Can we trust management?

Emmanuel Walker

Diwakar Yalpi

CYSE 201S Cybersecurity and the Social Sciences

11/16/2025

The journal looks at how rising cybercrime harms the financial stability of customer trust and organizational security in nations that are developing. Because it analyzes human behavior, this topic has a direct connection to social science ideas. Cybercrime is sometimes viewed as a technological issue, but it is strongly based on social patterns such as trying to shift societal norms around through digital systems. They use technology and interact with computers for a variety of purposes, and the distinction between the physical and virtual dimensions of organized crime is increasingly blurred. Social science ideas look at cybercrime through the perspectives of criminology, sociology, and economics analyzing human behavior.

Identifying some of the many types of cybercrime that affect banks, primarily the weakness within financial institutions, and how these attacks do affect the general population and the banking system as a whole. In theory, cybercriminals target institutions with inadequate cybersecurity infrastructures more frequently than others because of the easy access into their systems. Second, it may mean that cyberattacks damage the customer trusts the first time, then those companies could lose business unless they fix the problem in a timely manner. The more common types of cyberattacks are like phishing, identity theft, malware, etc. as well as the level of cybersecurity preparation. People in society would expect their systems to be highly protected, but these types of crimes continue. Citizens in this society cannot afford any economic losses, organizational disruptions, and customers should feel comfortable and feel like they can trust that their information is safely guarded. It is also up to that person to safeguard their privacy as well. “As much as firewalls and encryption software provide technical security measures, human actions tend to be the weakest link in cybersecurity frameworks” (Sutton & Tompson, 2025).

We could use a mixed-methods research design by using both qualitative and quantitative data. Using qualitative data from interviewing people about whether or not they have been attacked by any form of hacking and how did they handle the situation. On the other hand, with different case studies it could help with comparing quantitative data from financial loss statistics. This allows the researcher to determine not only how frequent hacks occur, but also why they occur and how banks respond. Interviews with bank personnel reveal organizational issues, training deficiencies, and enforcement limitations. Meanwhile, financial data and case histories provide evidence of the costs connected with security breaches. The data set can improve by providing a well-rounded perspective that includes both behavioral and institutional influences.

Data analysis involves thematic coding of interviews as well as describing the statistics of the financial information. Doing the qualitative data, I could see how the management is doing. Are they struggling with employee training, gaps in security protocols, and insufficient government regulation? If this is an ongoing problem, then the problem should be fixed sooner rather than later. The people in society should know that the people who keep their money safe in trustworthy enough to be able to have systems that are not easily accessible to outsiders. The quantitative research will see all reported financial losses and event numbers showing the growing severity of cybercrime. The use of both methods of study reveals the complex nature of cybercrime, it is influenced by both human behavior and technological variables.

Behavioral theory does relate to this well because of the environmental influences that determine human activities, including criminal or irresponsible behavior. “Is a theoretical perspective in psychology that emphasizes the role of learning and observable behaviors in understanding human” (McLeod, 2025). Employees who engage in risky practices regularly like clicking questionable links or failing to update passwords, are displaying behaviors that the

workplace culture doesn't need. Every job has one person who tries to sneak to do things that they are not supposed to be doing. Supervisors should have access to your system, but not your personal information, for better security. When banks fail to promote secure behaviors through constant training and monitoring because employees start to create patterns that make intrusions more likely.

For more marginalized groups, particularly in Saudi Arabia, economic and social gaps can influence vulnerability to cybercrime. Despite Saudi Arabia's technology advancements, not all populations have equal access to digital literacy, cybersecurity education, or safe banking services. “This advancement significantly boosted the participation of women in the technology sector from 7% in 2018 to an impressive 35% today, the highest rate in the Middle East and North Africa, and exceeding the averages of both the G20 and the European Union — reflecting the depth of the Kingdom’s transformation in empowering national capabilities in the digital economy” (*Saudi Arabia’s Digital Economy)*. Low-income workers, particularly foreign laborers who represent a sizable proportion of the population, rely on low-cost mobile devices and limited internet connections with inadequate safety precautions. That makes it easier for hackers to attack those affected by phishing scams, online banking fraud, and identity theft because they may not notice the warning signs or understand how to protect themselves. Also, migrant workers struggle to grasp cybersecurity warnings and check the integrity of digital communications due to language barriers. When financial institutions are cyberattacked, the consequences flow down to marginalized groups who may already be struggling financially. For example, increasing banking fees makes financial access more difficult for migratory workers and low-income Saudis.

In conclusion, the journal highlights the urgent need for greater cybersecurity in the financial industry. "This trust serves as a bridge that translates security awareness into action" (International Journal of Cyber Criminology). It underlines the significance of staff training, regulatory monitoring, and investment in digital security technologies. Cybercriminals impact more than just banks, but they impact public trust, and social well-being. Professionals need to take an inclusive approach to cybersecurity by connecting technology crime to social sciences principles. This provides a good perspective on how communities might safeguard themselves in the digital world.

Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behavior framework: A rapid evidence review. Computers & Security,148, 104110. https://www.sciencedirect.com/science/article/pii/S0167404824004152?via%3Dihub

McLeod, S. (2025, May 12). *Behaviorism in psychology*. Simply Psychology. https://www.simplypsychology.org/behaviorism.html

Saudi Arabia's Digital Economy: A New Era of Tech Growth, Innovation, and Global Impact Empowered by HRH the Crown Prince | Ministry of Communications and Information Technology. (2025). Mcit.gov.sa. https://www.mcit.gov.sa/en/news/saudi-arabia%E2%80%99s-digital-economy-new-era-tech-growth-innovation-and-global-impact-empowered-hrh

(2025, January). *Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management* [Review of *Controlling Cyber Crime through Information Security Compliance Behavior: Role of Cybersecurity Awareness, Organizational Culture and Trust in Management*]. International Journal of Cyber Criminology; Diamond Open Access. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/437/123