A self-destructing phone isn't the last word in security

March 5 2014, by Bernardi Pranggono

When is a broken phone not really broken? Credit: Hugovk

Businesses battling to keep their information safe pricked up their ears last week as it was announce that Boeing has produced a mobile phone that self-destructs should the wrong person try to use it.

It sounds like the stuff of Hollywood action movies but the idea of being able to protect phones in this way could offer the solution to a rising problem.

More and more employees are using their own mobile phones or laptop for work purposes and the consequences for their employers are alarming.

A recent survey showed that devices are being lost or stolen, putting sensitive data in the hands of strangers and even criminals. Even when it isn't lost, businesses have to think about how to cope with the threat of cyber-attacks. Devices such as smartphones and tablets typically contain a large amount of sensitive personal and corporate data and are often used in online payments and other transactions so this is a serious problem.

Boeing's proposition therefore seems rather attractive. While it is currently only for use by US government employees, the super-secure self-destructing smartphone developed by Boeing seems like the ideal way for businesses to make sure their staff remain connected when out of the office without the risk of losing company secrets.

The Boeing Black is designed to wipe itself of all data if it is tampered with. Detailed specifications remain confidential but what we do know is that the phone comes with lots of features for the security-conscious user and a "trusted boot" mode that is able to detect and thwart any attempt to root (hack into) the device –- or disable it if it can't.

To make it all the more secure, Boeing Black relies heavily on encryption technologies. It has media encryption for internal storage and can be configured to hinder certain functions based on location or the network it is connected to in order to avoid data loss.

The phone has embedded FIPS 140-2 key storage, meaning that it meets the highest standards for security set in the US. The crypto keys are stored on a unit that actively looks out for attack, be it electromagnetic or physical.

However, Boeing says the phone has also been designed with "modularity" in mind. Its hardware can be adapted to suit the individual needs of a business and it runs on the Android operating system, meaning the software is adaptable too.

And this might be its downfall. Modularity does not traditionally go hand-in-hand with security. There is always a trade-off between security and access. If the phone has a USB connector and microSD card slot, for example, information could be stolen from the phone before the device can trigger self-destruct function.

On the software side, the widespread use of open-source smart device platforms such as Android and third-party applications open up a huge range of possibilities when it comes to what you can do with your phone, but they are also attractive to the creators of malware. Smart devices are becoming one of the most lucrative targets for cyber-criminals for that very reason.

Boeing's phone is based heavily on the Android platform, which is notoriously insecure. It has been estimated that more than 98% of the malware detected in 2013 was aimed at Android devices.

This is not particularly surprising since Google, which runs Android, uses an "open security" strategy to gain the biggest market share possible. The more people able to use your platform, the more money you make, so Google wants to spread the net wide, even if that means letting in some bad guys. It has made the process of publishing an app on the Android platform very easy for developers but also provides too much space for malicious application creators. Android currently has more malware compared than other mobile operating system such as Windows Mobile, Blackberry and Apple.

So in going for adaptability, Boeing has made the security challenge

particularly hard. It might have produced something exceptionally secure according to current standards, but the fast pace of change in the development of malware could soon change that. The company itself may be dabbling in Android, but it continues to use the Blackberry platform as its standard, perhaps suggesting it is not entirely confident in Android.

Then there is the problem of advertising yourself to criminals. Since the Boeing phone is only going to be used by people handling highly sensitive data, simply having one in your hand should act as a clear signal to would-be attackers that you have something worth stealing in your hand.

And ultimately, as long you use some kind of memory to store information inside the phone, it cannot be truly secure. With digital forensics technologies, it may possible to regenerate the information stored in the memory even though the phone is in unusable condition. We have to hope Boeing has thought of this but the secrecy surrounding the details of the device make it difficult to tell.

If a phone like this is to be taken up by businesses on a larger scale, we may need to know more about what's in them. But that, in itself, might jeopardise their security. Businesses need to know what they're buying but they need to keep their secrets from criminals to make it worth the money. They might just be better off getting their employees to hold onto their phones more carefully when they leave work.