Cranky employees more likely to violate cybersecurity policies

January 25 2018

University of Delaware's John D'Arcy (above) worked with City University of Hong Kong's Paul Benjamin Lowry to survey professionals in organizations throughout the United States. Credit: University of Delaware

As professionals return to work after holidays, their moods are undoubtedly affected by the emotional impact of their holiday experiences, but these moods may be more critical to workplace cybersecurity than previously realized.

New research from the University of Delaware's John D'Arcy, forthcoming in the *Information Systems Journal*, suggests that people's positive or negative moods can affect the likelihood that they will engage in insecure computing behavior in the workplace.

Insecure workplace computing behavior includes things like using weak passwords, accessing unapproved software or not using two-factor authentication, explained D'Arcy, an associate professor at UD's Alfred Lerner College of Business and Economics.

Most organizations have formal policies that prohibit such behavior. To try and predict why people violate these policies, D'Arcy worked with City University of Hong Kong's Paul Benjamin Lowry to survey professionals in organizations throughout the United States about their workplace computing behavior.

The longitudinal survey found that "moods and emotions influence people's security-related behavior," D'Arcy said. "And these things vary from day to day, which can make people's behavior vary from day to day."

According to the survey, employees in better moods are more likely to have a positive attitude about security and are more likely to follow policy.

"On the flip side, if they're in a bad mood, what you get can change from day to day," D'Arcy said. "That makes it more likely that they will violate policy."

This makes sense for any employee who has felt especially inconvenienced by workplace security measures during a bad day: On a day that you were feeling more positive emotions, the extra effort likely wouldn't seem as annoying.

The team focused on insider security breaches because such threats are "a big deal," D'Arcy said, with industry research suggesting that as much as 80-90 percent of all security breaches are caused by noncompliant employee behaviors.

"That's how malware gets on the system," he said. "That's how companies get data breaches."

This study was especially unique, D'Arcy explained, because most previous studies on this topic have examined characteristics of employees that remain stable, like personality traits, instead of something that changes each day.

"It's transient," he said. "You can't just say 'Well, this person's more likely to follow policies all the time.' There's always been this assumption that some people are predisposed toward this behavior or some people aren't, whereas we can see now that based on these mood changes it's hard to predict."

The team also examined what might cause some of these mood changes in the workplace, and ironically, sometimes the cause of the employees' bad moods was the security policy itself. The research team calls this a security policy "backfiring."

"Sometimes if they're dealing with security requirements that they think are too restrictive or are a hassle, that can have a negative impact," D'Arcy said. "It's like too much security puts employees in a negative mood, which then again makes them less likely to follow policy."

This research suggests that employee moods and emotions could be critical new factors for IT and security professionals to consider when pinpointing the causes of security breaches and preventing insecure computing behavior.

In addition to considering the technical aspects of security, D'Arcy said, "You also have to think some more about these people issues, to begin understanding your employees and creating an environment where the security policies are not so restrictive where they're putting people in bad moods."

"The technical stuff still matters," he said, "but so does this."

More information: John D'Arcy et al. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study, *Information Systems Journal* (2017). DOI: 10.1111/isj.12173

Provided by University of Delaware