A return to the office could be bad for computer security

May 25 2022, by Kevin Manne

Credit: Pixabay/CC0 Public Domain

When employees feel they deserve superior technology compared to other employees—and they don't receive unrestricted access to it—they pose a security risk to their companies, according to a new University at Buffalo School of Management study.

Forthcoming in *MIS Quarterly*, the research explores "technological entitlement," a feeling some employees have that they are more deserving of high-tech resources, uses and privileges than their co-workers.

"When these exaggerated expectations of special status go unmet, entitled employees lash out in aggressive acts of misuse or abuse," says the study's lead author Laura Amo, Ph.D., assistant professor of management science and systems in the UB School of Management. "They have fewer qualms about breaking the rules because they consider themselves 'above' organizational restrictions on technology."

The researchers conducted three studies with independent samples totaling nearly 700 working adults. In the first study, they measured past computer abuse behavior and perceptions of restrictions on broad technology use. In the second and third studies, they modeled computer abuse intent by investigating restrictions on remote access and on personal- and company-owned technology at work.

Their findings show that technologically entitled employees pose a direct threat to the information security of organizations.

"If an average-sized company experienced a 10% increase in technologically entitled employees, it'd have to spend an extra $90,000 each year to mitigate that risk," says James Lemoine, Ph.D., associate professor of organization and human resources in the UB School of Management. "Proactive measures—such as user behavior analytics and employee training and awareness—can provide significant savings by reducing cyber risk."

Their findings also have implications for creating and implementing policy on employee technology use, and recommend involving technologically entitled employees in the process of policy-building to encourage buy-in.

"Organizations that work toward establishing fair policies will better mitigate security risks," says Emily Grijalva, Ph.D., associate professor of organization and human resources in the UB School of Management.

Tech entitlement also has implications for employees returning to the office—or being heavily monitored while working remotely—following the COVID-19 pandemic.

"These trends may be perceived as restrictions imposed by the organization, which could increase the security risk posed by technologically entitled employees," says Grijalva. "Businesses should carefully consider employee perceptions when deciding how to move forward with disabling or downgrading remote work options and implementing restrictions on remote workers."

Provided by University at Buffalo

Citation: A return to the office could be bad for computer security (2022, May 25) retrieved 25 April 2024 from https://techxplore.com/news/2022-05-office-bad.html