Researchers test brain activity to identify cybersecurity threats

April 22 2015

Iowa State researchers measured brain activity to better understand cybersecurity threats and identify what motivates employees to violate company policy. Credit: Bob Elbert

The old adage that a chain is only as strong as its weakest link certainly applies to the risk organizations face in defending against cybersecurity

threats. Employees pose a danger that can be just as damaging as a hacker.

Iowa State University researchers are working to better understand these internal threats by getting inside the minds of employees who put their company at risk. To do that, they measured brain activity to identify what might motivate an employee to violate company policy and sell or trade sensitive information. The study found that self-control is a significant factor.

Researchers defined a security violation as any unauthorized access to confidential data, which could include copying, transferring or selling that information to a third party for personal gains. In the study, published in the *Journal of Management Information Systems*, Qing Hu, Union Pacific Professor in Information Systems, and his colleagues found that people with low self-control spent less time considering the consequences of major security violations.

"What we can tell from this current study is that there are differences. The low self-control people and the high self-control people have different brain reactions when they are looking at security scenarios," Hu said. "If employees have low self-control to start with, they might be more tempted to commit a security violation, if the situation presents itself."

The study, a first of its kind, used EEG to measure brain activity and examines how people would react in a series of security scenarios. Researchers found people with high self-control took longer to contemplate high-risk situations. Instead of seeing opportunity, or instant reward, it's possible they thought about how their actions might damage their career or lead to possible criminal charges, Hu said.

For the study, researchers surveyed 350 undergraduate students to

identify those with high and low self-control. A total of 40 students – from both the high and low ends of the spectrum – were then asked to do further testing in the Neuroscience Research Lab at ISU's College of Business. They were given a series of security scenarios, ranging from minor to major violations, and had to decide how to respond while researchers measured their brain activity. Robert West, a professor of psychology, analyzed the results.

"When people are deliberating these decisions, we see activity in the prefrontal cortex that is related to risky decision making, working memory and evaluation of reward versus punishment," West said. "People with low self-control were faster to make decisions for the major violation scenarios. It really seems like they were not thinking about it as much."

The findings reflect characteristics of self-control in criminology, in which individuals with low self-control act impulsively and make riskier decisions. However, with traditional research methods and techniques, researchers could not determine if the low self-control group was more likely to act based on immediate gain, without considering the long-term loss, as compared to the high self-control group.

It's possible that social desirability bias, or the tendency to act in way that is viewed as desirable, masked the true intentions of participants. With neuroscience methods and techniques, the results are more reliable and provide a better understanding of human decision making in various circumstances, researchers said.

What does this mean for business?

The number of security violations grew to nearly 43 million last year, up from almost 29 million in 2013, according to The Global State of Information Security Survey 2015. The survey found employees, current

and former, were the top-cited offender. Not all employee security breaches were malicious or intentional, but those that were created significant risk to organizations around the world. This highlights the need for organizations to focus internally to protect sensitive information.

Laura Smarandescu, an assistant professor of marketing, has used psychological methods in prior studies to gain a better understanding of an individual's thought process. She says this study could help businesses determine which employees should have access to sensitive information.

"A questionnaire measuring impulsivity for individuals in critical positions may be one of the screening mechanisms businesses could use," Smarandescu said.

Other studies on human behavior recommend implementing comprehensive policies and procedures, training for employees and clear, swift sanctions against security misconduct to deter future violations. However, in regard to low self-control, traditional training may not cut it, Hu said.

"Training is good, but it may not be as effective as believed. If self-control is part of the brain structure, that means once you've developed certain characteristics, it's very difficult to change," Hu said.

More information: "The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective" *Journal of Management Information Systems*. jmis-web.org/articles/1222

Provided by Iowa State University