Before wearables thrive in enterprise, consider these cultural and security issues

by Mellisa Tolentino | Oct 9, 2015 | 0 comments

Wearables are deemed personal devices – those we use to keep track of our fitness progress, stay on top of important notifications, help us sleep better, remind us to eat healthier, and so on. But there is more to wearable devices, as they become part of the BYOD family in the workplace, as well as finding their own niches in the enterprise.

The growing potential of wearables for use in the workplace is getting noticed, one early device being the Motorola WT4000 Wearable System that allows for simplified inventory tracking and on-demand access to product information. Since 2004, Tesco PLC has been utilizing such devices to help employees efficiently take inventory in their various warehouses.

According to recent reports, consumers are interested in owning wearables in exchange for rewards, such as lower insurance rates. Some corporations are tapping in this concept, including Target Corp. which offered its 335,000 U.S. employees Fitbit smartbands to help them improve health and lower healthcare costs.

photo courtesy of Google Glass

Even Google Glass is finding its place in the workplace. Some doctors in the Emergency Department of the Beth Israel Deaconess Medical Center in Boston were given pairs of Google Glass, which allowed them to quickly access patient information for expedited assessments. And some are seeing Google Glass as a great tool for the education sector.

Indeed, the enterprise has room for wearable devices, but as with all connected devices, there's cultural considerations and security risks in adding more gadgets to the enterprise roster.

Roman Foeckl, CEO, CoSoSys Ltd., a company that delivers services to protect enterprise data and prevent data leakage, believes that despite the benefits of wearables for the enterprise, there are still aspects of it that needs to be addressed before it can be truly implemented.

Foeckl shares three things that needs to happen before wearables become the norm in the workplace:

Embracing Innovation

First off, companies should be open to allowing the use of wearable devices in the workplace not just for personal use but as something that could help increase employee productivity.

"What wearables represent is both the present and future for companies who are serious about meeting the needs of employees who wish to take advantage of a rapidly changing technology market. By meeting this trend head-on with a smart

outlook on policy and preventative technologies,organizations not only create satisfied and motivated employees, but it now has a more secure network and a new mindset around security where being proactive and strategic is the new norm and anticipating needs is what we strive for," Foeckl states.

Creating a Malleable, Update-able BYOD Policy

When employees started bringing their smartphones and tablets to the office, the enterprise had to adjust and create new policies as to the extent of use of the said devices in the office. Now that wearables are making their way to the office, Foeckl believes that new policies regarding these devices should be malleable, to be upgraded when needed instead of having to draft new policies every time a new device becomes available for the enterprise.

"Since it can be said with confidence that the mobile and wearable devices are just the beginning of this trend for blending our personal devices with business, there is a clear opportunity for IT teams to develop a proactive and ongoing mobile technology program that will adjust as new technologies emerge rather than wait for new technologies to reach critical mass and scramble to adopt a reactive stance. No longer can organizations have the luxury of meeting bi-annually or semi-annually for training; it now must become a regular feature of information security planning. By consistent and constant training for IT teams, organizations can ensure they are fully ahead of all aspects of new information security with wearable tech being one example," Foeckl added.

Keeping Sensitive Data inside Away from Prying Eyes

Aside from strong BYOD policies, Foeckl states that strong security measures should also be implemented. Some of the solutions Foeckl sees is Enterprise Mobility Management (EMM) or Mobile Device Management which enables IT to control what data will be made available in these wearable devices as well as remote wipe in case the device gets lost or stolen to prevent corporate data from leaked.

With the advent of wearables for the enterprise, IT Admins would have to be vigilant in monitoring what devices connect to the network and what data is being moved back and forward between the wearable and company computer. Foeckl added that at the same time, security vendors should add solutions that would be able to detect and control these wearable devices without disrupting their functions.

The enterprise can also benefit from wearables as it can add a layer of security. Take for example the Nymi band, a wrist-worn device that continuously measures the wearer's electrocardiogram or heart's electrical activity to verify the wearer and use that data to unlock, say, a computer. The use of a person's electrocardiogram as a password ensures that no other person can access sensitive information stored in a computer. You cannot dupe Nymi as, stated earlier, it continuously verifies the authenticity of the wearer. Also, Nymi has added two-factor authentication which utilizes a one-time code which is generated by the band itself. If two-factor authentication is active, without the unique one-time code, even if the person has been verified, the computer will not be unlocked.

"What's interesting is that future uses of wearable technologies can mean an added layer of security for the enterprise and user including two-factor authentication, applying users pulse for authentication, or location-based authentication – all of which can be used for policy compliance and context-based security as well. Context is the keyword here, because it's what's lacking now to data security solutions and could be soon compensated by wearables. So, their use can be extended in data security with great impact.," Foeckl concluded.