Email traffic gives clues to workplace threats

July 23 2013

Employees carrying out an insider attack at work can be identified from the language they use in emails according to Lancaster psychologists.

These attacks include everything from workplace theft to fraud, hacking and sabotage, resulting in the loss of millions of pounds to companies.

The study found that an analysis of the email language of employees within an office environment managed to identify 80 to 90 per cent of those actively stealing confidential information and passing it to a provocateur.

Their analysis found that the attackers were much more self-focused, using words like "me", "my" and "I" and they used more negative language compared with typical co-workers.

They also found that employees conducting an insider attack reduced the extent to which they mimicked the language of their co-workers. This reduction in mimicry, which suggests an inadvertent social distancing by the attackers, increased over time, such that by the end of simulation, it was possible for the researchers to use the combined metrics to identify 92.6% of insiders.

Researchers led by Professor Paul Taylor at Lancaster University created a six hour workplace simulation similar to a police investigation into organised crime.

The 54 participants were divided into different teams who had to work

together to gather and share information on "suspects".

One in four of the participants was asked to become an "insider" by covertly obtaining information without the knowledge of the others and passing it to a third party.

The researchers then examined the emails that participants sent to one another as part of their workplace simulation, looking for known indicators of emotion and social cohesion.

Professor Taylor said: "The act of conducting an insider attack carries with it cognitive and social challenges that may affect an offender's day-to-day work behavior. Our analysis looked for these changes in the email traffic of an organisation, and found subtle but distinctive ways in which insiders' emails differed from their co-workers."

The researchers concluded that: "Our findings demonstrate how language can provide an indirect way of identifying people who are undertaking an insider attack."

The research "Detecting insider threats through language change" is published in the journal *Law and Human Behavior* published by the American Psychological Association.

More information: psycnet.apa.org/psycinfo/2013-20282-001/

Provided by Lancaster University