THE PANAMA PAPERS "HACK"– A CYBERSECURITY WAKE UP CALL FOR SOUTH AFRICAN LAW FIRMS AND THEIR CLIENTS

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Lucien Pierce | April 26, 2016

The past week has not been a good one for law firms and their much vaunted reputation for client confidentiality. Major law firms across the globe have had to admit that sensitive and confidential client information has been "liberated" as a result of hacking attacks on their information technology (IT) systems.

It was reported in the Wall Street Journal last week, that major US merger and acquisitions firms including Cravath, Swaine & Moore and Weil, Gotshal & Manges had suffered IT system breaches. These law firms must be breathing sighs of relief given that that the spotlight is off them and squarely on Mossack Fonseca, the Panamanian law firm behind the Panama Papers Expose: probably the biggest data breach in history.

For those who have been living under a rock since Sunday 3 April 2016, the Panama Papers is an expose stemming from a leak of 11.5 million documents from Mossack Fonseca. The leak details the offshore holdings of 12 current and former world leaders and the opaque dealings of 128 additional politicians and public officials around the world.

Although there is some debate as to how the leak occurred i.e. whether it was as the result of a whistle-blower or an IT systems hack, Mossack Fonseca have attributed the breach to "a hack on an email server."

Mossack Fonseca, Cravath, Swaine & Moore and Weil, Gotshal & Manges are not the only major law firms to have suffered breaches in recent times. In fact, between 2011 and 2015, 80 of the largest 100 US firms by revenue, suffered a hack. It is not common for law firms to disclose such breaches. More often than not, the breaches come to light because they would have to be reported to comply with applicable legislation or, as in Mossack Fonseca's case, the breach just could not be hidden.

The UK Government publication Cybersecurity Guidance for Business, very succinctly, captures the implications of a data breach for most businesses. In essence, a data breach is likely to lead to "material financial loss through loss of productivity, of intellectual property, reputational damage,

recovery costs, investigation time, regulatory and legal costs. This could lead to reduced competitive advantage, lower market share, impact on profits, adverse media coverage, bankruptcy, or even, where safety-critical systems may be concerned, loss of life.

We can safely say that Mossack Fonseca and some of their clients have, since Sunday, ticked almost all the boxes listed above.

Interestingly, only 10% of South African businesses experienced a data breach during 2015. It would be comforting if such a low statistic could be attributed to extremely high information security standards in South Africa. The reality is more likely that this is because there is no legal requirement to report such breaches…yet.

The Protection of Personal Information Act, 4 of 2013 (POPI) will place an obligation on data processors, such as law firms, to report any breaches involving personal information, to the Information Regulator and to any data subject whose personal information may have been lost, damaged or unlawfully accessed or destroyed.

In addition, for the first time, new rules under the Attorneys' Act deal explicitly with information security by requiring that, insofar as attorneys and their practices are concerned, "all information, in whatever form, that is created, processed, communicated or retained (referred to in these rules collectively as "processed information") shall be processed subject to a degree of information security that is appropriate, having regard to the nature of the information and the purpose for which it is processed."

So, whilst it is possible, but unlikely, that South African law firms will have a trove of 11.5 million documents with riveting stories to tell, they would do well to ensure that the information security systems they have in place are appropriate for the types of information they deal with.

Likewise, law firm clients who are likely to suffer financial and reputational harm as a result of a data breach, would do well to undertake appropriate audits of their law firms' information security systems and obtain as many warranties and indemnities as they can.

Following these tips will go a long way to ensuring that law firms and their clients are not featured in what at some point in the future may become known as the "South Africa Papers".

Lucien Pierce is a partner at PPM Attorneys. He specialises in telecommunications, media and technology law, with a particular focus on information security and data protection. He can be found at ppmattorneys.co.za.