BusinessManagement DAILY

APRIL 1, 2015

Wearables in the office: Security risk?

The use of wearable tech devices is on the rise. A recent PricewaterhouseCoopers report found a fifth of adults in the United States already own one, and additional sales could top 130 million units in 2018.

Devices such as smartwatches, fitness trackers, posture correctors and headphones are all on the market and making their way into workplaces. These devices also pose real privacy and security threats that employers' IT departments need to control carefully, says David Upton, CEO of DA Systems, a software company focusing on the transportation and delivery sector.

Upton lists some concerns to consider when it comes to wearable tech devices at work and how to mitigate them.

• **Corporate privacy.** Certain devices, such as Google Glass, can record and transmit everything the wearer sees. It's important to develop a strong privacy and security policy for an organization to protect itself. This shouldn't be difficult for most forward-thinking organizations to implement and will generally be an extension of their existing social media and BYOD (Bring Your Own Device) policies.

• **Data security.** If a device is stolen, intercepted or hacked, all the data flowing back and forth in real time is compromised. This can include company information or personal data. Features that automatically wipe a stolen device or require biometric identification to log in can mitigate some of this risk.

• **BYOD or enterprise?** If everyone brings their own device, the company ends up with several different brands and software platforms to try to integrate. On the other hand, purchasing devices for everyone at the company can be expensive. It will be up to your organization to decide how much everyone depends on such devices and if it's worth it to make them a standard issue item for employees.

• **Employee privacy.** Since these devices can collect and transmit so much sensitive data, it's imperative that this data be used correctly. Monitoring activity levels and productivity is a good, internal use of data, for example. Sharing heart rates and sleep routines with health insurance companies to determine premiums is an overreaching invasion of privacy.

— Adapted from "5 Essential Wearable Tech Security Tips," David Upton, BetaNews.

© 2021 A *Business Management Daily*