The hidden risks of BYOD in corporate training, and how to mitigate them (Sep 15)

While it is a simple, cheap way to ensure learners have mobile access to corporate training apps and performance support resources, there are definite security risks for companies practicing BYOD.

Posted by Chloe Green on 17 September 2015

70% of employees receive no instruction about the risks of using their own devices at work

Want to use your own phone for work? You might already be doing it. You might be syncing your work email, researching a project online, or promoting a new product all on your mobile device. In fact, you're probably not even thinking twice about it.

Bring Your Own Device (BYOD) policies formalise this and validate employees' work on their own mobile devices. In fact, according to a recent study by TechPro Research, 74% of organisations have adopted or plan to adopt BYOD.

The BYOD trend is so widespread that Gartner predicts 70% of professionals will be doing work on their personal smart devices by 2018.

Why not apply this trend to corporate training programs, especially with the rise of mobile learning (mLearning) functionality in learning management systems?

Almost three-quarters (74%) of learners report using mLearning tools while travelling and another 52% use the tools while lying in bed after waking up. For employers looking to train their employees, it's tempting to use BYOD to ensure new workers can access training materials more often.

After all, people are likely to have their personal device on them at all times, and this presents more opportunities for them to brush up on a course, watch a training video, or play a learning game.

But in this headlong rush to use employees' own devices for business activities, there are hidden risks. Indeed, the dark side of BYOD is only recently starting to get some serious attention from security researchers and IT experts alike.

Everyone seems to agree that the most obvious, potentially damaging risks involved in BYOD come on the security side:

A smartphone with sensitive corporate data could get lost, a tablet with access to the company's intranet could upload malware through a compromised app, and a public Wi-Fi connection could be used to steal passwords and data on employees' devices.

These are all legitimate risks, to be sure. Yet there's one BYOD risk that seems to be getting considerably less attention, but which is potentially just as damaging as a security breach, and maybe even more-so for the long term health of your company.

The legal challenges of BYOD break down into three distinct buckets:

Intellectual property

Who owns the content on an employee's phone when the employee uses the phone for work?

If, as part of an mLearning exercise, an employee creates a piece of content, do they own the copyright to that content, or is it "work for hire" and the property of the company?

eDiscovery

The Southern District Court of Illinois recently fined a company almost a million dollars for 'the failure to preserve and/or untimely production of business related text messages on certain employees' cell phones.'

The message is very clear: when employees use personal mobile devices for work-related activities, those devices and the data on them become discoverable during lawsuits. Preservation of that data also becomes partly the responsibility of the employer.

Employee reimbursement

In a landmark case out of California last year, **the Court of Appeals ruled**:

'When employees must use their personal cellphones for work-related calls, Labor Code section 2802 requires the employer to reimburse them. Whether the employees have cellphone plans with unlimited minutes or limited minutes, the reimbursement owed is a reasonable percentage of their cellphone bills.'

While this ruling only applies now to employers in California, and only refers to minutes, not data, it sets a worrying precedent for BYOD adoption in the rest of the country. Smart trainers will need to make allowances for a wider application of this ruling when planning for the future of mLearning and BYOD at their company.

Are you prepared to reimburse employees for the time they spend on your mLearning app outside of work? Can your company track the data and usage to determine a 'reasonable percentage' of an employee's cellphone bills to pay?

How to mitigate legal risks with BYOD in corporate training

To reduce your company's exposure to these hidden legal risks, do these three things:

Create and communicate a BYOD policy. A good BYOD policy, effectively disseminated to employees, can inoculate you against many of these risks.

Make sure to include what constitutes acceptable use of the mobile device, what security measures an employee must implement on the device, privacy and monitoring rules, and reimbursement policies or lack thereof.

Put technical precautions in place. This could cover anything from setting up a VPN, to restricting access to corporate networks for mLearning apps, to copying work-related information to a corporate server.

Ensure employment and contractor agreements spell out how IP is handled. A sentence added into employment contracts can save a lot of headache later on.

While it's impossible to completely avoid the legal risks inherent in using BYOD for corporate training, being aware of them, and setting up precautions to mitigate them, can protect you and your company from a lot of potential pain.

If you choose to ignore them instead, you do so at your peril.