Article Review #2: Controlling Cyber Crime through Information Security Compliance Behaviour

Twaitney Addison

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Dr. Jordan Quinn

April 6, 2026

Introduction/Bluff

This article review covers a 2025 study by Ghaleb and Pardev published in the International Journal of Cyber criminology. The study looks at why some employees follow cybersecurity policies and others do not, specifically fousing on how things like workplace culture, security awareness, and trust in leadership play a role. The short version is this: it is not enough to just hand employees a list of rules and expect them to follow it. The study found that when people feel connected to their organizations, trust their management, and actually understand why securit matters, they are ar more likely to do the right thing when it comes to protecting information.

Relation/Connection to Social sciences principles

What makes this study interesting from social science perspective is that it treats cybersecurity as a human problem, not just a technical one. One of the core principles of social science is empiricism, which basically means you back up your claims with real data instead of just guessing. This study does exactly that by surveying 261 employees and running the numbers to see what actually predicts secure behaviour. It also connects to the principle of determinism, which is the idea that behaviour has cause you can identify and study. The researchers are not

saying employees randomly choose to follow or break security policies. They are saying specific factors push people in one direction or the other. The study also reflects objectivity b using a statistical method called structural equation modeling to test its ideas, Which keeps personal bias out of conclusion. On top of that, It builds on existing theories rather than starting rom scratch, which reflects the social science principle that knowledge is cumulative each study adds towhat we already know. Overall, the research treats huan behaviour in the workplace the same way social scientists treat behaviour anywhere: as something shaped by environment, relationships, and individuals psycology

Research Questions/Hypothesis/Independent Variable/Dependent Variable

-**Research Questions**: The study is really asking one big question in a few different ways, What makes employee actually follow cybersecurity policies? More specifically, it looks at whether workplace culture matters, whether awareness training works, whether engaged employees are safer, and whether trusting leadership changes how people act.

-**Hypothesis**: The researchers came up with six hypotheses. They predicted that organizational culture would influence compliance, that cybersecurity awareness would influence compliance, that employee engagement would strengthen the effect of both culture and awareness on compliance, and that trust in upper management would act as a bridgeconnecting culture and awareness to actual behaviour. All six predictions turned out to be supported by the data.

-Independent Variable: The independent variables are organizational culture, cybersecurity awareness, and employee engagement. Employee engagement also worked as a moderating variable, meaning it changed how strong the other relationships were. Trust in upper management acted as a mediating variable, meaning it helped explain how the other factors led to compliance.

-Dependent Variable: The dependent variable is information security compliance behavior basically, whether or not employees actually follow the security policies their organization has in place.

Types of Research Methods Used

This study used a quantitative approach, which means it collected numerical data and used statistics to find patterns. The researchers sent out surveys to 261 employees working in different departments like IT, operations, HR, and quality assurance at production companies. The surveys were distributed both in person and online to reach as many people as possible. Participants were chosen specifically because they regularly use digital systems and deal with information security in their jobs, so their answers would actually be relevant. Every question on the survey came from scales that had already been tested and validated in past research, which makes the results more trustworthy. Responses were given on a scale from one to five, ranging from strongly disagree to strongly agree.

Types of Data Analysis Used

Once the survey data was collected, the researchers used a method called Structural Equation Modeling, or SEM, to analyze it. SEM is useful because it can test multiple relationships at the same time instead of looking at each one separately. Before getting to that, they ran a Confirmatory Factor Analysis to make sure all their measurements were actually capturing what they were supposed to capture. They also checked reliability using Cronbach's Alpha and other measures to confirm the survey questions were consistent. The model fit was tested using several statistical indicators, and the results showed the model matched the data well. In the end, the model explained about half of the variation in both trust and compliance behavior, which is a solid result for this type of behavioral research

Connection to other Course concepts

This study connects pretty directly to what we have been covering in class about the human side of cybersecurity. One of the biggest takeaways from the course is that people are often the weakest link in any security system, not because they are careless on purpose, but because behavior is complicated and shaped by a lot of factors. This study backs that up by showing that things like culture and trust which are not technical at all have a huge impact on whether people actually follow security rules. The study also ties into the psychological theories we have discussed. The Theory of Planned Behavior says that people are more likely to do something when they see it as normal and expected in their social environment. That connects directly to what this study found about organizational culture when security is treated as a shared value rather than just a policy on paper, employees are more likely to internalize it. Social Exchange Theory, which looks at how people respond to how they are treated, also shows up here. When employees trust their leadership and feel respected, they give that back through responsible behavior. These are not abstract ideas the data in this study actually shows them playing out in a real workplace setting.

Overall societal contributions of the study/Conclusion

Overall, this study does a good job of making the case that cybersecurity is not purely a technology problem it is a people problem. The findings show that when organizations invest in building a strong culture around security, help employees actually understand the threats they face, keep workers engaged, and earn their trust, compliance improves in a meaningful way. That matters beyond just one company or one industry. Data breaches affect real people their personal information, their finances, their privacy so organizations that do a better job at this are also doing right by the public. The study gives researchers and practitioners a concrete model they can build on, and it reinforces the idea that lasting security is built the same way most good things are: steadily, intentionally, and with people at the center of the effort.

Reference

Ghaleb, M. M. S., & Pardaev, J. (2025). Controlling cyber crime through information security compliance behavior: Role of cybersecurity awareness, organizational culture and trust in management. International Journal of Cyber Criminology, 19(1), 1–26. https://doi.org/10.5281/zenodo.476619101

Article Link:

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