BRING YOUR OWN DEVICE?

CapaSystems
...because time matters

BRING YOUR OWN DEVICE
LEADS TO SLEEPLESS NIGHTS

Mix of personal and business applications on same IT devices makes IT departments worry

We all do it—use the same IT device for work and personal purposes. That goes for our smartphones, tablets, laptops, etc. There's no doubt that it's flexible and helps reduce costs for users and employers alike. But what about the security of your company in this universe of personal and business apps provided by a Bring Your Own Device (BYOD) culture?

Users constantly cross the line between business and pleasure. The ability to switch between the two in a split second increases end user satisfaction and productivity. BYOD also lets you reduce the costs and time spent on configuring devices and supporting users. But there is a challenge in this BYOD culture: security. Especially the more pleasure-oriented apps are lucrative for hackers to exploit—and then the company's data is in danger of being infected with malware and other bad stuff.

Research shows that Danes on average have 33 apps on their smartphones, and if we add Germany, Norway, Sweden and the UK, the average is 32.2 apps per device according to Mobile Planet. We are also frequent guests on social media of the more personal kind (for example Facebook, Twitter or Instagram). People from these countries are still a bit reluctant when it comes to making purchases via their mobiles—only 33.6% make online purchases via their smartphones, but that doesn't change the fact that the risk of attacks on the device and its data is real! And when we use the company VPN connection via our IT devices, the gates to the company's data become wide open.

Malware worms its way in through apps and begins to eat the company's bandwidth, which leads to reduced network speeds and reduced productivity. If we look at the above-mentioned countries, where wages are high, that can cost companies their future competitive edge.

That makes it interesting to look at how you can stop the security weaknesses associated with BYOD without sacrificing user productivity and flexibility.

Many organizations have tried this without success, because measures like encryption, security checks and mobile IT policies are hardly ever enforced in real life.

Another way is to try to take control of security by banning download of specific apps. This, however, is typically met with frustration among users—why do they suddenly need to delete their favorite game? Anyway, users will always find ways to keep their favorite games because, despite all good intentions, the security of the company is not at the top of their minds. Convenience and pleasure play much larger roles.

Companies can choose to manage and control users' apps through Mobile Device Management software that provides central control of software deployment and configuration changes on all devices. Several of these solutions let you easily and quickly roll out simple as well as complex software without the need for involving or disturbing end users, and IT departments are able to roll out enterprise applications from Apple App Store and Google Play to iOS and Android devices.

The threat from BYOD is very real, and it understandably costs many CIOs sleepless nights because of the disasters that a data security breach can potentially result in. Imagine if your company is close to a revolutionizing breakthrough, and you then become the victim of a hacker attack. Several years of research could be lost, and the financial consequences could be disastrous.

This security problem is by no means a new phenomenon, but it is highly relevant to discuss it regularly, because new inventions and creative hackers constantly change the threat assessment. Simply ignoring BYOD is not an option.

MasS360 have developed

"THE TEN COMMANDMENTS OF BYOD"

10 pieces of advice about Bring Your Own Device:

1. Create your security policy before you purchase the technology
2. Make sure that you know the actual number of devices, and notify users before you do something
3. Roll-out must be simple, secure, and also offer the ability to configure devices
4. Roll-out and configuration changes must take place simply and quickly without disturbing users
5. Provide users with a smoothly running self-service platform
6. Protect personal information and explain the company's privacy policy to users
7. Keep corporate and personal data separate
8. Manage your data usage—formulate thresholds to help users
9. Constantly monitor devices used in the company to ensure that they adhere to the security policy
10. Keep in mind how BYOD will affect the company's ROI.

CAPAINSTALLER

CapaInstaller is software that helps you automate installation and update processes, stay in control and use your time effectively. With CapaInstaller's centralized distribution features you'll no longer need to manually install software on users' computers—no more driving back and forth between locations. You'll have more time for important tasks, and you'll be able to respond more quickly to user queries. Fast responses mean more efficient and satisfied users—parameters that any IT department is being assessed against.

PERFORMANCEGUARD

PerformanceGuard helps you identify IT problems whenever and wherever they occur, whatever the cause, and whichever end user they affect. It does this by monitoring the actual quality and quantity of IT service deliveries from the end user perspective. With PerformanceGuard you can identify downtime, monitor user experiences, measure and evaluate defined KPIs, etc.

Book a meeting

Call us to book a presentation of our products that can save you and your organization vital time.

CapaSystems
...because time matters

CapaSystems A/S
Roskildevej 342C • DK-2630 Taastrup
Tel. (+45) 70 10 70 55

www.capasystems.com