



Using Behavioural Science to help understand Technology Adoption Risk Perception

by Jim Sailor

It is rare that a week goes by without a major news story about technological innovations that are changing the business world. It is also rare that a week goes by without hearing a story about companies or governments suffering from massive breaches in cybersecurity. As advances in technologies such as artificial intelligence, big data, cloud computing, and many others continue to surge forward, Chief Information Officers (CIOs) are faced with balancing the potential benefits of adopting game-changing tech with the possible catastrophic risks that come with a hyper-connected and digital world.

Today's fast-changing technology risk landscape is tricky to navigate and has led to challenges for traditional IT risk assessment tools which typically utilise rational analytic calculation based on historical data and past experience. With new technologies, because there is a lack of existing data and evidence to use as a basis for quantitative risk assessment, much of the judgement of risk is inherently perceptual and susceptible to bias. As such, there is increasing recognition that there are limits to the purely rational approach and a growing interest in applying behavioural science in understanding technology adoption and management to provide a more comprehensive view of risk.

I conducted research for my dissertation, 'New Technology Risks – Professional Perceptions in Malaysia', with the hope of contributing to the nascent body of work on understanding behavioural risk perception in the adoption of technology. I did this by building and piloting an exploratory model for measuring and analysing risk perceptions of eight emerging technologies. The

theoretical basis for the model was developed from Slovic and Fischhoff's 'psychometric paradigm' and customised to be relevant for the field of technology adoption. The psychometric paradigm is a well-established psychological measurement tool that challenges the notion that people perceive risk in a fully rational way and helps to explain biases such as availability and affect.

Working with the National ICT Association of Malaysia, I surveyed one hundred business executives in Malaysia with the sample split between IT 'experts' (CIOs and others in technology management) and 'non-experts' (from other management roles). The sample was structured this way to reflect recent industry trends toward decentralization of technology procurement; where previously almost all purchase decisions were made by technology specialists such as CIOs, the pervasiveness of technology applications has brought others into the equation. Marketing, finance, human resources, and others now have advanced technology solutions specifically geared to their areas of responsibility and are therefore increasingly involved in judging technology benefits and risks.

In addition to mapping out the eight technologies' risk and benefit profiles, the research uncovered some interesting results including the following two points.

Conflation of risk probability with severity of damage – For seven out of the eight technologies measured and most clearly for mobile devices, big data, and artificial intelligence, if respondents felt that a technology has more potential for severe damage, then that technology was often also rated higher on the probability of an incident occurring. In reality, major incidents that do major damage such as full-scale hacker attacks or massive losses of data occur only rarely while relatively low-damage incidents such as work delays from temporarily crashed systems would be much more likely to happen. This aggregation of probability and severity is in line with other psychometric paradigm research where dread risk perceptions (such as for terrorism or nuclear power) are often correlated with increased beliefs about the likelihood of a risk incident – suggesting what Cass Sunstein calls 'probability neglect'.

Non-expert susceptibility to availability bias – Within the study I attempted to trigger availability bias by priming a randomly selected set of respondents with a statement regarding the risk of adopting new technology and then assessing whether this would affect their risk judgements. While experts showed no significant differences between treatment and control groups, non-experts showed significant treatment effects on perceptions of riskiness for three of the tested technologies. This finding suggests that non-experts were more susceptible to the availability priming and agrees with other risk research that has found that non-expert risk perception is more prone to bias while experts tend to be more stable in their perceptions.

Technology investments are often costly and risky, but also have the potential to transform business strategies and results. Overall, the study helped to cast some light on how businesspeople perceive the risks and benefits of new technologies and showed that potential biases should not be ignored. A better path forward may be to rethink how risks are being assessed and to foster an environment of clear risk communication and education among expert and non-expert business leaders. There is no doubt that CIOs and other leaders will continue to face difficult choices when it comes to tech adoption and hopefully they will benefit from better understanding and using behavioural science in informing the decisions they make.

This blog post was written by Jim Sailor as a summary of the research undertaken for his dissertation as part of the Executive MSc in Behavioural Science at LSE, 2015-16. Jim is currently based in Kuala Lumpur, Malaysia and provides consulting and advisory services across Asia. Follow him on linkedin <https://www.linkedin.com/in/jimsailor>

Comments are closed.