

Cybersecurity

Financial consequences and directors duties

Gordon Owili

Technology has transformed the way business is conducted from providing services online to customers, to storing data in the 'cloud' while accessing information. With advances in internet technology, lawyers must keep abreast of the various legal issues associated with cybersecurity.

According to the 2016 'Australian Government Cybersecurity Strategy', it is estimated that by 2019, the average Australian household will have twenty-four devices connected online. A 2016 study by the Ponem Institute (which comprised a benchmark study of 314 companies

spanning ten countries) estimates that the total cost of a data breach is US\$4m. The Ponem study also found that the cost incurred for each lost or stolen record containing sensitive and confidential information is US\$158 on average. According to an IBM study, small and mid-sized businesses are hit by 62% of all cyber-attacks.¹

The financial consequences of a cybersecurity event – the Yahoo case study

Companies and even the financial markets are becoming more adept in pricing the consequences of breaches that result from a cybersecurity event. Take the Yahoo case as a case in point. In July 2016 Verizon Communications announced plans to acquire Yahoo for US\$4.8b.² The acquisition would, it was reported, create one of the largest technology companies in the world.⁴ In September 2016, Yahoo announced that at least 500 million user account credentials had been stolen from it in late 2014. Yahoo also announced that, at the time, twenty-three lawsuits seeking class action status had been filed against it over the breach. In December 2016 Yahoo disclosed that it had discovered a breach of more than one billion user accounts that occurred in August 2013 (this breach was believed to be separate from the September 2016 data theft).

Cybersecurity

As a result of the data breach, it is likely (and there has been speculation) that Verizon might ask for a \$1b discount on the company.⁴ In fact, after the September data theft, Verizon's general counsel, told reporters that the company has "a reasonable basis" to suspect that Yahoo's massive security breach could have a meaningful financial impact on the deal.⁵

Directors' obligation to discharge their duty with care and diligence

To date there has not been any case(s) of note, at least not in Australia, brought against directors relating to a cybersecurity breach, however, because markets are getting better at quantifying losses associated with a cybersecurity breach it is something we can expect to see a lot more of. One of the duties of directors is the duty of care and diligence. This duty is imposed on directors by, inter alia, s 180(1) of the *Corporations Act 2001* (Cth). If we accept that a cybersecurity threat is a foreseeable risk (the IBM study mentioned above tells us so) then a cybersecurity risk is relevant to the directors duty of care and diligence. It is therefore not inconceivable that directors who fail to consider cybersecurity threats could be found liable for breaching their duty of care and diligence if a cybersecurity event materialises that causes harm to the organisation. Another factually scenario, in which a directors could be found liable, is where they make an affirmative decision regarding cybersecurity that permits a breach, such as, approving the installation of an inadequate cybersecurity system. It is therefore prudent that directors take into account especially those cybersecurity risks deemed material to the operation of their organisations.

Gordon Owili is a Certified Finance and Treasury Professional (CFTP), a Fellow of Finsia (F Fin) and a Senior Associate Certified Insurance Professional (ANZIIF (Snr Assoc) CIP). Gordon has several years' experience in law, finance and risk management. He has worked at EY, BHP Billiton, Honeywell and Veolia. Gordon has an LLB, a BSc (Biomedical Science), a Graduate Diploma of Applied Law (specialising in Commercial Litigation), an MBA (specialising in Finance), a Master of Applied Finance and Investment (specialising in Corporate Finance and Advisory) and a Master of Business Law.



- 1 Gary Miller, 60% of small companies that suffer a cyber attack are out of business within six months, (23 December 2016), The Denver Post <<http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/>>.
- 2 Tom DiChristopher, Verizon to acquire Yahoo in \$4.8 billion deal, (25 July 2016), CNBC, <<http://www.cnbc.com/2016/07/25/verizon-to-acquire-yahoo.html>>.
- 3 Daniel R. Stoller, Cybersecurity Diligence Issues in Verizon-Yahoo Merger, (23 August 2016), Bloomberg BNA <<https://www.bna.com/cybersecurity-diligence-issues-n73014446704/>>.
- 4 Kate Conger, Yahoo discloses hack of 1 billion accounts, (14 December 2016), TechCrunch <<https://techcrunch.com/2016/12/14/yahoo-discloses-hack-of-1-billion-accounts/>>.
- 5 Seth Fiegerma, Verizon says Yahoo's massive breach could impact deal, (13 October 2016), CNN <<http://money.cnn.com/2016/10/13/technology/verizon-yahoo-breach-material/>>.