# It's time to take encryption a lot more seriously

By Oliver Potgieter

9 Sep 2014

Just like backup is something every business owner knows has to be done right but often isn't, data encryption is emerging as another essential requirement which is routinely ignored. And just like backup, many business owners find themselves shutting the stable door once the horse has bolted - and suffering the consequences of a breach in confidentiality as a result.

Oliver Potgieter

The necessity for encryption is heightened with the increased mobility of data, whether on smartphones, laptops or USB thumb drives. There are, of course, legal obligations to protect data, particularly if it is customer information. Failure to do so can even carry criminal liability.

Be that as it may, encryption typically falls into the 'too hard basket'. It's a hassle for those in IT to ensure that data is encrypted; for those in charge of the purse strings, encryption tends to look like a cost without a clear return. This perception is as true for the small to medium enterprise as it is for quite considerable companies; even in organisations with 1000-plus users encryption is often the one obvious hole in the IT strategy.

But does encryption have to be all that difficult? No it doesn't. However, the 'traditional' approach to end-point security has been hard in the past, with manual processes and potentially high overheads, and management akin to something out of a nightmare.

Encryption doesn't have to be like that, but this is a major reason for the ostrich approach.

Solving the problem starts by identifying where and what the data is, and examining the risk areas. Data that moves is more susceptible to interception; for example, a company which has USB drives embedded in the business process is at particular risk if the drives are unsecured and move between work, customer, and home computers with no control.

Once you know where and what the data is, you need to work out how to protect the information and at what level. For example, some free open source solutions (FOSS) may be suitable for lower-level requirements, but these come with their own potential shortfalls. The recent confusion around the status of open source encryption solution TrueCrypt demonstrates the inherent risk of depending on FOSS, particularly for mission-critical applications. For more robust and elegant encryption, enterprise-level solutions may be necessary.

The simple question to ask is 'how important is my data and company reputation'? The best way to consider that question is to imagine the consequences should that information get into the wrong hands.

Far better to do something about it before, rather than after that actually happens.

## ABOUT THE AUTHOR

Oliver Potgieter is the director of Alto Africa