The Psychology of Decision-Making and Risk

by John Laskey & M. E. Kabay, PhD, CISSP-ISSMP

The following article is a contribution from John Laskey. Everything that follows is entirely John's work with minor edits from Mich.

Good risk management is fundamental to the security profession. When risks are overlooked or underplayed they can have a direct impact on a business and its reputation. When risks are overplayed, security becomes an inhibitor to productivity and challenges our credibility as professionals. And whenever security is seen as unnecessary, wasteful or uncompetitive then the stock of all security professionals goes down.

Sophisticated tools have been developed to assess security risks. The complexity and responsiveness of these tools require good levels of trust and understanding between security professionals – who understand the risk – and senior executives – who own the assets at risk. So if we wrap up the tools, the experts and the executives inside a good governance structure then we ought to get good security. But there's something missing.

A few years back I sat in a theatre of over 200 senior government security managers and professionals on a three day seminar. One session was different: it was about psychology. The speaker emphasised how the decisions we make about security were influenced by personal perception rather than real likelihood.

To illustrate this he gave the audience a hand-out describing a risk-related problem. Those on the right were given a version described in terms of the savings involved in the situation while those on the left were given the same information but described in terms of the losses involved. From a risk analysis standpoint both versions were identical, only the way the information was being presented was different. However, this seemingly trivial difference in wording radically changed risk attitudes. When asked to choose which of two actions to take those on the right (given the saving version) strongly preferred the safe option while those on the left (given the loss version) strongly preferred the risky option. It was a revelation. Unwittingly we experts had shown how our powers of decision-making and our attitudes to risk were influenced by how information is presented. The speaker showed how a range of other psychological factors can affect how we perceive and act in the face of risk.

The speaker was John Maule< http://business.leeds.ac.uk/about-us/faculty-staff/member/profile/john-maule/ >, who is Emeritus Professor of Human Decision-Making at Leeds University Business School, England. Maule has been active in heightening public awareness about the limitations to the intuitive judgement of risk. To this end he has submitted written evidence to a Select Committee of UK Lawmakers on Economic Affairs< http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeconaf/183/183we19.htm >. He argued for greater awareness of the often personal, emotional responses that can shape and drive law-making. Maule has also highlighted the role of personal perception in response to fears of terrorism. In the aftermath of the 2005 Al-Qaida inspired bomb attacks on London's transportation system in which over 50 people were killed and over 700 injured, the BBC noted that many more London commuters were now choosing to walk or cycle. Maule argued that this was because such methods gave commuters the feeling of being more in control, not because it actually made them safer. For a generalised comparison, UK government figures for 2005< UK government figures for 2005 < http://webarchive.nationalarchives.gov.uk/%2B/http%3A/www.dft.gov.uk/adobepdf/162469/221412/221549/227755/roadcasualtiesgreatbritain2005a >show 372 pedal cyclists and 1224 pedestrians were killed or seriously injured in accidents in the greater London area (Table 46a, page 116 in text). No such figures were cited by Maule, but he held that graphic media coverage< http://www.guardian.co.uk/flash/page/0%2C%2C1808096%2C00.html > of the attacks had lodged in the minds of London commuters, making them feel that travelling on the subway was much riskier than it really was. This led them to take action that actually *increased* rather than decreased their exposure to risk.

Maule also holds an interesting view on group involvement in decision-making. In a published response < http://www.independent.co.uk/opinion/letters/letters-the-hs2-project-2053404.html > to a particular theory ("Nudge theory is only short term") he argued that "…when people are actively involved in making a decision they are more committed to it and will stick to it longer, even when the outcomes are not as good as expected." This observation should reassure those of us who worry whether senior executives have the time or inclination to grasp the more complex points of our art.

This analysis of human risk perception might paint a rather bleak picture. After all, we must use complex risk assessment tools that are the domain of experts. Then we have to put our conclusions into language that non-experts with high degrees of responsibility can grasp. And now Professor Maule tells us that we also need to think much more about the way we draw our conclusions on risks. Indeed, in a recent book (*Decision Behaviour, Analysis and Support< http://www.amazon.com/Decision-Behaviour-Analysis-Support-French/dp/0521709784/* >) Maule and his co-authors (Simon French and Nadia Papamichail) describe a range of techniques for improving thinking in risk situations. Though we know that security management can work and that our security experts do their jobs well and in the interests of the business, there are lessons for all of us in Maule's work.

I think we just need to take a little more time to ask ourselves whether we are worrying about the right things and reacting to them in a proportionate and timely way. In addition, we need to reflect more on how we are thinking and to develop our understanding beyond our first thoughts and impressions.

* * *

John G Laskey< http://www.linkedin.com/pub/john-laskey/28/b28/b69 > is a British security consultant who has worked for the UK government in national security and emergency response since 1986. As IT Security Officer for the Home Office he was responsible for the security risk management of a number of high profile systems developed to increase government and public security. John is a founder of and assessor for the UK government Infosec Training Paths and Competencies (ITPC)< https://www.instisp.org/SSLPage.aspx?pid=422 > scheme from the Institute of Information Security Professionals< http://www.instisp.org > that formally certifies those working in UK government information security projects. In addition to his experience in project security and security awareness, John has advised senior government managers on the health of major projects and programmes and he is a certified lead auditor for the ISO 27001 security standard. He is also a member of BCS, the Chartered Institute for IT< http://www.bcs.org/ > and of the Security Institute< http://www.security-institute.org/ >.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *