Korie Cooper
4/7/26

This article by Ghaleb and Pardaev, published in the International Journal of Cyber Criminology examines the organizational and psychological factors that influence employee information security compliance behavior in production companies. Organizational culture, cybersecurity awareness, and employee involvement are the strongest predictors of security compliance, with trust in management serving as a reinforcing factor.

This journal relates to several topics in the social sciences, including behavioral science, social control, culture and socialization. Organizational culture can condition normal behavior to include safety and security in workers as well as get trust in management's authority and legitimacy. The study applies quantitative data and uses statistical models to analyze the relationship between organizational culture and security behavior.

Research Question: What organizational and psychological factors influence information security compliance in production companies?
Hypothesis: Organizational culture, cybersecurity awareness, employee involvement, and trust in management each positively predict compliance behavior.
Independent Variables: Organizational culture, cybersecurity awareness, employee involvement, trust in management.
Dependent Variable: Information security compliance behavior.

Types of Research Methods Used
The study used a quantitative by collecting survey data from 261 employees across multiple departments using scales from prior journals.
Types of Data Analysis Used
Structural Equation Modeling (SEM) via STATA and Confirmatory Factor Analysis (CFA) were used to test hypothesized relationships and validate the measurement model.

Connection to Course

Employees are more likely to adopt information security behavior if they see their organizational members behaving in information security ways. Employees weigh the potential risk before deciding whether or not to behave in information security ways. Employees' trust in management with respect to information security behavior corresponds to the human factor.

Conclusion

Cybersecurity can be affected as much by human behavior as by technology, and therefore managing information security requires organizations to take into account a host of organizational and social factors. This journal for practitioners provides insights on managing

the workforce and information security policy in industries with very high compliance requirements, such as defense and government.

Reference
https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123