



Encryption and beyond

Every time there is a high-profile data breach the media screams out about the need for encryption right across the board. Unfortunately with the economic climate in its current condition, some people will do anything to raise cash so further steps are needed to secure information

The encryption of data on USB devices, CDs or DVDs has received a lot of coverage since the HMRC lost a couple of discs a while back. By adopting encryption and thus doing away with the potential catastrophe of a member of staff losing vital information, a company is taking a massive step in the right security direction.

For example, BlockMaster recently announced a contract to distribute over 100,000 SafeSticks (secure USB devices) to NHS hospitals across the UK. The units will provide security for all removable storage through encryption.

The SafeSticks will provide the NHS with protection through mandatory password protection and automatic hardware encryption and timer lockdown functionality which locks the units if there is no user activity for a configurable period of time, preventing data loss if they are lost or stolen.

Robert Howorth, Senior Technical Architect at West Suffolk Hospital NHS Trust, commented: "We were faced with the constant challenge of keeping our data safe, but also ensuring staff can work remotely to increase efficiencies. The security of patient data is of paramount importance to us."

This is a major concern for companies across all sectors of business today. If you want to enable employees to work remotely or to be able to transfer information from one point to another, USB sticks are the ideal solution but what kind of risk are you taking on board in order to do this?

Daniel Östner, CEO at BlockMaster comments: "The number of unsecure USB sticks lost each year is a problem we cannot sweep under the carpet. We need to be proactive with USB security and not wait for a breach to happen until we think about it. It's fantastic news to see that the NHS is leading the way with USB security. The introduction of best-practice and diligence by organisations will protect sensitive data on portable devices and prevent embarrassing, as well as costly data breaches."

Mike Bienvenu, Technical Director, of installer Softek continues: "Critical data loss is on every IT Director's mind, and with a frightening 66 per cent of all USB sticks being lost or stolen, data stored on memory sticks simply has to be encrypted - the challenge has been achieving this quickly and easily without employee re-training or disruption."

The actions of the NHS should be applauded as a huge proactive step, but in the case of the average commercial UK business, encryption only deals with part of the USB dilemma. The technology of today allows you to download data in seconds and whilst there are many different types of systems available in order to stop someone from reading the information on a lost or stolen device, what about those deliberately downloading data in order to sell or distribute it maliciously?

The recent farrago with the MP's expenses showed just how easy it is to be able to cause maximum disruption if you have the right data and someone willing to buy it. The temptation to make money out of information one has access to is always going to exist. In this situation encrypting data on a USB device/CD/DVD etc would not have worked, some other measure such as port monitoring/port denial is needed to prevent the data being downloaded in the first place.

There are so many facets to data security there is only one panacea; get rid of all humans. It is the user that is the risk not the computer. Even down to the basics. How many of your staff would you trust not to plug in a USB pen that they had found on a train, just to see what is on it? Your data is at risk from all angles but in particular from the person sitting in front of it.

Andy Clutton MCIJ

E: andy.clutton@risk-uk.com