Humans are largely the problem in cyber security failures

October 31 2014, by Robyn Mills

When people think about cyber and information security they often think about anti-virus software and firewalls; however, according to an information security expert from the University of Adelaide, organisations would become a lot more secure if employers invested in more security-related training for staff.

Dr Malcolm Pattison says until recently, research into information security (electronic and physical data security) focused on computers, software, data communications and policies, and while these are important, the human aspect was largely overlooked.

"While high-quality hardware and software plays a critical role in the security of an organisation, there is now a growing body of research that suggests the behaviours of computer users can be one of the biggest threats to an organisation's information security," says Dr Pattinson, a research fellow in the University of Adelaide's Business School.

"For example, the best password processed by the most sophisticated software, using the latest in computer facilities becomes useless when the password is written on a sticky note and stuck on a monitor for easy access.

"Humans are a major problem. What we think, what we know, what we do, how we do it and why we do it are perhaps the key to attaining and maintaining an acceptable level of information and cyber security in an organisation," he says.

Dr Pattinson says security breaches don't just happen at computers - staff also need to be conscious of storage and disposal of physical documents.

"Information security usually refers to digital data security; however, it also refers to physical data security," Dr Pattinson says.

"Many organisations provide secure bins for confidential documents to be shredded but it's still up to individuals to dispose of material correctly."

Dr Pattinson says the good news is that staff training can be a lot more affordable than purchasing the latest hardware and software, and there are a few key behavioural changes that would make an organisation considerably more secure.

"Training could be facilitated in a cost-effective manner," he says. "Better knowledge about the policies and procedures surrounding information security will positively influence people's attitudes and in turn, improve their behaviour.

"Small changes like locking a computer when someone leaves their desk; not using public wifi on work computers and mobile devices; keeping passwords secret; correctly disposing of documents; and reporting any unidentifiable visitors can lead to a safer workplace," he says.

Dr Pattinson is a member of the Human Aspects of Cyber Security research group, which is a collaboration between the University of Adelaide's Business School and the Defence, Science & Technology Organisation (DSTO).

Provided by University of Adelaide