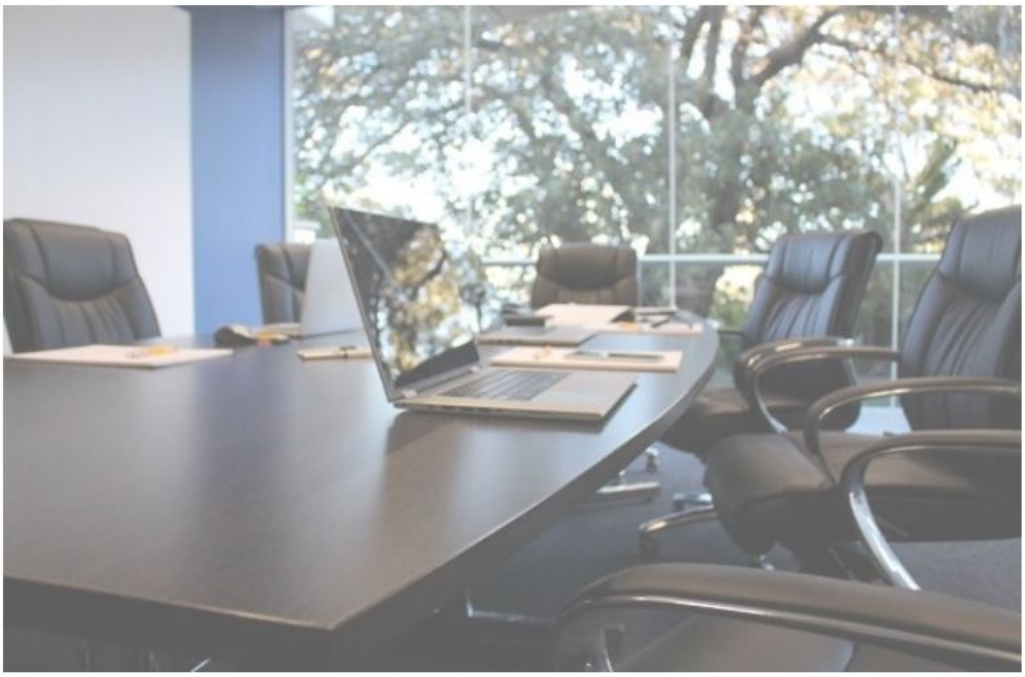
Not just an IT issue – why cybersecurity should be on the board agenda

Annelies Moens | June 20, 2017



In the digital age, every organisation – be it private sector, public sector or not-for-profit – is a 'data business'. Annelies Moens of Information Integrity Solutions Pty Ltd, discusses why directors need to engage on cyber security.

Imagine that accounting standards required organisations to take account of, and value, their data assets. In adding data to the balance sheet, many company directors would be surprised at the data their organisations hold, or that those data assets (which are often collected without payment or at a low cost) are valuable.

In misunderstanding the value of the data they possess, organisations may both ignore the opportunities inherent in those data assets and fail to adequately protect them and open them up to cyber security risks. There is something, however, about the intangibility of data assets that causes organisations to fail to account for their value and protect them adequately. This issue is compounded by the fact that the valuation itself is difficult. Traditional ways of measuring asset value such as 'market value' and 'historical cost' may be a poor fit for measuring the future economic benefits of data holdings.[1]

Failure to fully understand the value of data may lead boards to allocate data management and oversight to IT personnel thereby missing the important role the board itself has to play in the strategic management of this asset. One of the key factors that distinguish more cyber-resilient organisations from less resilient ones is that cyber security is regularly discussed at the most senior board or management level.[2]

And yet, we are in an age where data has never been so valuable, nor the opportunities for innovation so great, and the risks of data breach and cyber incidents so high. The arrival of new business models – such as ride-sharing, homestay accommodation and GPS-enabled fitness apps – and the expansion of existing goods and services – to include, for example, real-time tracking of delivery or arrival times, integration with mapping and location-based technologies, monitoring and optimisation of product performance via sensors and the internet of things and the tailoring of products and services to user preferences – are evidence of the wealth of opportunities that await businesses willing and able to use and protect their data assets effectively. Cyber security and privacy are unavoidable considerations.

All too often, it is weak or non-existent governance of data that garners attention. And indeed, when things go wrong, the impact on company directors themselves is brought into sharp focus. A serious data breach sustained by Target in late 2013 resulted in the resignation of Target's CEO and CIO – it was reportedly the first time the head of a Fortune 500 company was ousted due to a cyberattack.[3] Target has also recently settled class actions totalling $25 million.[4] There is also the risk that a cyber security incident will significantly affect business and shareholder value (or even result in the closure of a business)[5].

However, when organisations effectively address and mitigate cyber security and privacy risks through strong governance processes, wider opportunities can be grasped. Relegating cyber security to IT personnel is to fail to fully comprehend the strategic value of data and places organisations at a disadvantage when navigating strategic business decisions involving data.

This blog is based on an article first published in the March 2017 issue of Governance Directions, the official journal of Governance Institute of Australia.

[1] Juergen Sidgman and Malcolm Crompton, 'Valuing Personal Data to Foster Privacy: A Thought Experiment and Opportunities for Research' *Journal of Information Systems*: Summer 2016, Vol. 30, No. 2, pp. 169-181, 2016.

[2] Australian Government, Australian Cyber Security Centre, 2016 Cyber Security Survey p.16

[3] Kevin Lonergan, 'Don't let a data breach destroy you: a history lesson', *Information Age,* 14 September 2014.

[4] Patricia Hurtado, 'US retail giant paying almost $25 million to end data breach probes', *Sydney Morning Herald,* 24 May 2017.

[5] See for example, 'Case study: When a hacker destroys your business', *CIO*, 3 March 2015; see also 'Verizon wants $1B discount on Yahoo deal after reports of hacking, spying', *New York Post,* 6 October 2016