Top tips on creating an enterprise risk strategy for wearables

Can wearables bring security and efficiency to the enterprise? Absolutely, it just takes some tactical risk assessment.

It's time to get wearables on the side of enterprise security, instead of fearing them

For our personal lives, the emergence of wearable technology has represented a new way to track our health, augment our visual surroundings and check our email. Bringing these new capabilities into the enterprise opens a whole new world for collaboration, easier communication and greater productivity.

However, as wearable technology becomes increasingly blended into our personal and professional lives, organisations need to ensure they are prepared to address the risks that come along with the benefits.

Smart watches, for example, can easily be converted into listening devices because they can record audio and then transfer and stream the recording.

IT admins have already started to detect wearables in company networks and are often unsure of the type of device or the potential threats they bring. There are a handful of enterprises that are integrating wearables in their network as part of their productivity increase program.

For example, Tesco has begun using a wearable inventory systemin their warehouses to track product orders. Over the next few years, things will start to change as the number of organisations that recognise the benefits of wearables increases.

Not only will they support employees' use of wearables, they will offer them for general use. Risks are manageable, but they should be treated with extreme care.

By taking the following steps, organisations can ensure they are experiencing the full benefits of wearables without leaving themselves open to any risks.

Make updates to existing policies and keep them easy to update

For any organisation with a BYOD policy, a wearables policy is a logical next step. Since wearables come with

many risks and benefits similar to those of other mobile devices currently used by enterprises, adding policies should be a simple upgrade rather than needing to draft an entirely new plan, as we saw with smart phones and tablets.

By taking these steps now, organizations can take advantage of the slower than expected roll out of many better-known products, like Google Glass and the Apple Watch, and can be prepared for when consumer demand hits market perceptions.

While these products may have underperformed media expectations, it would be foolish to use that as an excuse to delay developing a wearables addition to an enterprise BYOD information security plan.

Since we have still only seen the beginning of the trend of blending our personal devices with business use, 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.

Organisations no longer have the luxury of meeting bi-annually or semi-annually for training; regular trainings and updates must be included in information security planning.

By consistently staying ahead of new information security threats and solutions, organisations can significantly reduce the risk of a costly data breach - wearable technology being one example.

Keep sesnsitive data from falling into the wrong hands

Beyond a strong, proactive mobile policy, there are a number of solutions available to ensure that enterprises keep up with the rapidly evolving IT landscape and the newtypes of devices employees bring to work.

Given the light and easy nature of wearables, solid mobile security software like Enterprise Mobility Management (EMM) or Mobile Device Management (MDM) solutions, should be used to keep sensitive company data from exiting the company and falling into the wrong hands.

In the BYOD era, where the line between work and leisure gets thinner each day, EMM or MDM solutions can provide the security for sensitive information to be stored on personal devices through detailed control over companies' mobile devices.

Mobile Application Management (MAM) is another great solution that should be adapted to monitor what applications are and can be installed on wearables. Data resides on a wearable device and there is always the risk of that device being lost or stolen and then manipulated to recover the information.

Remote wiping of mobile devices is a good thing to look for when searching for a security solution. As a preventative measure, a solution that can analyze the information that is being transferred from the wearable to a mobile device should also be considered in order to protect against data leakages.

IT admins should have a real-time view of the devices that are connecting to the network and what kind of data is being moved back and forth between them. At the same time, security vendors should add capabilities for detecting and controlling these devices without disrupting their practical functions.

Another interesting thing to consider is that future uses of wearable technologies could potentially mean an added layer of security for the enterprise and user, including two-factor, user pulse or location-based authentication - all of which can also be used for policy compliance and context-based security.

Context is the keyword here, because it is what's currently lacking in data security solutions and could soon be solved by wearables. The use of these devices can actually be extended in data security with great impact.

Make innovation your ally

Beyond all else, wearables present a unique opportunity to change the mindset found within organisations that harbors fear of new technologies. As we adopt a proactive approach to embrace new employee technologies, we

can experience an increase in employee productivity and a reduction in insiders and malicious threats to the corporate information security structure.

This would be the result of ongoing security processes made possible though proactive practices rather than more costly reactive ones.

What wearables represent is both the present and future for companies that are serious about meeting the needs of employees who want to take advantage of a rapidly innovating technology market.

By meeting this trend head-on with a smart outlook on policy and preventative technologies, organisations not only create more satisfied and motivated employees, but also have a more secure network.

A new mindset around security, where being proactive and strategic is the new norm, can lead to great strides toward a more functional organisation.

Sourced from Roman Foeckl, CEO, ***CoSoSys***