Data encryption adoption represents a significant opportunity

Vision, meet reality

By Andrew Buss, October 2010

Originally published on
CRN CHANNELWEB.CO.UK

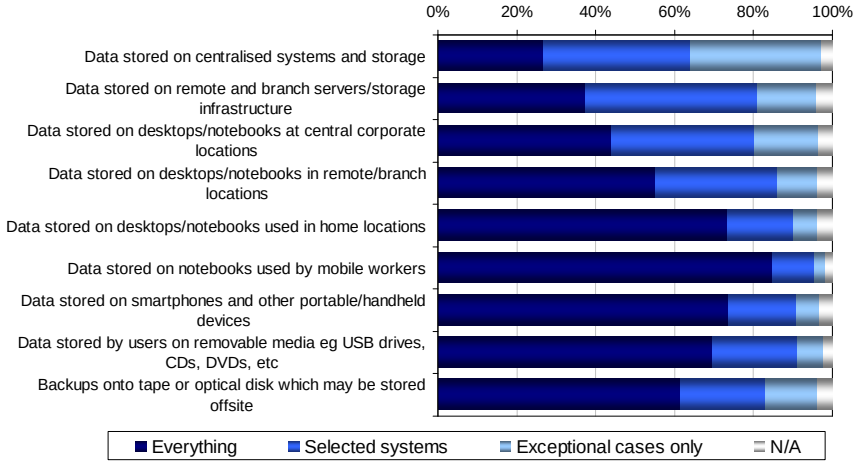
Data protection continues to be a top of mind subject for many companies. Data losses continue to occur on a regular basis across both public and private sectors. With increasing penalties for data breaches and new responsibilities coming with impending data loss notification regulations, encryption is one of the key tools to reducing business risk by enabling effective data protection.

We recently ran an online poll examining the difference between the vision and reality for encryption. Bearing in mind that online polls tend to be self-selecting, it is fair to say that a good number of respondents will have a healthy interest in IT security or encryption. This will bias the numbers somewhat towards protection or encryption compared to a more balanced or random sample but is a great indicator of what IT security professionals are thinking.

One of the first takeaways to emerge is that encryption increasingly is being used as a pro-active data protection strategy. In the past, encryption in many cases was used to lock the barn door after the horse had bolted. While this remains the default response for a significant number of companies, it is new drivers that are now pushing the implementation of encryption. These include advances in working practices such as mobilisation and home working; a recognition that the amount and detail of data being stored is snowballing; Compliance directives, such as the PCI DSS, together with tougher legislation have also led to the realisation that doing nothing is no longer an option.

The realisation that encryption is part of the overall data protection approach means that it is interesting to see where its deployment is felt to be of most advantage. It is of no great surprise that the top targets for encryption are geared around the move to mobility, particularly mobile notebooks, but also cover smartphones and computers used for work in home locations.

In an ideal world, which of the following do you think should be encrypted and to what degree?

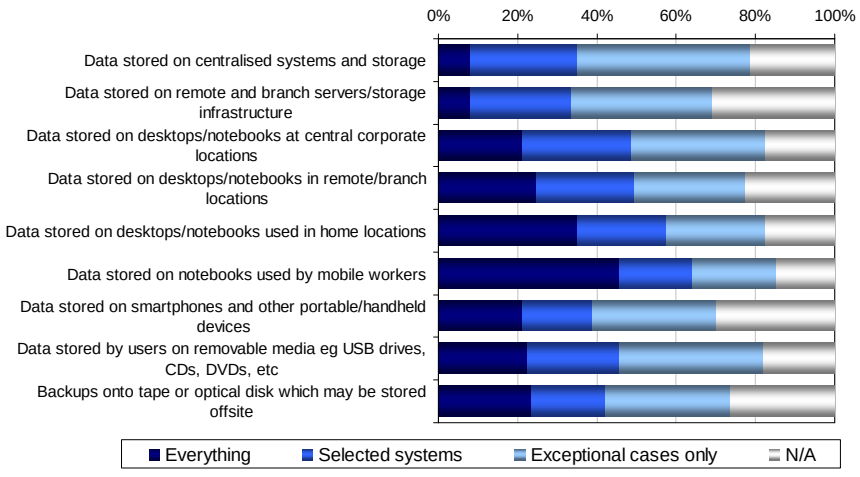


Source and Copyright : Freeform Dynamics Ltd
Online survey (383 total respondents) completed June 2010

What is also interesting is that the need for protection is based around the perceived vulnerability to loss or theft. Mobile notebooks are perceived as needing encryption more than PCs in central corporate locations. But thefts can and do occur regularly from office locations. Also, backup encryption is viewed as important as they may be stored offsite, but data on servers in remote branches or in the data centre are not. But in many cases, these servers may be just as much a risk for data loss if, for example, disks are disposed of without secure erasure of the data on them, or the data exists in the form of easily copied, unprotected virtual machines.

What is even more interesting is contrasting the vision of where encryption should be used with what is actually being done today, and the difference is profound.

Which of the following are currently encrypted in your organisation and to what degree?



Source and Copyright : Freeform Dynamics Ltd
Online survey (383 total respondents) completed June 2010

If we look at the encryption of data stored on notebooks by mobile workers, which is where encryption is most widely implemented, the biggest barrier is not to do with the load on systems or the cost of the solution, but is instead concerns around the practical implementation of the solution. This is followed, perhaps surprisingly considering the feedback we keep getting about the headaches involved, by the challenges of key management. And these challenges are not unique to encryption on notebooks. It is a common theme around pretty much all encryption implementations, despite the increasing availability of low-cost solutions and more integrated offerings.

Clearly there is a lot of room for improving data protection with encryption. The fact that there is such a disconnect between vision and reality is down to a combination of factors, but also means that there is a significant opportunity to add value by integrating the various encryption technologies into an integrated and manageable "stack".

Encryption is a broadly applicable technology, suited to both infrastructure and client, and to protect data at rest, in motion and in use. That means that strategically, encryption should be a unified implementation across the company, regardless of where it is used as all the elements will have to interact and interoperate. Realistically, this is not likely to happen overnight. But planning for this can help.

The first priority is to deal with the immediate pain points around mobility and compliance that numerous customers will feel. In many cases this will mean protecting the data at rest on devices, most likely a notebook or smartphone or else a portable storage media such as a USB stick or writeable DVD. This could be achieved through encryption of the entire device, as with some smartphones, or through tools such as file encryption or full disk encryption for PCs or servers.

The trick will be to avoid re-inventing the wheel and to re-use where possible existing infrastructure tools such as key management systems. Getting a single platform to cover multiple encryption implementations is still challenging, although the situation is starting to become a little more integrated. The key management platform must also retain compatibility for long periods of time as data held in backups, archives and even in more active locations may need to be accesses over a period spanning decades.

Once the basics have been addressed, which should start to close the gap between vision and reality, a more integrated approach may be suitable. Encryption can be extended further into the infrastructure so that data on servers, for example, is protected, not just when it is copied onto a notebook. After all, many security breaches, whether intentional or accidental, occur on the "inside" of the company.

And once these encryption fundamentals are in place and in widespread use, further refinements may make sense. Technologies such as Rights Management and Data Leakage Protection can help to protect data at what is arguably the weakest link, the end user that has a legitimate right to access it.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.