Some employees more likely to adhere to information security policies than others

October 6 2020

Credit: CC0 Public Domain

Information security policies (ISP) that are not grounded in the realities of an employee's work responsibilities and priorities expose organizations to higher risk for data breaches, according to new research

from Binghamton University, State University of New York.

The study's findings, that subcultures within an organization influence whether employees violate ISP or not, have led researchers to recommend an overhaul of the design and implementation of ISP, and to work with employees to find ways to seamlessly fit ISP compliance into their day-to-day tasks.

"The frequency, scope and cost of data breaches have been increasing dramatically in recent years, and the majority of these cases happen because humans are the weakest link in the security chain. Non-compliance to ISP by employees is one of the important factors," said Sumantra Sarkar, associate professor of management information systems in Binghamton University's School of Management. "We wanted to understand why certain employees were more likely to comply with ISP than others in an organization."

Sarkar, with a research team consisting of Anthony Vance of Temple University, Balasubramaniam Ramesh of Georgia State University, Menelaos Demestihas of Wellstar Kennestone Hospital and Daniel Thomas Wu of Emory University School of Medicine, sought to determine how subcultures influence compliance, specifically within healthcare organizations.

"Every organization has a culture that is typically set by top management. But within that, you have subcultures among different professional groups in the organization," said Sarkar. "Each of these groups are trained in a different way and are responsible for different tasks."

Sarkar and his fellow researchers focused on ISP compliance within three subcultures found in a hospital setting—physicians, nurses and support staff.

The expansive study took years to complete, with one researcher embedding in a hospital for over two years to observe and analyze activities, as well as to conduct interviews and surveys with multiple employees.

Because patient data in a hospital is highly confidential, one area researchers focused on was the requirement for hospital employees to lock their electronic health record (EHR) workstation when not present.

"Physicians, who are dealing with emergency situations constantly were more likely to leave a workstation unlocked. They were more worried about the immediate care of a patient than the possible risk of a data breach," said Sarkar. "On the opposite end, support staff rarely kept workstations unlocked when they were away, as they felt they were more likely to be punished or fired should a data breach occur."

Researchers concluded that each subculture within an organization will respond differently to the organization-wide ISP, leaving organizations open to a higher possibility of data breaches.

Their recommendation—consult with each subculture while developing ISP.

"Information security professionals should have a better understanding of the day-to-day tasks of each professional group, and then find ways to seamlessly integrate ISP compliance within those job tasks," said Sarkar. "It is critical that we find ways to redesign ISP systems and processes in order to create less friction."

In the context of a hospital setting, Sarkar recommends touchless, proximity-based authentication mechanisms that could lock or unlock workstations when an employee approaches or leaves a workstation.

Researchers also found that most employees understand the value of ISP compliance, and realize the potential cost of a data breach. However, Sarkar believes that outdated ISP compliance measures have the potential to put employees in a conflict of priorities.

"There shouldn't be situations where physicians are putting the entire hospital at risk for a data breach because they are dealing with a patient who needs emergency care," he said. "We need to find ways to accommodate the responsibilities of different employees within an organization."

More information: Sumantra Sarkar et al, The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context, *Information Systems Research* (2020). DOI: 10.1287/isre.2020.0941

Provided by Binghamton University