BYOD:

A Minefield For Data Security

TechKnowledgey

https://www.techknowledgeyinc.com/

One of the big drivers behind the adoption of any BYOD policy is employee convenience. Being able to handle all activities–work related and personal–is a serious time saver. Considering that most of us conduct our personal digital lives 24/7 and that our employers now expect us to be available off standard working hours, two separate physical devices is almost a non-starter. Realizing this fact, most companies are adopting some version of BYOD. This guide discusses the privacy and security issues that are introduced by the concept of BYOD and draws attention to a few concerns that should be addressed in the design of your BYOD policies.

We need a little background, however, before going on. Prior to discussing the various issues that should be incorporated into a BYOD policy, let's look at three commonly mentioned reasons for adopting BYOD.

The first is the assertion that BYOD saves money. There are a few things to consider here before you jump on the 'save money' bandwagon. Given how important optimizing collaboration and communication has become for most organizations, money saving should not necessarily be the sole factor behind the BYOD decision. The primary driver behind a BYOD initiative should be specific business goals, such as facilitating collaboration.

Also under the umbrella of money saving, it is important to understand that the savings from shared equipment costs and data plans can be easily measured, but other accompanying costs may be less transparent. There are nascent costs with BYOD. The increased complexity of maintaining security and upgrading software on multiple hardware platforms does not come without increased IT labor investment. BYOD will increase technical support costs. Additionally, the increased exposure of data stored on employee-owned devices represents a potential risk that will have real costs attached to it, should a breach occur.

The second reason for adopting BYOD is employee convenience. Obviously, that is an important consideration. Employee satisfaction has links to increased productivity and retention, both of which connect to the bottom line. And practically speaking, it is likely that some work-related business is taking place on personal devices whether it is permitted or not. However, there are certainly specific situations and industry sectors where security and confidentiality concerns create unacceptable levels of legal exposure for an organization. These all have to be taken under consideration before adopting a BYOD policy.

The third reason is summed up with one word: collaboration. Improving communication between and among employees, clients, and other stakeholders is a key focus of the present business environment. Any policy enabling greater collaboration using all available devices is considered positive. This notion that collaboration matters to productivity is what is

1840 W. Lincoln Ave., Goshen, IN, 46526

behind the concept of Unified Communications. Restricting device usage may deter easy, smooth communications and that has implications for productivity.

Issues to address in a BYOD policy

Employee Privacy Concerns - One issue that arises with BYOD are employee's concerns about the privacy of personal data and applications. Because these are their own devices, they have an enormous amount of personal data, including health information, photos, texts, emails and other information stored on the device. Also, apps they may have installed could potentially reveal information about their religion, politics, sexual orientation or other characteristics that they may consider private and off-limits. Concern that their employer could see their personal data is a legitimate worry; there are Human Resource implications here. Knowledge of certain data about an employee could make an employer vulnerable to discrimination laws. What about GPS tracking? Can the employer track employee whereabouts? The employer has a compelling interest to track the device in case it is lost or stolen, but the employee has similar competing concerns about privacy.

There are no absolutely correct answers here, but a perception of overstepped boundaries could lead to an atmosphere of distrust that can be counter-productive. It is also important that these decisions be made with knowledge of all applicable local, state and federal regulations.

In short, just be aware BYOD is a complex matter that can't be handled within the silo of IT.

Data Security implications

Probably the most prominent concern among those who have to address the BYOD issue is the increased risk to data security. Obviously, the more devices you have with the ability to connect to your data, the more opportunities you create for a breach. Simply put, a house with 20 doors and 50 windows with multiple lock styles is a bit more vulnerable than a house with one door and one window. BYOD increases risk to the organization. Data breaches bring a few layers of concern. First, the loss of proprietary data can effective your competitive status in the market. However, the real high-visibility concern is the theft of your customer's personal data. Theft of personal data brings three serious consequences. First, data breach laws require informing all victims of the data breach and in some cases, the media must also be informed. This public visibility can have long-lasting implications for brand value. Second, you face a short- and long-term revenue hit. Customers angry and frustrated, as well as others who learn about the breach through social media, word-of-mouth, and traditional media sources, may move their business to the competition. Third, data breaches can bring civil penalties. In the case of the General Data Protection Regulation (GDPR) in the European Union, these penalties can be extremely severe. (And keep in mind, the GDPR doesn't just apply to entities physical operating within the EU.

1840 W. Lincoln Ave., Goshen, IN, 46526

It applies to the data of any user who is a citizen of the EU.) In summary, given the severity of the consequences and the increased vulnerability created by BYOD, it is important to create a BYOD policy with strict parameters. It cannot be a "wild west" of anything goes.

IT support and maintenance

The discussion of the importance of maintaining security brings up some very practical considerations for your IT department. You will need to place limits on the BYO part of the issue. There are a wide array of possible devices out there. Supporting all of them would be overwhelming. In addition, users don't just BYOD, they bring their own Operating System and their own software applications and all of those applications' multiple versions. Trying to support and control an almost limitless list of entry points into your data is both unwise and impossible. IT will need to place limits on which devices and operating systems it will support.

Another point to consider is how much the company will rely on the individual user to install and upgrade company-required applications? Will IT be responsible for those duties? By placing the burden on IT, you ensure all the proper versions are being used, but you increase the labor requirement, which may become impractical.

In summary, there are a lot of issues regarding BYOD that create security concerns. BYOD policies have a lot of moving parts which makes preserving data security a difficult task,. Make sure you are recognizing all the areas for a potential leak or breach of data.

CONTACT DETAILS

Jesse Good
Marketing Coordinator | TechKnowledgey, Inc.
Email: jgood@tkiapps.com
Phone: 574-971-4267
https://www.techknowledgeyinc.com/