Workplace autopilot threatens security risk perception

February 8 2008

Safeguarding sensitive information - no matter how sophisticated the IT system - can never be foolproof, according to research published this week by Leeds University Business School.

The loss of a CD by HM Revenue & Customs in November 2007 containing personal and financial details of over 7 million families claiming child benefit was swiftly followed by assurances that such a mistake would never happen again. Earlier this week, an agency of the Department for Health admitted that over 4,000 NHS smartcards, giving potential computer access to patient records, had been lost or stolen - and nearly a third of these in the last year alone.

But no matter what steps an organisation takes, they will always run the risk of being compromised by human psychology and the way we perceive risk on a day-to-day basis, says Professor Gerard Hodgkinson, Director of the Centre for Organisational Strategy, Learning and Change (COSLAC).

“Our research shows that organisations will never be able to remove all latent risks in the protection and security of data held on IT systems, because our brains are wired to work on automatic pilot in everyday life,” he says.

“People tend to conceptualise the world around them in a simplified way. If we considered and analysed the risks involved in every permutation of every situation, we’d never get anything done! If I make a

cup of tea, I don't stop to weigh up the probability of spilling boiling water on myself or choking on the drink."

Survey participants, all of whom regularly used IT systems in the course of their work, were asked to list examples of possible data security risks, either imagined or from their own personal experiences. A further group were asked to comment on the probability, underlying causes and likely consequences and impacts of the most commonly described scenarios.

Despite the survey data being collected over a period of two years, many of the risk examples envisaged by the study participants ironically matched – with surprising accuracy - some of the recent security lapses relating to information technology.

Says co-author Dr Robert Coles, "The results showed that when asked to focus on potential problems, employees seemingly exhibit a highly sophisticated perception and categorisation of risk, and insight as to the consequences of risky scenarios. However, this perception isn't always translated into practice and elementary errors are still happening - and will continue to happen."

The authors say that the results are useful for highlighting blind spots in what workers perceive as risk and probability, which will enable organisations to improve their induction and training processes.

The research also highlights the need to pay closer attention to the design of information security processes themselves. "Perhaps organisations should consider involving the potential users when developing crucial business processes," says Dr Coles. "A well designed system should not allow these mistakes to be made. We need more triggers and mechanisms in the workplace that make us stop and think before we act."

Source: University of Leeds