Abstract

This dissertation explores the application of Routine Activity Theory (RAT) to develop a preventive framework for data breaches, aiming to enhance current cybersecurity tools. By examining the potential of traditional criminological theories to inform cybersecurity practices, this study seeks to bridge the gap between social science and technological fields. RAT, a theory traditionally used to explain crime patterns through the convergence of motivated offenders, suitable targets, and the absence of capable guardians, is adapted to the cyber domain to identify key variables and mechanisms that contribute to data breaches.

The research begins with an extensive review of existing literature on RAT and cybersecurity, followed by a detailed analysis of data breaches to identify common patterns and vulnerabilities. Through this analysis, the study aims to validate the applicability of RAT in predicting and preventing cyber incidents. The proposed framework incorporates these findings to provide organizations with a tool to assess their cybersecurity posture, identify potential risks, and implement targeted preventive measures.

Despite inherent challenges, such as the limited availability of detailed cyberattack data and the need for a flexible theoretical model, this dissertation demonstrates that RAT's adaptability can be leveraged to address the dynamic nature of cyber threats. The study's findings suggest that integrating criminological theories into cybersecurity strategies offers a promising avenue for enhancing defenses against data breaches.

By fostering interdisciplinary collaboration, this research contributes to a more comprehensive understanding of cybersecurity threats and presents a novel approach to developing proactive security measures. The dissertation concludes with recommendations for future research and the potential for regulatory frameworks to improve transparency and data availability, ultimately enhancing the robustness of predictive models and preventive strategies in cybersecurity.