Vol. 4 No. 7
July 2012

BUSINESS*insights*

BYOD — Rational or Risky?

Today's most popular trend is consumers carrying a smart phone, tablet or other device that lets them connect to the Internet everywhere they go. One of the places these consumers go is to work, so that practice has earned the acronym of BYOD or Bring Your Own Device.

BYOD affects every kind of business, large or small. Wikipedia reports that BYOD has made "significant inroads in the business world with about 90% of employees already using their own technology (in at least a limited capacity) at work."

Opinions vary dramatically on what this BYOD trend means to business. In his report, "Enterprise-Grade BYOD Strategies: Flexible, Compliant, Secure," analyst Andrew Borg of the Aberdeen Group paints a picture of the overall pros and cons of BYOD:

"Since 2008, Aberdeen research has been tracking a radical transformation taking place in the enterprise: more and more organizations are permitting, even encouraging employees to bring their own mobile devices into the workplace to be used for work purposes. While at first appearing to radically lower the cost of enterprise mobility while making its productivity and communications advantages available to a much broader group of employees, it also introduces new risks and may actually significantly increase costs if not properly managed."

BYOD presents a new arena in which you must weigh the pros and cons and then set up company policies designed to keep everyone productive while reducing your risks. Here are the issues you need to consider:

The Pros —

- **Use of new, more productive technologies:** Technology advances happen so quickly, it's difficult and costly for your business to adapt them as they are introduced. With employees buying and using newer devices, your company can take advantage of the capabilities provided by newer technologies.

- **Reduced acquisition costs:** BYOD implies the worker is using his or her own device, so your business is relieved of the cost of providing that device. If the device is replacing one provided by your company, such as a cell phone, that cuts your business costs. As Good Technology states in its State of BYOD Report, "50 percent of companies with BYOD models are requiring employees to cover all costs -- and they (those employees) are happy to do so."

- **Reduced maintenance costs:** Your business must provide staff or pay outside service providers to upgrade and support the technologies you use in your business. Workers using their own devices may reduce or eliminate the need to support the operation of those devices. If you do provide support, however, it may be less, as workers may take better care of something they personally own.

- **Worker satisfaction:** The entire reason BYOD came about in the first place is that people want to use their own devices. They picked them out because they like the way they work and like using them. In theory, being able to use their own devices has the potential to increase worker satisfaction and productivity.

IDeACOM® NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org

BUSINESS insights

The Cons —

There is only one con in this BYOD scenario, but it's a big one -- security. With company-provided devices, security can be built in and you can have greater control over how those devices are used. With employee-owned devices, security becomes trickier:

- **Data access:** If employees are going to access your business network from their own devices, you may want to require them to add security tools that will keep the data safe as it is being accessed.

- **Data privacy compliance:** If your business is in -- or does business with -- financial, healthcare or other industries regulated by HIPAA or other federal privacy rulings, it's critical that users comply with these regulations even if using their own laptops or tablets. This issue could be the determining factor on whether you do or do not allow any business to be conducted on personal devices.

- **Theft:** Although there is risk of business laptops and other devices being lost or stolen -- especially when employees are in the field -- the risk multiplies many times when workers take their devices home with them every night and everywhere else they go.

- **Termination:** When an employee is fired or quits, normally the devices they have used are company owned and stay with your business when those employees leave. If employees are using their own devices, it's critical to not only terminate their log-in privileges, but make sure any company-related data is removed from their devices.

It's difficult to weigh the potential cost savings and productivity advantages against risks of being a BYOD-accepting business. To decide, you may want to meet with your employees and IT support provider to discuss these pros and cons. This should help you formulate a BYOD policy that is understood and has the promise of being a safe and positive addition to your operation.

IDeACOM® NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org