Article Review #2: Psychological Traits of Cybercriminals Essay

Student: Shaun Farmer

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor: Dr. Diwakar Yalpi

Date: November 7, 2025

Psychological Traits of Cybercriminals: A Comprehensive Review for Improved Cybercrime Prevention

BLUF

The study is a systematic literature review that pairs psychological traits and contextual factors associated with cyber offending with organizational, legal, and technical controls for prevention. It argues that "layered approaches" are necessary to minimize the societal impact of cybercrime, including recurrent training and awareness programs, incident response and disaster recovery plans that have been tested, data-protection compliance, and public–private information sharing (Trinh et al., 2025).

Relation/Connection to Social Science Principles

The article connects to several foundational "social-science lenses" in this course: (1) behavioral and psychological approaches to understand offender motivation and social-engineering methods; (2) institutional and organizational perspectives on culture, norms, training, and policy design; (3) legal and regulatory instruments such as GDPR and CISA as social control mechanisms; and (4) collective action mechanisms like Information Sharing and Analysis Centers to facilitate cooperation and norm-enforcement across stakeholders.

Research Question / Hypotheses / Independent Variable / Dependent Variable

Research Question: What psychological traits and contextual factors characterize cybercriminals, and which prevention strategies are most effective for reducing cybercrime? Hypotheses: As a literature review, the paper does not formally test hypotheses; the reviewed and synthesized literature suggests that stronger training, policy, and coordinated response measures decrease attack success and impact. Independent Variables (from the aggregated

studies): offender characteristics (e.g., risk-taking, rational actor traits); organizational controls (awareness, incident response, disaster recovery plans); the regulatory environment; and technology posture (AI/ML tooling, IoT hardening) Dependent Variables: the dependent variables include different cybercrime outcomes such as breach occurrence and frequency, detection/response times, economic losses, and organizational resilience (Trinh et al., 2025).

Types of Research Methods Used

The authors perform a systematic literature review, collecting peer-reviewed journal articles, frameworks, notable incidents, and standards. They use thematic synthesis to organize findings rather than conducting a primary experiment or survey, following best practices for evidence-based aggregation (Trinh et al., 2025).

Types of Data and Analysis Used

The data sources include primary empirical studies, policy documents, case study analyses, and technical reports. The data analysis is a thematic synthesis: the article organizes the evidence into categories/domains: human factors and offender psychology; organizational preparedness (training, incident response, and disaster recovery planning); legal and regulatory compliance; information sharing and collaboration; and emerging challenges (APTs, AI/ML, IoT) (Trinh et al., 2025).

Connections to Other Course Concepts

Routine Activity Theory resonates throughout the piece: the importance of capable guardianship (training, monitoring); motivated offenders such as those in APT groups; and vulnerable targets (suitable targets) like unhardened IoT endpoints. Other class concepts, such as human-centered security, similarly undergird the review's focus on awareness culture as a

"human firewall." Governance and policy material from the course connect to the authors' discussions of GDPR/CISA and how compliance serves as a behavior-shaping institutional mechanism. Sociotechnical systems thinking is also reflected in the dual-use aspects of AI/ML systems, which are useful for both attackers and defenders (Trinh et al., 2025).

Connections to the Concerns or Contributions of Marginalized Groups

The paper implicitly references disparities across organizational sizes and resources, noting that small and medium-sized enterprises (SMEs) and other resource-constrained groups are at a higher relative exposure and experience slower recovery in the absence of easily implemented controls. It highlights the need for research on psychological effects on victims as well as more accessible, affordable security solutions, pointing to equity issues in cyber resilience.

Overall Societal Contributions of the Study / Conclusion

This review bridges offender psychology and mental models, organizational "best practice," and policy and regulation to offer a comprehensive overview of "layered" defense measures: training and awareness culture-building, tested incident response and recovery plans, alignment to standards for compliance, and collaborative information sharing. It also highlights priority fronts (APTs, AI/ML dual-use, IoT risk) and knowledge gaps (behavioral cybersecurity, SME resilience) in the field. Collectively, the insights could underpin more coordinated, human-centered cybercrime reduction strategies, with particular benefit for underserved organizations and populations (Trinh et al., 2025).

References

Trinh, D. T., Dinh, T. C. H., & colleagues. (2025). Exploring the psychological profile of cybercriminals: A comprehensive review for improved cybercrime prevention. International Journal of Cyber Criminology, 19(1), 116–133. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/452/133

Article Link:

https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/452/133