Why Information Security Risk Assessment is a good idea

Long ago at the beginning of my career an enlightened manager explained to me that “if you can’t measure it, you can’t manage it”. This lesson has stuck with me over the years and been proved right time and again in operations, projects and risk management that I have been involved with.

This goes to the heart of operational risk management as it relates to information security within businesses. If you haven’t identified, analysed and prioritised data loss risks within your organisation you can’t effectively manage the total risk to the business. You will have no idea of which risks are most likely to materialise, and therefore where resources should be concentrated for maximum impact. Failure to carry out a risk assessment and develop an action plan leads to a tactical approach to risk management resulting in piecemeal solutions that are often expensive and don’t generate real risk reduction for the organisation.

The Information Commissioner (ICO) was granted increased powers in April 2010 to impose monetary penalties of up to £500,000 for serious contravention of the principles of the data protection act. Within their own documentation the ICO cites “failure to carry out any risk assessment” as one key factor making a monetary penalty more likely in the event of a data loss, on the basis that that the data controller “knew or ought to have known” that there was a risk of the incident occurring.

A common misconception is that information security risk relates only to information technology. In actual fact there are many areas where risk needs to be considered such as Governance, Physical Security, Disposal, Employee Controls and Third party contracts. Conducting a full risk assessment across these areas builds a strategic approach and helps develop a culture of information security within the business thus making a data loss incident less likely. If a data loss does occur the ability to show that a risk based approach has been taken and that actions are prioritised and planned is a much better position from a regulatory perspective than one where there is no evidence of any attempt to manage risk effectively.

An established risk assessment methodology provides a structure within which standards can be applied resulting in a consistent treatment of risk across the business. This structure leads to an objective categorisation of risk which is vital to understanding the priority of the actions that need to be undertaken to reduce it. Many organisations also value an independent external view such as that provided by us as this allows impartial assessment of measures in place and facilitates benchmarking and recommendations based on broad experience of information security risks across many organisations.