How big is your bomb?

David Cadin, partner at Bedell Cristin, looks at the increasing mountain of data generated and stored by businesses

David Cadin: 'As the cost of storage decreases, the amount of data retained is only going to increase'

Let's start with three facts:

- 'In 2011 we...created more data than in the entire previous history of mankind'
- One million business e-mail messages are sent each second or about 90 billion per day
- One gigabyte will store 10,000 documents (or nearly 900,000 pages of plaintext)

LIKE it or not, the computer is here to stay. Email, social media, electronic documents, digital images are an integral part of daily life whether it be at work, rest or play. The amount of electronic information now created and stored is astonishing. As Andreas Weigend remarked, it is increasing exponentially; in 2013 we will probably again create more data than in the entire previous history of mankind.

As the cost of storage decreases, the amount of data retained is only going to increase. Businesses and individuals are sitting on top of vast amounts of information which unless they are well organised could present a serious issue in future.

Take a home computer with a modest amount of memory; add in 40 years of family use, lots of emails with attachments, and correspondence, policies, bank statements all scanned on and you could be looking at a few million documents. Unfortunately, you could actually be looking at those documents at a time when the owner of the computer has just died; sorting it out when the architect of the filing system is no longer around to guide you would be, to put it mildly, a challenge.

Applying that to the business environment is even more alarming. According to Kelvin McGregor-Alcorn, a director leading the Electronic Disclosure Group at Deloitte London, the average amount of data now being found in users' corporate mailboxes has increased tenfold over the last four years and on average users are now holding between 30 and 50 gigabytes of data (or 300,000 to 500,000 documents). Multiply that by the number of users, and even small businesses are sitting on huge amounts of ever-increasing data; data that you probably cannot easily delete.

The problem with keeping everything forever is that you shouldn't. The Data Protection (Jersey) Law 2005 says that you should not keep personal data 'for longer than is necessary'. While this is not exactly helpful in imposing a definite time limit for retention of records, periods of ten years or 20 years are sometimes considered appropriate.

Whatever data you keep and however long you keep it, there is the risk that at some stage you may be asked to retrieve something from the mountain of material and depending upon who is doing the asking (for example, the court, the police, the JFSC, clients, data subjects etc), you may not have very long to do so and may be subject to penalties if you do not or cannot comply. At which point, the issue of data management might look more like a ticking time bomb. Especially when the request leads you to ask yourself some tricky questions (such as what data do we hold, in what format, do we still have the software, does anyone know how to use it, how do we get the data back, what do we have to search for, can we do those searches, what do we do then, how much is this going to cost?)

Although difficult questions, they can in fact be answered relatively simply with some forethought, a little bit of work and a clear (and applied) policy. Indeed, two key points from a recent Bedell Cristin seminar on data management were (a) have a broad discussion in your business now about the data you hold; and (b) be prepared and have a protocol for dealing with data.

Of course, the best time to do this is now; not when you are faced with an order from the court requiring disclosure within 48 hours or when your loved one has just died. It's good to talk, especially if you are talking now about what you hold, where you hold it and in what form. Once you have drawn that line in the sand, you can then move on to consider what you actually need to have, where and in what form. Having done that, it is then time to think about creating a policy, implementing it and making sure that everyone sticks to it so that you can be confident that at any point in the future, you know exactly what you hold and where.

Moreover, for a business, offence can often be the best form of defence; if you have a policy and apply it then you may be able legitimately to limit the extent of requests for your data and discourage or resist requests for data that has passed its destruction date (irrespective of questions about whether electronic data is ever truly deleted). However, if you do not have a policy or you have one but do not apply it, then there is a real risk that at some stage you might have to roll your shirtsleeves up and start examining enormous amounts of data.

And 'enormous' is not an exaggeration: let's take one user with a mailbox containing 30gbs of data (or 300,000 documents); if it took you 30 seconds to review each document to decide whether it is relevant to a particular issue, it would take one person, working seven-hour shifts, 357 days to review this amount of data manually...

Need I say more?