Does your Board know about GDPR?

Within a lot of organisations the IT department is seen as a function to support the business and seen just as an overhead. The Board is not always that interested in the detail (although some companies like Dominos Pizza and their mobile app show businesses beginning to embrace IT[1]), but the pending General Data Protection Regulation (GDPR) is something that *will* affect all companies and the board level directors need to be aware.

Governments are fed up with the frequency that personal data is being lost or stolen, and organisations like the ICO currently do not have the power to award fines in excess of £1,000,000. For some large global organisations this is a paltry sum and therefore data protection is not high on the agenda. The current draft of GDPR is suggesting €100,000,000 or 5% of annual global turnover whichever is the greater as the fine. This will now mean large organisations will have to take personal data privacy seriously.

Some commentators are suggesting that the above fines will be used for all breaches. Having read many articles, my view is that the fines issued will not necessarily be at the full €100,000,000 / 5% turnover value, especially for small organisations and public sector companies that just won't have these funds. The fines in my view will be issued according to the company sector and size, but GDPR gives the ability to fine up to these much larger numbers for the larger private sector companies.

So failure to conform with GDPR will mean heavy fines for any organisation. However what is GDPR? There are hundreds of pages in this regulation and it is still evolving. The basics are that there must be easier access to personal data, and should an EU citizen request that their personal data is deleted then it MUST be removed from all media including tape backups etc. as long as there is no legitimate grounds to retain the data. Personal data can be anything from name, email address, photo, even an IP address associated to an individual.

This regulation will be a single law for all 28 member states in the EU. One Continent, One Law. GDPR will be applied to any data of an EU citizen held anywhere in the world. Therefore the GDPR will also impact non EU organisations that might hold EU citizen data. They will also have to conform to the regulations and be liable to the same fines if the regulations are breached.

As well as deleting any personal data when requested, the regulation also is designed to make sure that the data is safe and secure. Organisations will need to have 'State of the Art' technologies in place to make sure that there is no data breach. If there is a breach, the regulatory body and the individuals concerned MUST be informed within 24 hours providing detail of the breach, not just that a breach occurred.

The regulation has not been finalised yet, but the belief is that this should happen early 2016. When it is in place companies will have 2 years' grace to put the technologies required in place. That sounds a reasonably long time, but let's face it, do you know where all the instances of personal data are for anyone that might request it to be deleted? When you know where this data is, how will you redact, update or delete the content as required by GDPR including deleting tape and archived content? How will you secure your data and network to prevent data breaches? Remember some of these breaches might not be from careless staff, but from malicious code being left in your environment by viruses and other such threats.

GDPR is coming and will affect all companies. It is time to start thinking about what data discovery tools and data security technologies you will need to invest in.

Andrew Salmon is the IT Director for TrueSwift Ltd.

[1] http://www.independent.co.uk/news/business/news/domino-s-pizza-sales-up-19-thanks-to-mobile-app-a6693761.html

Published: 5th November 2015