Fujitsu Statement of the Month
September 2011

A plea for more freedom: why companies should embrace new mobility trends
Dr. Joseph Reger, Chief Technology Officer at Fujitsu Technology Solutions

If, as an international company, you're on the hunt for fresh talent, you will have noticed that new hires are considering more factors than just the once all-powerful aspect of starting salary – and are taking a wider look at what makes a new company an attractive place to work.

One of the major «soft factors» that the new generation of young professionals are taking into consideration is to ensure that they retain some personal freedom when it comes to communicating – which for employers means allowing new employees to communicate in the style that they have naturally adopted in their private lives, as digital natives.

This includes of course the use of social media– but more than ever it also includes using specific devices that young people are familiar with. Better not to communicate at all than to be saddled with a device that's terminally unhip.

That's how the trend «Bring your own device» (BYOD) emerged in the United States a few years ago – and as so many trends before, has made its way over the pond.

At first glance, allowing employees to connect their own devices to corporate networks seems like a really bad idea that will leave enterprises open to data leakage and other threats. A closer look, however, shows that this is already a reality today for most European companies, too.

Time to establish the rules

This is no time to stick one's head in the sand. Instead, it's an opportunity for companies to establish some strict rules for BYOD. That's the only way CIOs will be reassured that any employee-owned devices that are connected to the corporate network are at least regulated – instead of being snuck on to the network via a backdoor. That's got to be better all round. And in environments where managed processes are established that allow employees to connect their own devices, then this is a solution to what today is a pretty anarchic situation.

As a CIO, what should you consider if BYOD is something you plan to establish? I think BYOD appears attractive to the CIO, since it promises to free him of the chores of hardware asset management, allows him to avoid making hardware choices and makes it possible to establish a firm ceiling cost per device, by establishing an employee allowance.

Still, BYOD also brings a twofold challenge: data leakage and unauthorized access to networks. The first problem has been around for a while, with IT managers very concerned about the large memory capacities of very portable devices like smartphones and slate PCs. Just as before, with USB sticks, one of the challenges for IT managers is to control what's being copied off the network on to portable storage devices, into e-mail, or to file-sharing sites. Today, there are plenty of enterprise solutions designed to address just this problem.

Dr. Joseph Reger, Chief Technology Officer at Fujitsu Technology Solutions

The threat of unauthorized access to company networks is one that CIOs are especially concerned about when the breach comes from within the firewall – i.e. from a non-authorized PC or slate that is simply hooked up to the corporate network. Again, most enterprises have defenses in place against such things happening.

Furthermore, there are technologies available that provide isolated execution environments for access to the enterprise network on client devices – and I strongly recommend they are being used.

For example, future IT departments will be managing simply virtual desktop images running on client machines that may or may not be employee-owned. Fujitsu is offering a Portable Zero Client, which connects to any Windows-based PC via USB and provides access to a

completely secure IT environment – no matter what's on the host machine itself.

Shift in focus

What we're seeing is a shift in focus from managing physical devices such as PCs and notebooks, to IT managers taking care only of the corporate image running as a virtual machine on a host.

The best way to manage and secure BYOD devices of all kinds is to draw a very clear line in the sand as to what technology is the responsibility of the employee, and what's managed by the company. We're seeing early implementations now of virtual machines running even on smartphones, which means that every device – be it a notebook, a slate PC or a smartphone – can run a corporate desktop as a virtual machine and provide a secure execution environment separated from the private environment on the same device.

So in short, although BYOD may seem like a bad thing to do, if done properly, it can be very beneficial. Even more: The consequences of not moving with the times are that companies who turn their backs on BYOD will find themselves losing out in the future, in the war for talent. Given the choice of working for Company A, where BYOD is supported, and Company B, where it is not, you'll find that the new generation workforce will vote with their feet and choose a company whose philosophy towards IT is more aligned with their personal views. If you're not flexible with regard to changing technologies then you're going to fall behind the competition.

Press Contact:
Silvia Finke
Knobel Corporate Communications
Tel.: + 41 (0)41 768 99 43
s.finke@knobel.ch
September 2011

© Copyright Fujitsu Technology Solutions GmbH 2011