Information Security & Privacy – It’s not my bag baby, or is it?

I am imagining a time in the not too distant future (actually it’s here already) where post security breach board meetings play out like a scene from an Austin (Danger) Powers movie. It’s the one where upon discovery of an embarrassing Swedish implement, Austin’s embarrassment is amplified when piece by piece the evidence of personal ownership is revealed, first the receipt, then the warranty card completed in his own hand writing and finally the book he authored which clearly states it is ‘my bag baby’.

Now imagine being a board member or senior leader of an organisation after an information security breach – often what emerges is an embarrassing picture where piece by piece it becomes evident that on his or her watch, there was a poor understanding of the information risk and they had failed to ensure adequate technical and organisational measures existed to protected data.

Beyond the embarrassment, imagine the impact on the organisation if the post breach assessments show there was little demonstrable evidence of information security governance and that data privacy and security didn’t feature in the organisations priorities.

All pretty worrying for a leader in today’s climate where they are most likely expected to fall on their sword, or in the case of larger organisations, publicly demonstrate their remorse or management failings.

Unlike, the Austin Powers scenario, I do not believe business leaders naturally shy away from the embarrassment or accountability after a breach, however I wonder how many leaders have truly grasped the thorny nettle rather than simply assumed IT has it covered because ‘it’s an IT Thing’ .

So, here is an important message, information security cannot just be an ‘IT Thing’ because a failure to manage it can affect your organisations customers and employees lives, destroy careers, hit share prices, bring organisations to a halt and destroy in minutes reputations that have taken years to build. Because of these risks, information security needs to be a ‘business thing’ that is driven through the organisation by the board in a way that touches every department and every employee – in short, it needs to be a culture so achievement of the organisations objectives are not constrained by the risks it is exposed to in the data it stores, processes or transmits.

It really is the boards ‘bag baby’

So what are the right questions for the board?, Here are a just few to get you thinking.

As a member of the board, how many of these questions could you answer yes to

- I understand what sensitive data the organisation stores, processes or transmits
- I understand how the data is regulated and whether it is lawfully processed
- I understand who would want to get to it and why
- I understand the risks associated with its loss, exposure or corruption (personal, regulatory, operational and financial)
- I understand who it is shared with
- I am confident it is adequately protected
- I am confident that as the business changes, processes will ensure the data remains secure or private
- I have a clear understanding of how the organisation will respond to and manage an incident to limit the impact.

Understanding the data and associated risks is often an early step in knowing how to manage information security and privacy – An information security risk assessment is a great starting place as it will answer many of the questions for the board, but if completed properly will help an organisation understand which of the risks they should care about most (relevant to the risk and the organisations appetite for the risk) and how to prioritise their spend and efforts to the greatest effect and in what time and order. Once you know your risk it becomes easy to make decisions about how to treat the it and best allocate your resources. Once you’ve got the right destination in mind, the job of implementing security and privacy becomes much easier. Maintaining your position moving forward is a whole new conversation, and the subject of a later article.

Want to understand more about information and cyber risk? Get in touch at acompton@cortida.com

+44 (0) 207 164 669
info@cortida.com
www.cortida.com
150 Minories, London, EC3N 1LS