Young, impulsive, IT savvy = greater cybersecurity risk

November 17 2015

Researchers from the University of Adelaide say Australian businesses should start to think outside the square when it comes to preventing cybersecurity threats in the workplace – such as profiling their staff's computer behaviour.

The suggestion follows latest research that has detailed the range of human behaviours associated with increased cybersecurity risks for companies.

The work, conducted by the Human Aspects of Cyber Security (HACS) research group in the University's Business School, has helped to better understand the individual factors that lead to higher security risks.

"Information security professionals have been attempting to convince senior management for many years that humans represent a major risk to the security of their computer systems," says Dr Malcolm Pattinson, Research Fellow in the Business School.

"All it takes is for one employee to click on the wrong link or open the wrong attachment in an email and the organisation can have a major cybersecurity breach, resulting in stolen information, damage to data, significant work downtime, and loss of revenue."

Dr Pattinson and colleagues have developed tests that can help determine the level of cybersecurity awareness among workers. They've outlined the specific factors that play a role in this, including: an employee's age,

education level, ability to control impulses, familiarity with computers, and the worker's personality type.

"This kind of 'cybersecurity profiling' could be very useful in helping an organisation to identify the level of human risk within their workplace, and in adopting processes and strategies to overcome it," he says.

"For example, we know that people who are impulsive often make mistakes. Accidental, naïve behaviour leads to cybersecurity risk. Age is a factor – the younger you are, the more vulnerable you're likely to be.

"Interestingly, people who have less understanding of how computers work may be less at risk because they're often more cautious. Those who think they know it all will tend to be more self-assured, and that's when they can make a serious mistake by clicking on the wrong email link or not noticing that attack software has been installed on their computer."

Dr Pattinson says information security culture comes from the top of an organisation down. "The more managers start to pay attention to these issues, the better that company-wide culture will be," he says.

Provided by University of Adelaide