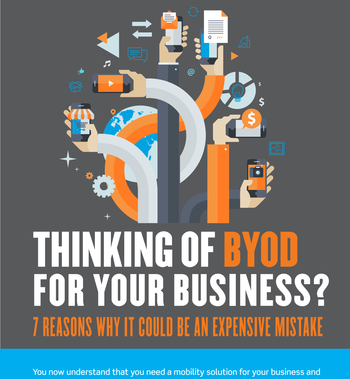


THINKING OF BYOD FOR YOUR BUSINESS?

7 REASONS WHY IT COULD BE AN EXPENSIVE MISTAKE

You now understand that you need a mobility solution for your business and are all ready to implement a mobile transformation journey – and it's probably about now you're are thinking 'why can't I just use my personal mobile phone?' We all have one, therefore it seems like an easy solution. But have you considered the full implications of allowing your employees to use their own phones – known in the industry as BYOD (Bring Your Own Device)?

The large majority of employees in the US, UK, and Spain want to keep their personal and business tasks and communications separate, according to new data provided to BI Intelligence by telecom-web convergence company tyntec.

1 SECURITY PROBLEMS

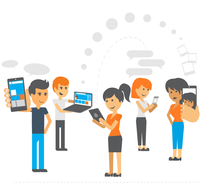
ACCORDING TO A BT SURVEY ONLY 1 IN 10 IT MANAGERS BELIEVES BYOD USERS UNDERSTAND THE IT RISKS INVOLVED

THE GLOBAL COST OF CYBERCRIME WILL INCREASE TO $2 TRILLION BY 2019.

Security is one of the biggest issues with BYOD because allowing consumer devices onto corporate networks brings significant risks – especially for staff, such as clinicians, or retail assistants accessing consumer or patient information, making using consumer phones (which can be accessed outside the work environment) a no-no for staff who are dealing with sensitive personal or commercial information.

PWC FOUND 32% OF COMPANIES WERE THE VICTIMS OF CYBER CRIME IN 2016.

SKYCURE REPORTS THAT 21% OF ORGANIZATIONS HAVE TRACED A DATA BREACH TO THEIR BYOD PROGRAM.



2

THERE'S A REASON WHY BUSINESS DEVICES ARE BORING – THEY'RE FOR BUSINESS, NOT PLEASURE.

BRING YOUR OWN DISTRACTION

There's a risk that if you encourage 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, they will do just that. Bottom line, consumer devices will hurt productivity which for most businesses is the strategic goal of implementing a mobility program!

3 MIXING PERSONAL AND BUSINESS DATA

How do companies with BYOD stop employees who are leaving the company from walking away with a significant amount of their client data, available at a touch of the button on their device? This can also be flipped for the employees – they may feel their own privacy is at risk if they do personal web surfing on a device that is linked to their company's systems.

RUGGEDIZED DEVICES

4

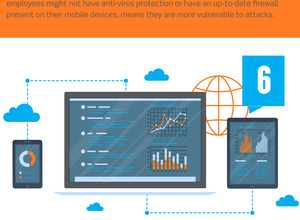
Unfortunately, there are business environments out there that consumer-grade technology cannot withstand. If employees are working in areas where they are likely to drop their phone on a concrete floor, or expose the phone to water, dust, strong disinfectants, or if they require a device to monitor temperature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

5 EXPLOITS VULNERABILITIES

97%

ACCORDING TO A STUDY CONDUCTED BY HP, 97% OF EMPLOYEE'S DEVICES CONTAINED PRIVACY ISSUES, AND 75% LACKED ADEQUATE DATA ENCRYPTION

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



6

DEVICE DISPARITIES

With BYOD, your employees are likely to have a whole plethora of devices, all with different capabilities and operating systems that run different programmes at different levels of quality. Most companies might not have an IT department resource to ensure all business applications, data workflows work on every different device of each individual employee – which is required for a profitable return on investment – it is hard to get programmes that are of high quality and cover all platforms and devices. Also introduces increased resource costs to manage.

7 COST

Having to pay for the device and also the data plans that go along with the devices can actually increase the total cost of ownership for the organization. Also, trying to implement guidelines and security for the devices can end up costing the organization more than they originally planned for when they implemented the BYOD system.

spectralink