Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Seven reasons why BYOD could be an expensive mistake for businesses

While many companies now recognise the need for a mobility solution there are still many reasons why a bring-your-own-device (BYOD) approach may not be the best approach for the business.

Ilan Rubin, managing director, Wavelink, said, “Using BYOD can seem like a simple solution; it lets employees use devices they’re comfortable with and lets businesses avoid investing upfront in devices. However, the full implications of letting employees BYOD should be considered, as there may be a better approach depending on the business and the industry.”

There are seven reasons why adopting a BYOD policy could be an expensive mistake for businesses:

1. Security. Security is one of the biggest issues with BYOD because of the security risk posed by consumer-grade phones. When staff use these devices to access patient or consumer information, that information can potentially be hacked more easily than with a purpose-built device.

2. Bring your own distraction. There's a risk that encouraging staff to bring in their own devices that are more suited to watching videos, playing games and keeping up-to-date with their digital social lives, will mean they will do just that. Consumer devices may reduce productivity, which for most businesses is the strategic goal of implementing a mobility program.

3. Mixing personal and business data. Companies with BYOD risk employees that are leaving the company walking away with a significant amount of client data, available at a touch of the button on their own device if strict policies aren’t in place. On the flipside, employees may also feel their own privacy may be breached by their employer if they are connected to the company network.

4. Ruggedised devices. Unfortunately, there are business environments that consumer-grade technology can’t withstand. If employees are working in areas where they are likely to drop their phone on a concrete floor, or expose the phone to water, dust, strong disinfectants, or if they require a device to monitor temperature in a cold environment like a freezer, they will need special handheld devices designed for these tasks.

5. Vulnerabilities. Employees could be downloading mobile apps and connecting to external Wi-Fi spots without the correct security protocols in place. This creates serious security holes that can be exploited by hackers. Coupled with the fact that employees might not have anti-virus protection or have an up-to-date firewall present on their mobile devices, this means they might be more vulnerable to attacks.

6. Device disparities. With BYOD, employees are likely to have a plethora of devices, all with different capabilities and operating systems that run different programs at different levels of quality. Many companies might not have an IT department resource to ensure all business applications and data workflows work on every different device, which is required for a profitable return on investment.

7. Cost. Having to pay for both the device and the data plans can increase the total cost of ownership for the organisation. Also, trying to implement guidelines and security for the devices can end up costing the organisation more than it originally planned for when it implemented the BYOD system.

Ilan Rubin said, “Businesses should look instead for purpose-built devices, such as the Spectralink Versity, that have the best features of a consumer smartphone and a ruggedised enterprise phone, to address these BYOD concerns.”