

ITAnalysis – Should encryption be optional?

By Fran Howarth, Principal analyst, Quocirca Ltd

No organisation is immune from obligations to comply with the laws of the countries they operate in and most countries, including those in the EU, have data protection laws that apply to all. Data protection laws are mainly concerned with the privacy of individuals and aim to ensure the safe keeping of information about them, collected and stored by businesses and governments. Such laws limit the ways that personal information can be processed, stored and used in order to protect the privacy of individuals.

Advances in technology have increased the ability to process, store and share vast amounts of data on individuals for a variety of uses, ranging from tax databases held by governments to customer lists and financial records held by banks and retailers. However, the ability to share this information is also one of the key factors that is leading to data breaches becoming more and more widespread.

Data breaches occur for a variety of reasons, from deliberate attempts to steal data to carelessness with portable computing and storage devices. And the problem is getting worse as the number of such devices proliferates. According to data breach clearing house Data Loss DB, of the data breaches that were made public in 2008, more than 32% resulted from the loss or theft of laptops, mobile phones, or other portable media and storage devices.

There are many ways that an organisation can protect itself from such losses, including using technology to determine and enforce which individuals can access what information, and what they can do with it. Data loss prevention tools can discover where information resides and monitor and report on all usage of data, imposing controls on where information can be transferred according to policies set. Such tools can prevent information being transferred to portable devices in the first place.

However, there are many legitimate cases where an organisation wishes its employees to carry sensitive information with them, such as a field engineer needing to access product blueprints or a doctor carrying sensitive medical information regarding patients. The best way to protect information on the move on portable devices is to ensure that it is fully encrypted at all times when the device is idle or powered off.

But should something that is considered best practice could also be considered to be optional? In the eyes of many authorities, that is no longer the case. In the US and many other countries, security breach legislation has been passed that demands that organisations that suffer a data loss that could lead to personally identifiable information being compromised must publicly notify the effected individuals. However, there is at least one caveat in most of these regulations—if the data that was lost was encrypted in an acceptable manner, it is considered that the data is secure and no public disclosure of the breach is necessary.

Even in jurisdictions where specific data breach laws have not been passed yet, including most countries in the EU, existing laws related to human rights, privacy and data protection allow authorities to take sanctions against organisations that have suffered data losses owing to inadequate levels of security protection being applied. The following statement was recently issued by the Information Commissioner's Office in the UK and applies equally to public and private organisations: "Where the information held on a laptop or other portable device could be used to cause an individual damage or distress, in particular where it contains financial or medical information, they should be encrypted. The level of protection provided by the encryption should be reviewed and updated periodically to ensure that it is sufficient if the device was lost or stolen, you may need to seek specialist technical advice. In addition to technical security, organisations must have policies on the appropriate use and security

of portable devices and ensure their staff are properly trained in these. If it is brought to the Commissioner's attention that laptops that have been lost or stolen have not been protected with suitable encryption he will consider using his enforcement powers."

Any organisation that requires its employees to work remotely should take a hard look at its policies regarding information that can be carried on portable devices and should consider using encryption for any device that may end up with sensitive information stored on it. At present, the best way to do this is to deploy full-disk encryption software, looking for products that offer strong centralised management capabilities for ease of deployment and management.

In the future, self-encrypting hard drives and portable devices will start to become widespread. A new standard published in early 2009 by the Trusted Computing Group—the Opal standard—is designed to address the issue of data at rest to provide protection against offline attacks. This standard is being embraced by a number of storage vendors, including Fujitsu and Hitachi, which are incorporating the standard into their products and will shortly make available self-encrypting drives based on this standard, allowing interoperability among all storage devices and ensuring that devices ranging from desktops to USB sticks are fully encrypted when powered off.

Quocirca's recently published freely available report, [Removing the complexity from information protection](#), discusses how full-disk encryption can aid organisations in reducing the risk of data loss through device loss or theft, and looks to the future when self-encrypting devices will become the norm.

Comment Article

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at
<http://www.quocirca.com>