

## Could your mobile device land your CEO in court? —by Sean Glynn, Credant Technologies

*Are business people breaking the law? If you use a portable device to store contact information, you are probably subject to some data security regulation, law, statute or mandate. On a laptop, smartphone, PDA or any other endpoint, data encryption is the best technical method to secure personal data.*

The humble PC is now about 25 years old, and the IT security industry—which has been with us for almost as long—has been changing in the last 2.5 years much faster than it did the last 25.

The Smartphones powered by the Windows Mobile, Symbian, Apple and Blackberry operating systems are microcomputers in their own right. But their processing capabilities are significantly lower than the power of their desktop cousins. Our best estimates here at Credant are that the smartphone in your pocket or purse probably has the processing power of a PC of about a decade ago.

And therein lies the problem. On most smartphones, encrypting data on the fly—if done the wrong way—can consume much processing power, and time. Frustrated by the static hour-glass symbol indicating that the device is encrypting, users more often than not lose patience and cancel the process.

What can possibly go wrong if you don't encrypt the data on your portable device? Quite a lot. Consider the growing number of states that have adopted data security laws and statutes—they wouldn't have addressed data security if there were no good reason to do so. Even the American Recovery & Reinvestment Act (ARRA) of 2009 mandates additional data breach notification requirements for certain types of companies and activities.

The data security issue is compounded by the fact that many company employees use their own portable devices for business—or vice versa—without these devices being protected by the full range of security safeguards applied to company PDAs, smartphones, and laptops.

The need to ensure compliance with laws and regulations consistently across the board moves the issue of data protection out of the “good-to-have” and into the “must-have” realm. Luckily, data can be secured—effectively—with expert knowledge and seamless software that won't slow the device down.

Take, for instance, the latest crop of Palm mobile devices which have a data capacity of at least 2 gigabytes if, not much more, and can store thousands of e-mails and medium-sized documents. If unprotected, this data is wide open to anybody with a mind to do a “bit of monitoring” or launch a malicious cyber attack.

Encryption is one of the techniques available to protect mobile communications. It won't stop eavesdroppers—be they profit-driven industrial spies or the NSA—or the good old hackers from intercepting your messages, but it will stop

them from gaining any useful information.

Protection of data stored on laptops and smartphones used interchangeably for business and in private is highly recommended, given the growing number of high-profile device thefts. In many states, it's legally required that company contact information, staff home addresses, mobile phone numbers, and even home phone numbers are protected.

To give an example, the new Massachusetts regulation 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth states in 17.03: “Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information.

Who is liable under this regulation. As defined, a “person,” is a living person, or it can be a corporation, association, partnership or another legal entity of the Commonwealth. In other words, this “person” could be the owner of a business or a company executive and could conceivably include the person who stores information about a business or company on their portable device.

If the data is on a smartphone, laptop, or other endpoint device, and it is there by company consent, then it's the company that's liable for any data misuse. In other words, if your portable device falls into the wrong hands, your boss could find himself (or herself) in a courtroom. Even if the data is on the mobile device without the company's knowledge, the company is still liable because it has failed to protect the data. There is simply no way round this.

Protecting data on mobile devices involves both technical and organizational measures. Data security on mobile devices is an evolving area, with an evolving legal framework—it would thus be best not to let the courts define it.

Organizational security measures can be enforced through a formal security policy designed to protect the mobile device and its data. Devising appropriate technical measures is more difficult. If the goal is to protect the corporate mainframe, then we would obviously be thinking about a firewall. Most mobile devices are sold without firewall protection, so it's up to users to keep confidential information safe.

Encryption is an advisable course of action. Ultimately, if a company or private laptop, PDA, or a smartphone contains sensitive customer information, then both you and your boss should seriously consider ensuring data security on those devices.—Or face the judge.