Remote workers are more aware of cybersecurity risks than in-office employees: New study

September 26 2023, by Joseph K. Nwankpa and Pratim Milton Datta

Credit: Pixabay/CC0 Public Domain

Workers who telecommute tend to be more aware of cybersecurity threats than those who spend most of their time in a physical office and are more likely to take action to ward them off, according to our new peer-reviewed study.

Our findings are based on Amazon Mechanical Turk survey data collected from 203 participants who recently switched to full-time remote work, as well as from 147 in-office workers, across multiple organizations within the United States. We didn't collect data on hybrid workers.

We asked employees the same series of questions about their work arrangements as well as their understanding of cybersecurity threats, and the actions they've taken to defend against them.

To account for other factors likely to influence how an employee responds to perceived cybersecurity threats and risks, we controlled for key participant characteristics and various factors, including age, gender, industry type, company size, job position and the duration of remote work. In addition, we tried to ensure the robustness of our data by conferring with other experts and using various statistical techniques.

We found that remote workers, on average, were more mindful of cybersecurity threats and could better recognize safe cybersecurity practices and protection measures compared with office-based employees. Similarly, our data showed that remote workers were more likely to take cybersecurity precautionary measures than their in-office counterparts.

Why might this be the case?

When employees work from the office, they generally expect their organization to provide and deploy security countermeasures to deal with cyber threats and risks. As a result, in-office workers may become complacent about cybersecurity awareness. This could account for in-office workers taking fewer steps to shore up their cybersecurity.

In contrast, the lack of an institutional cybersecurity framework forces

remote workers to become more mindful of the risks they may be exposed to.

Employees are the first line of defense against cybersecurity attacks, which have been on the rise. Cyber attacks around the world increased 38% in 2022, according to Check Point Research, which provides cyber threat intelligence.

And one of the main ways hackers manage to worm their way into corporate computer networks is via employees—for example, with a phishing email.

During the early days of the COVID-19 pandemic when much of the workforce was sent home due to lockdowns, cybersecurity was a big concern. In cybersecurity jargon, it increased the "attack surface," or the sum of all ways an organization's network is exposed to potential security risks. Companies worried whether employees working remotely would take cybersecurity seriously.

With remote work becoming increasingly the norm for many companies, our research suggests that this risk isn't as great as once feared.

We still need to determine whether heightened cybersecurity awareness and precautionary behavior among remote workers will diminish over time. Research suggests that cybersecurity awareness acquired through training and knowledge programs tends to dissipate over time.

As remote working arrangements become more mainstream, does security complacency set in for these workers? It is important to know how long the increased cybersecurity awareness will enable precaution-taking behavior and how remote workers can renew and sustain this vigilance.