Blurred Lines: Device Security and Ownership in the Post-PC Era

- Posted by Alastair Mitchell on August 29, 2013 at 10:20am
- View Blog

Sitting at your PC in a fixed office location and closing the door on your work when you leave the office has fast become a thing of the past. Today, we're constantly connected via our smartphones, tablets and laptops.

Chances are you've already sifted through your inbox and responded to emails before you've even walked through your office door, you've reviewed the agenda and related documents as you travel to that all-important meeting and your colleagues can contact you at any time, regardless of location. This is the post-PC era and we are constantly connected.

Research house IDC's Smart Connected Device Tracker predicts that tablet shipments will surpass PCs this year, with the tablet market expected to hit a high of190 million shipment units -- year-on-year growth of 48.7%. The smartphone market is also expected to grow by 27.2%, while PC shipments are set top decrease by 4.3%.

This meteoric rise of mobile devices -- along with the cloud -- has resulted in the rise of the power worker. These workers have combined personal devices and services with those provided by the enterprise to create their own virtual workplace. They have personally selected a mixture of tools that ensure they are productive and work effectively regardless of the time, place or the task in hand. For enterprises, this presents a number or security and control issues.

In Huddle.com's Mobile Enterprise Landscape study, carried out by Ipsos MORI, 73% of U.S. office workers using enterprise-owned tablets download personal software and apps, while 52% use personal laptops, tablets and smartphones to store and work on enterprise content. So companies are presented with a security conundrum. As well as ensuring the safety of enterprise data when it leaves the company's four walls on mobile devices, companies need to also mitigate the risk of employees inadvertently downloading viruses or other malware their phones, tablets and laptops.

And when it comes to stashing enterprise content on personal laptops, tablets and smartphones, U.S. office workers aged 18–24 years old are the most likely culprits: 51% keep work documents on personal laptops, 42% store work files on personal smartphones and 11% keep enterprise documents on personal tablets. Given that millennials are not just tech literate, but used to using whatever technology they want to get their jobs done (as I mentioned in my previous post), this shouldn't come as a surprise. But how can the enterprise deal with this coexistence of devices in the workplace given that it's becoming the norm and not solely a generation issue? The answer lies in looking beyond the device.

Controlling devices is yesterday's problem. We have now moved beyond that and IT departments should now be looking at how to control the cloud tools and services being used. People are going to mix and match the devices they use and while organizations can retain control over enterprise-issued devices, there is little they can do about personal devices. You need to control where the information stems from and that means turning to enterprise-grade applications that combine usability with security measures such as granular permission, encryption in transit and at rest, and remote wipe capabilities.

The post-PC era is well and truly here and we now need to look beyond the device to securing the data in the cloud.

Alastair Mitchell is co-founder and CEO of Huddle.com.