Fear can inspire remote workers to protect IT resources

January 11 2023

Credit: Unsplash/CC0 Public Domain

Fear of what could go wrong is the greatest motivator when it comes to getting remote workers to protect their employer's information technology security, according to a recent study in *Computers & Security*.

But it tends to work best when employees also have a solid understanding of the severity of potential security threats, including the knowledge of what to do when the worst happens.

As millions of Americans continue to work remotely, the research provides employers with key insights to keep their valuable information safe.

"Employees need to feel this is a big deal if it happens, so the number one thing employers can do is to clearly communicate what the threats are and how serious they could be," said Robert Crossler, corresponding author for the study and associate professor in the Carson College of Business at Washington State University. "Because for most people this is not their job. Their job is to make something or sell something, not to make good security choices, even if it is critical for their organization."

For the study, the researchers examined and compared two approaches for motivating security compliance behaviors in a changing work environment.

Protection motivation theory posits that organizations can encourage secure behaviors through fear appeals, threat messages and promoting self-efficacy, or the ability to respond to a particular threat. The practice, which often utilizes surveillance to monitor employee actions, has been used effectively for decades to deter people from engaging in risky behaviors at work and to discourage unhealthy practices such as smoking or having unsafe sex.

The second approach Crossler and his collaborators examined is stewardship theory. Stewardship theory is a form of reciprocal agreement that tries to motivate the employee's behavior through a sense of moral responsibility that is not forced. In this approach, management attempts to get the employee to buy into the organization's overall vision

while giving them organizational support to act independently when confronted with a security threat.

For the analysis, 339 people who worked at companies with IT security policies were recruited to answer a scenario-based survey. The three survey scenarios describe common policy violations that are relevant to remote work situations, such as the use of unauthorized storage devices, logging off a sensitive account when it is not in use and refraining from sharing one's password with others.

Each respondent randomly read one of three of the scenarios and then indicated their likelihood to act in a certain way based on various protection motivation and stewardship theory factors. Although working from home would seem to require relying on concepts more consistent with stewardship theory, the study showed that an approach that relied on the fear and threats emphasized in protection motivation theory was far more effective at preventing employees from violating security policy than a strictly stewardship-based approach.

One novel aspect of the study was that Crossler and his collaborators also considered a security approach that integrated factors of the two theories together.

The researchers found that promoting a sense of collectivism, a concept from stewardship theory that emphasizes the mutual benefits of good behavior for both the employee and the employer, helped increased the efficacy of protection motivation theory-based methods.

"Basically, what we found was that the more workers felt that their organization's resources were their own, the more likely they were to respond in the desired way," Crossler said. "Instilling a sense of collectivism in employees is only going to help enhance people's likelihood of protecting security policies."

The study, which was conducted in collaboration with researchers at the University of North Texas and Oklahoma State University, also showed that in some cases, a protection motivation theory approach to IT security would back-fire and result in security misbehaviors. As a result of their analysis, the authors recommend that companies should consider removing or reducing surveillance practices that are a common aspect of protection motivation theory. Where such removal is impracticable, employers should consider providing employees with contextual reasons for performing such monitoring.

"This is really the first study that brings stewardship theory and protection motivation theory together in the context of IT security for people working from home," Crossler said. "While stewardship theory did not work as well as protection motivation, our results suggest that managerial decisions informed by a stewardship perspective can help to provide a further understanding of security policy violations that motivates employees to make the right decision."

More information: Obi Ogbanufe et al, The valued coexistence of protection motivation and stewardship in information security behaviors, *Computers & Security* (2022). DOI: 10.1016/j.cose.2022.102960

Provided by Washington State University