Report on Patient Privacy Volume 23, Number 3. March 09, 2023 Are Your Workers Data Protectors or Stewards? For Best Results, Organizations Should Foster Both

By Theresa Defino

In some respects, assuring compliance with HIPAA has always been a challenge because many health care providers, particularly physicians, pride themselves on maintaining patient confidentiality—even when they aren't. Nurses, too, may feel a sense of belonging to an organization whose members all share the same commitment.

But what happens when those individuals physically leave their team and work from home, as did many who could switch to remote work during the pandemic? Would they still be good "stewards" and adhere to policies to safeguard the privacy and security of patient information? Moreover, organizations already struggle to keep their training engaging and productive. What could they do as security threats increase along with remote work to enhance compliance?

These questions puzzled Robert E. Crossler, professor of information systems at Washington State University, and David Biros, chief of information technology management at Oklahoma State University, whose wife is a nurse.

"We were talking about protection motivation theory," one focus of Crossler's research, which involves strategies such as threats, fear and surveillance to influence individuals, he told *RPP.* Biros said he "felt that his wife's experience in the health care space was different, that she ... felt like she was a part of that team, like caring for people and being part of her hospital was part of her identity," Crossler added. She embodied the stewardship theory, which calls for a personal sense of moral responsibility bolstered by support from the organization.

Crossler and Biros, who were joined by coauthor Obi Ogbanufe, an assistant professor in the University of North Texas' Department of Information Technology and Decision Sciences, launched a study to pinpoint which theory alone would work best in a primarily remote environment or whether a combination would. The title of their paper published earlier this year in *Computers & Security* gives away the conclusion: "The valued coexistence of protection motivation and stewardship in information security behaviors."[1]

The researchers presented survey participants with one of three scenarios in which an individual named Terry knowingly violates the employer's specific information security policies by downloading a "customer database" with "sensitive financial and purchase history" on a USB drive for use during travel; remaining logged into an online inventory ordering system even when not using it; and sharing a password because a coworker needs access while Terry is "away on a business trip." There were a few nuances among the scenarios, such as the size of the firm, how long Terry had worked there and job status (mid- or low-level manager).

The scenarios all include justifications for the violations: saving time and money and enhancing efficiency. Survey participants were then asked to respond to a question and a statement to assess their intention to commit an information security violation: "What is the chance that you would do what Terry did in the described scenario?" and "I would act in the same way as Terry did if I were in the same situation."

Next, the authors presented a series of statements grouped into 12 categories to assess the motivations and perceptions that might trigger a violation (and conversely, influence compliance): threat severity, fear, rewards, self-efficacy, response efficacy, response cost, organizational support, collectivism, psychological ownership, organizational commitment, autonomy and perceived surveillance.

Although mostly self-explanatory, threat severity dealt with whether violating a policy like Terry did in the scenarios would cause a problem or security breach for the organization; fear referred to a worry that the organization would be affected and was not about personal repercussions; rewards related to a perceived benefit from the violation (such as time saved); self-efficiency got at how easily the worker can comply with a policy; and response efficacy was the correlation that complying with a policy would result in better information security.

The findings are based on 339 individuals who completed the survey in May 2020. At the time, 73% were working “outside of the office due to COVID-19.” About half were male. The average age was 40, and 84% said their organization had information security policies.

Protection Theory Appeared More Prevalent

Although the respondents’ type of employment wasn’t specified, their responses are relevant to health care workers, Crossler said. “I don’t see a whole lot of difference between health care and protecting information and the [same] responsibilities that other organizations have. All of the scenarios I think absolutely would apply” to health care workers, he said.

According to responses to the questions, it appeared the protection motivation theory explained more compliance behaviors, in contrast to researchers’ expectations that “the stewardship theory would have been stronger,” said Crossler. The study also revealed specifics that could help HIPAA privacy and security officials design compliance programs.

Previous studies have shown the stewardship model is a “stronger driver” of behavior, and “maybe it was even amplified as people went home,” Crossler said. “We thought stewardship theory might have mattered because people were entering the home environment, but it was in the midst of the season when [workers thought] ‘I’m glad I have a job, that I can work from home. I need to do what I can do to make sure that our organization keeps moving forward.’”

The study also found that the more educated the respondents were, the more likely they were to violate an information security policy. This may be based on a worker thinking, “I’m educated, I know what I’m doing, so I know better,” and don’t have to follow policies, he said. “But what makes this interesting” was that those with higher incomes were less likely to violate. “That would suggest...that people who’ve been doing this for a long time and are doing well begin to recognize” the value of compliance, he added.

Making a comparison to health care workers, Crossler noted that “at some level, that would tell me that maybe the young doctor who isn’t making the [higher] income yet, hasn’t lived the experiences, might be your more apt violator of these policies.”

As measured by the response efficacy and self-efficacy questions, the authors also found that workers won’t comply with policies they believe don’t address a threat or are too difficult to follow.

Examine ‘Rewards’ for Violation Potential

The more difficult it is to comply with a policy, “the more likely it is for someone to...believe that, either they’re not going to be able to do it,” or that “they’re going to make mistakes” so they don’t adhere to the policy, he said.

Whether there is a “reward” for noncompliance also affects behavior. Crossler explained that the reward aspect relates to whether something of greater value is achieved if the worker doesn’t comply with the security policy and gets at the “tension” the employee feels. The worker is asking, “What am I rewarded for at work? Am I rewarded for getting my job done and doing it in an efficient way, or am I rewarded for properly securing and maintaining organizational resources?”

Crossler offered an example of the reward theory in action, one that might be familiar to health care officials. “I’ve seen this described to me, anecdotally…when I talk to doctors about the nurses who won't lock their workstation, because it’s that one more step for them to get to the information they need to help their patient,” he said. Organizations need to understand and address “the tension between how do we ensure that we’re locking the sensitive data while the nurse can still quickly attend to the needs of the person,” which is the nurse’s job.

Even if the system automatically locks out the user due to inactivity, nurses “got really good about [finding] ways to trick the system into thinking you were still moving the mouse,” he added.

Threat Knowledge Can Drive Compliance

Responses to the survey also showed that when workers feel fear, they appear less likely to violate information security policies. Crossler clarified that the fear is not about personal consequences but rather the potential damage to the organization.

That type of fear would stem from a different strategy—deterrence. “Deterrence theory is really about punishing the person [for violations]. Protection motivation theory is really understanding how people internalize how bad the actual data breach would be” if it resulted in a “loss of that information,” he said.

The study also confirmed prior findings that “when people feel monitored, surveilled, [they] resist that. If we take people and we put them in their home environment and they feel like you’re surveilling them and watching them…that is having a more detrimental effect on people” rather than the “controlling effect” the organization had hoped for, he added.

HIPAA officials could integrate the study findings into their compliance programs in two ways, according to Crossler. Compliance programs could focus on the aspects of protection motivation theory that stress ensuring workers understand the threats, believe complying with a policy will address them, and can follow the procedures required, he said.

Utilizing aspects of the protection model, organizations should target the “threats, control mechanisms and the policy compliance that we want to have based on what is going on today,” he said. Threats are “always changing,” and hackers are playing a “game of cat-and-mouse” with organizations. “As soon as we get good at blocking one threat, the bad guys adapt and they’re coming at us from a different angle,” Crossler added.

‘Demonstrate You Trust Your Employees’

“But I would also encourage organizations to culture an environment that builds stewardship,” he said, adding, “I don’t think stewardship is the sort of thing that you would get just through a training program.”

Instead, this “really becomes the nature of who you are as an organization” through ensuring the “support mechanisms” are in place and demonstrating “that you trust your employees and give them the autonomy to do their jobs and keep the security” of the information they handle, he said.

Compliance plans should "focus on those points where people have to make decisions, whether being able to recognize when [they're] being phished, [not] sharing passwords, avoiding shoulder surfing when you're outside of the office" and building "situational awareness of where you're able to pick on those areas and identify those areas where behaviors absolutely matter," he said.

Crossler added that while this is not specifically addressed in the paper, "I would argue that the more control you can take out of your employee's hands where you can" and automate security, the better.

In sum, both strategies are important, Crossler said.

A protection motivation theory-inspired compliance program will "focus on 'What are the threats? What can you be doing about it? Here are the skills to be able to do something,' whereas the stewardship [model] and people feeling like they're stewards in the organization is more about what the organization is. [This is] a longer-term sort of thing that doesn't change nearly as much. It really is about the culture of the environment," he said.

[1] Obi Ogbanufe, Robert E. Crossler, and David Biros, "The valued coexistence of protection motivation and stewardship in information security behaviors," *Computers & Security* 124, January 2023, 102960, https://bit.ly/3mi185Q.