workplaces is not only already in full-swing, but these approaches have been proven to enhance productivity and even increase employee retention.

## The Case For

The Evolving Workforce Project conducted an in-depth study on mobility in the workplace and productivity, finding that "83% of global workers believe technology advances have enabled them to be more productive." Cisco also found that U.S. workers save an average of 81 minutes per week by using their own devices, while Tech Pro discovered that 75% of companies either already allow BYOD or have plans to integrate a BYOD policy in the near future, owing directly to the increased productivity and availability they allow.

With the incorporation of BYOD and mobile devices, employees are accessing company data and resources on-the-go and staying connected at all times, which increases worker availability and thus productivity. Because of the remote access BYOD enables, flexible working hours also continue to become more prevalent, meaning lower office operating costs, better employee retention and a talent recruitment process not hamstrung by location.

## The Case Against

With all that added flexibility and productivity though, comes a cost. More access points, less oversight and devices that can be lost anywhere combine to mean one thing: more vulnerability.

Over 50% of organizations rely on users to protect their own devices, which is a sobering reality considering that by the end of 2017, nearly half of all employers will require employees to use their own devices for work in some capacity. Another recent study conducted by HP revealed that 97% of the apps installed on employee devices have some sort of exploitable privacy issue, with 86% lacking basic security defenses and 75% inadequately encrypting data.

A recent survey of 882 IT professionals conducted by Crowd Research Partners revealed some further statistics supporting the case against BYOD:

- 21% had suffered a security breach traceable to BYOD
- 24% said mobile devices in their organization had connected to a malicious Wi-Fi hotspot
- 39% said the devices which had connected to malicious Wi-Fi hotspots had downloaded malware

**Where Companies Stand**

So when caught between clear gains in productivity and employee satisfaction, and the obvious threat to sensitive data incurred by the use of BYOD practices, where do organizations draw the line? Security, for the time being, wins out. Nearly three-quarters of IT professionals who responded to a recent study said they would sacrifice productivity for increased security, which makes sense, considering the average financial loss incurred by a data breach currently stands at nearly $4 million.

Even with the majority of IT professionals favoring security at the expense of productivity, however, BYOD is quickly becoming the standard in workplace technology rather than the exception. Finding the sweet spot, an acceptable level of risk where security and productivity are maximized, is paramount.

**A Happy Medium?**

According to experts like Southeastern Grocers CISO Chris Gay, who will be speaking at the upcoming 2017 Cyber Security Exchange in Amelia Island, Florida , it starts with conducting a risk-based analysis before ever considering incorporating new technologies. "What's going to be moving, where are our points of emphasis and what's the risk if that data gets out?" From there, Gay says, "it's about understanding that the end-user of that device…owns that risk. It's up to the end user to follow the procedures [to ensure they're using new technologies in the safest way possible].

After you've decided if adopting a new piece of technology would be a net benefit, it's time to start thinking about how to incorporate it in the safest possible way. According to Tom Smith, VP of Business Development at CloudEntr, that starts with encrypting the data itself to be prepared for the inevitable breach. "Beyond that, you should have a BYOD policy in place that includes mobile device management (MDM) which gives IT access to any devices that may access your business network, along with the capability to wipe a device if it is lost or stolen," says Smith.

Stephen Pao, General Manager, Security Business with Barracuda Networks, recommends the following BYOD security tips to help companies maintain flexibility without compromising resources:

- Offer a secure and reliable internet experience
- Help manage device and applications settings to ensure data integrity and security
- Distribute corporate network settings (proxy, Wi-Fi, Exchange, etc.) to personal devices upon enrollment
- Utilize strong passwords and encrypt sensitive data
- Set strong application control policies

Other BYOD best practices can include giving employees access only to their department's files, incorporating layers of security which require each new device to be authenticated by the domain controller and having a well-defined email security policy along with cyber-safe educational programs for employees.

## Summary

The quantifiable boosts in employee productivity and satisfaction and the enhanced convenience and utility of mobile devices mean BYOD programs are set to become the standard for the majority of organizations in the coming years. Security continues to be a top priority for IT professionals, even at the expense of productivity, but as businesses continue to go mobile, investing in a thorough risk assessment and a tailor-made BYOD security strategy is a sound idea.

Has your organization implemented BYOD, or are you considering it? Are there any pros or cons you would add to the mix?