



VNUNet – Footsteps in the Sand

By Clive Longbottom, Service Director, Quocirca Ltd

I recently had the honour of being among a team of storage managers from large companies around the UK.

Discussions centred mainly around virtualisation and maximising utilisation rates, bringing together disparate vendors' kit as a single resource pool and how to manage data growth as voice and video are brought in to the mix.

However, the area of data disposal led to some serious debate. The vast majority were not overly concerned about the fact that a simple deletion of data leaves the data still on the disk; only the headers go, and you are at the whim of the disk controller as to how and when it overwrites the information with new data.

The main approach was that "secure deletion" of data was only needed on data disposal - i.e. on getting rid of the disk drive itself - and for this, a large hammer was the preferred approach.

But, let's look beyond the initial reaction of 'why would I want to ensure secure deletion of data in an environment that I control?' and see whether a degree of paranoia is called for.

Data retention laws are becoming more commonplace, and data disclosure is being used by legal and governance bodies worldwide to ensure that things are as they should be.

With the likes of Microsoft and the UK government finding that emails do not easily disappear, maybe a better approach to secure transfer and deletion of certain types of information may be worth considering.

How about taking a fairly simplistic case? A person creates an email locally on their machine. This is then submitted, and a replica is stored on the server.

The server sends this email to the recipient's server, where another copy is made, and then it is delivered to the recipient, where another copy may be created.

Should the recipient decide to forward this message, we see the same happening again: more copies (which is wasteful of storage resources anyway), and more footprints in the sand enabling anyone to trace the route of a communication even if the original message has been deleted.

The same applies to all sorts of information - transactions within databases, the creation and backup of documents and so on - and each time we take an action, we are leaving traces.

In the majority of cases, it makes no difference. The information contained within the majority of documents and emails have little real business value, and even fewer have the capability to negatively affect the corporate brand should they be uncovered.

But there will always be some. There may be the discussions around a possible merger/acquisition, there may be the in-depth analysis of the competition, there may be documents detailing specific opportunities within prospects and customers.

We may want to choose not to be forced to disclose these should a court request it. We may want to be able to regard these items as being just the same as a private person-to-person discussion, with a degree of deniability around the actual contents.

So, how can we do this? Well, we can start by ensuring that we understand the priorities of different types of information, such that only the information that really needs special handling gets the full treatment.

We can then take the necessary steps to create an environment for informational safety:

- We can apply security at the intellectual property asset level (document or data field) to ensure that only those who are meant to see information do get to see it

- We can apply controls on what can be done with the document, for example stopping a document from being printed, from cut and paste working, from being forwarded to others
- We should apply the capability to rescind document access from those whom we decide we aren't as sure about as we might once have been, such that the document will self-destruct from their device should they try to access it
- We need to make sure that when we delete a document, it is deleted. The disk drive on which it resides should hash over the file contents repeatedly until only the most in-depth forensic tools would be able to recover the underlying information
- Not only do we need to ensure that it deletes from us, but that it also deletes from any other systems where it resides, from our own backups and mirrors, from any recipients inboxes, from their file systems and so on, and that this is done through secure deletion

Is this paranoia? I think that we have to take it as a given that within the majority of large organisations there will be information that it is unwise to have committed to any electronic form, but that email being one of the main means of communication will ensure that it is there.

Whether we want to have a means of legal deniability, or just corporate deniability, for some of the information is what we need to decide.

Linux has a built-in Shred command to get rid of information, but Windows and most flavours of Unix do not.

Even with Linux, we have a dependence on being able to see the physical disk, rather than the virtual pointers being held in a virtualised storage environment.

Therefore, we need to look at what else can be done, and a fully integrated storage management/information lifecycle management environment should be able to offer some form of solution.

Some of the vendors in this space are looking at the problem, but until there is end-user pull, it is unlikely that we will see general availability of such capabilities, with only government security services and other high-requirement places having solutions in place, generally via bespoke coding.

Maybe it's time that we started making more noise, telling vendors that secure information and secure forensic deletion is a full requirement.

Only then will the vendor community put in the work to provide a fully integrated solution that is easy to use and yet really ensures that what we want to stay private, stays private and what we want deleted is deleted to all but the most stringent of forensic examinations.

There are point solutions available in the meantime, but making them available to everyone in an easy to use manner is not so easy.

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, Dell, T-Mobile, Vodafone, 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>