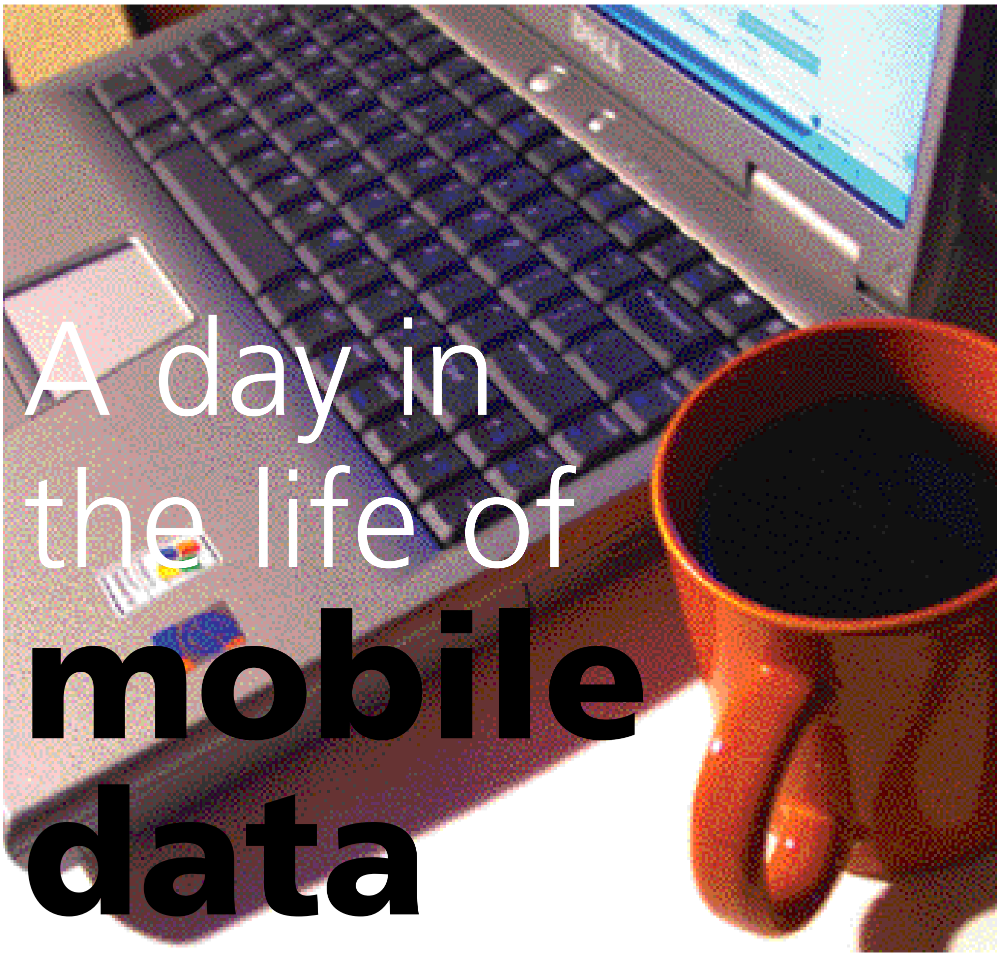

A day in the life of **mobile data**

Very few companies worry about the cost of replacing mobile devices, it's more about the value and amount of data that resides on them and the adverse consequences to the company if the data on these devices falls into the wrong hands.

According to a recent Gartner study over 80% of new and critical data is now stored on mobile devices – so securing these devices is becoming a business necessity and one that can no longer be ignored.

Let's take Ben, a typical mid-level company executive and look at how much data he uses in a working day and how easily he can jeopardise the company if this data goes missing. Ben wakes early on Monday for a big day that will include a quick stop at the office, two airline flights, a client sales presentation, and a dinner meeting with a potential partner firm.

Before leaving home, he copies the sales presentation he worked on over the weekend from his home computer to a 250 MB USB data storage device for transport to the office.

After arriving at the office he boots up his notebook PC, and then logs in to the network to update his CRM files and download the revised product roadmap and the new price sheet.

He almost goes through the familiar steps of synchronising his contacts, calendar and certain documents with his smartphone, but then remembers that the new Bluetooth enabled version transfers that information automatically. Still, he must manually load the sales presentation from the USB device. Feeling sleepy, he dozes briefly on the train out to the airport, then sits in the gate lounge area making sales calls and setting appointments while logged onto a 'hotspot' for email access.

After the aircraft reaches cruising altitude Ben uses his notebook PC to finalise his sales plan for a meeting with the company CEO. He saves the proposal on the notebook, and, just in case, also copies it to the USB device

Arriving at the airport, he takes a cab to the client office and makes a few more calls on his Smartphone, while referencing files from the notebook PC perched on his lap.

The sales call goes well, but the client wants to know how long the project will take. Ben uses a local internet connection to access and download the appropriate information on parts and labour availability. After signing an NDA, Ben is allowed to copy confidential information regarding the client's new project from a floppy.

The new client president invites Ben to lunch. He leaves his briefcase and PC at office, but takes the Smartphone with him.

After a cab ride back to the airport, and the familiar routine of waiting, loading and landing, Ben rents a car for a quick drive to the hotel.

At the hotel, he briefly leaves his belongings in the car while he checks in at the front desk.

At dinner, Ben's CEO gives him advance notice of a favourable analyst rating of the company, but also discloses some potential litigation that might affect how the company may market its product. Ben makes some notes on the Smartphone for follow up. Ben then agrees with his boss to see a musical at a nearby theatre. He leaves the notebook PC in his hotel room, but takes the Smartphone.

Late that night he downloads a few more emails, make notes from his meetings and drops exhausted into bed. "Where is that USB device?", he mutters as he falls asleep.

Although Ben is only a mid-level executive, he still has access to very sensitive company data which he is storing on numerous mobile devices.

This vignette clearly demonstrates that, for just this one executive on one day, the company had multiple risks of losing very valuable and sensitive information. Consider how easy it would have been to leave the notebook, the smartphone or the USB device on the train, in the cabs, at the

airport, on the airplane, in a rental car or at the restaurant. Mistakes like that happen frequently.

But sometimes data loss is no mistake but instead is the result of planned or opportunistic theft. Ben's catnap on the train might have tempted a watchful thief to swipe the phone, notebook or storage device. Other thieves are known to work airport lounges and rental car counters of hotel lobbies. Leaving a PC in a hotel room is a common occurrence that can also lead to theft. And how smart is it to leave a notebook PC sitting in the conference room of a client while out for lunch?

These are commonplace risks that people have learned to at least recognise, even though their behaviour does not change. But there are other, subtle and less known ways for data to leak out. Consider the Bluetooth personal area network technology built into the smartphone. If Ben inadvertently leaves his smartphone in Bluetooth's 'discover' mode, adept foragers can penetrate the device remotely to empty out the information that Ben thinks is still secure. Could he have exposed his PC to the insertion of spyware or a Trojan when he used his client's network?

Because of the scope and sensitivity of the data that he carries, Ben is a walking treasure trove for competitors or thieves, and a potential time bomb for his own company. The company must implement a mobile device security system with the following:

Automatic and transparent protection of all data

Ben needs a system that will automatically and imperceptibly encrypt everything he stores on his PC, smartphone or USB device which will also maintain security as he synchronises the information between them.

Robust operation with an Efficient help desk

Ben should feel confident in the quality of the system and also know that if a problem develops he is not stuck, no matter where he is and that at the end of a phone he can get hold of authorised administrators who can recover data, or if he can access the online help desk, he can probably solve the problem himself.

Enterprise enforcement of security policies

It's not all about Ben – the company bears the greatest risk. Company security officers understand the crucial importance of a mandatory and enforceable security system that assures compliance with company security policies. An enterprise security management infrastructure is required to deploy encryption and authentication capabilities on each mobile device, keep policies up to date, and to continuously monitor compliance.

Just as importantly, the company must be able to centrally store all the keys and authorities necessary to access data on any personal computing device.

Proof of security

Today it is not sufficient to merely have purchased a security product, companies need to prove that the security system, including technology, policy and procedures, is properly implemented and continuously effective. Since few organisations have the expertise or budget to assess the technical merit of enterprise security products, they should seek products that have been independently evaluated by government-certified laboratories as complying to at least mid level FIPS or common standards.

Summary

Mobile devices are an important, growing, and productive part of the information infrastructure of modern enterprises. However, greater efficiency in the field carries a heightened risk of compromising sensitive and confidential information via carelessness or opportunistic theft. Even the most diligent employees cannot adequately protect the company's data, so the organisation must provide an effective security system that automatically protects data according to central policies.

Martin Allen, MD Pointsec Mobile Technologies www.pointsec.com