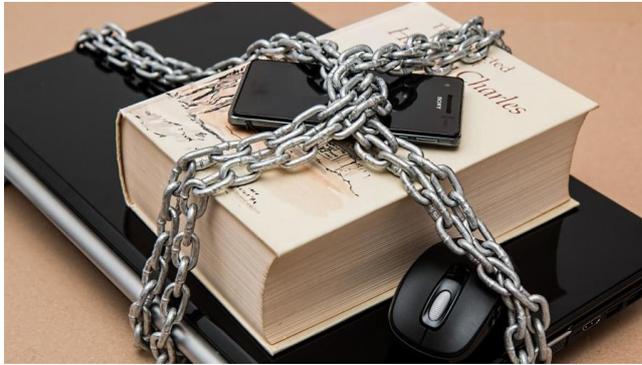


What did we learn in records management in 2015 and what lies ahead for 2016?

15/12/2015

By John Culkin



As 2015 comes to a close there's a nagging feeling in the records management sector that businesses still aren't learning the lessons of previous years – and that 2016 will provide even more challenges.

It is traditional in December – in almost every business sector – to look back on the big stories of the year and consider what was new and what should be remembered.

But when it comes to records management the uncomfortable answer is that what we probably learned exactly the same as we did in 2014, 2013 or 2012.

The more we share online and the more things we connect the harder the job of keeping information safe becomes – and that will inevitably be the big challenge of 2016, too.

A Crown Records Management Survey earlier in 2015 revealed two-thirds of people interviewed – all of them IT decision makers at UK companies with more than 200 employees – admitted losing important data.

A quarter said they their business had been hacked and a quarter had reported a data breach.

These figures are alarming – but they don't come as a big surprise in an era in which data breaches continue to make headlines and in which businesses still struggle to get a grip on keeping information safe.

If you think back on the some of the headlines of 2015, then data breaches featured heavily.

Here are the biggest breaches that defined the year:

1. In the US, hackers gained access to the customer data of more than 100 million people – the country's biggest ever data breach – after targeting nine companies that included banks (including JP Morgan) and newspapers (including the Wall Street Journal).

2. The Ashley Madison infidelity dating website made front page headlines when the data of subscribers – 37 million customer records – was stolen and then published by hackers.
3. Children's technology and toy firm Vtech suspended trading on the Hong Kong stock exchange after admitting a hack that reportedly saw 4.8 million customer details stolen.
4. Carphone Warehouse suffered a cyberattack which put the personal information of 2.4m customers at risk.

It seems no business is safe from a potential hack and heading into Christmas even our kids' toys are not secure. Maybe Santa knows our secrets after all!

The underlying trend, however, is that criminals are increasingly targeting personal information – and human error is continuing to put that information at risk as businesses fail to protect it properly.

The history of the last year suggests not a lot will change in 2016 but there is legislation on the horizon that could prompt change – and a greater public awareness of data protection issues could also drive the agenda.

Here are few predictions as we look ahead to a new year and, just maybe, a new start:

- More people will start to falsify their data and trust organisations less. For example, why give a real date of birth when a made up one will still get you free services?
- Customers will start to question why some apps need access to contact and call details that have no relevance to the app being used. Expect an increase in the number of stories about battery-draining and inappropriate data-collecting apps for all the new shiny phones Santa has delivered for Christmas.
- People will start to realise they are targets for hackers that want to steal data – it's not only 'other people' who are at risk
- The EU General Data Protection Regulation (EU GDPR) will be ratified and it will suddenly dawn on businesses just how much it will affect them – especially when it comes to privacy by design on new projects, protecting themselves against data breaches, reporting data breaches and handling requests from customers to alter or delete data.
- Data processors will suddenly want to change contractual terms as their liability increases for data protection under the EU GDPR – the responsibility having previously been shouldered largely by data controllers.
- Safe Harbor 2.0 – the rushed replacement for the previous agreement which was ruled invalid – will probably be challenged on similar grounds of US surveillance.

- Cloud services will start to shake off their image of vulnerability and by the end of the year cloud will be mainstream. Only the most sensitive information will be stored on premise. IT staff without cloud experience are going to have to get it fast and many will have to re-train. The new mobile cloud-based world will continue to grow throughout 2016.
- Jurisdictional challenges will come to a head in 2016, such as the case of Microsoft having to relinquish Hotmail data stored in Ireland to US authorities. This could have huge implications with the fragmentation of the Internet into trusted zones where data can be kept e.g. within the EU.
- Cloud providers will have to consider geographic locations more than they currently do. Until now, cheap electricity and data connectivity have been their main concerns.

John Culkin, Director of Information Management at Crown Records Management

Read more: <http://www.itproportal.com/2015/12/15/what-did-we-learn-in-records-management-in-2015-and-what-lies-ahead-for-2016/#ixzz3wWyZNRGX>

Submitted by Ruth Edge – Cardinia Shire Council