MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

A Review on the Application of Lifestyle-Routine Activity Theory in Cyber Criminology

Riya Raj CA[1]* and Caeiro D[2]

[1]Masters student, Department of Forensic science, Kristu Jayanti college, India
[2]Assistant professor, Department of Forensic science, Kristu Jayanti college, India

***Corresponding author:** Riya Raj CA, Department of Forensic Science, Masters Student, Kristu Jayanti College, Bengaluru, India, Email: riyaraj5345@gmail.com

Review Article
Volume 9 Issue 3
Received Date: July 15, 2024
Published Date: July 26, 2024
DOI: 10.23880/ijfsc-16000401

Abstract

In an age dominated by technology across all facets of living, the rise of cybercrime emerges as a significant issue for the individuals. The integration of lifestyle-routine activity theory (L-RAT) in the field of cyber criminology offers a robust framework for understanding the dynamics of online victimization. This review paper explores how L-RAT can be useful in detecting the unique characteristics of cybercrime. By examining the key components of L-RAT like motivated offenders, suitable targets and the absence of capable guardians by demonstrating its relevance in digital context. This review also synthesizes the empirical studies and theoretical advancements that apply L-RAT to various forms of cyber crime including online frauds, identity theft and cyber stalking. Additionally by also addressing the implications of cyber security practices and policy making by highlighting strategies to mitigate risk and to ensure online safety. The paper aims to highlight the importance of L-RAT in providing an understanding of cyber criminal behavior and victimization ultimately contributing to more effective prevention and intervention measures in the digital age. The article concludes with suggestions for future research directions to improve the applicability of the theory in the cyber space. By exploring various studies, the article highlights the usefulness of the theory to explain cyber victimization, criminal behavior and the effectiveness of preventive measures in the digital world.

Keywords: Cyber Criminology; Lifestyle Theory; Routine Activity Theory; L-RAT

Abbreviations

L-RAT: Lifestyle-Routine Activity Theory; 2FA: Two-Factor Authentication.

Introduction

Lifestyle-Routine Activity Theory (L-RAT) offers a framework that examines how individuals' everyday habits and lifestyles impact their susceptibility to crime. Introduced by Lawrence E. Cohen and Marcus Felson in 1979, L-RAT was originally used to explain patterns of victimization in physical crimes like burglary, robbery, and assault. According to the theory, three key factors influence the likelihood of crime: the presence of motivated offenders, the presence of suitable targets, and the absence of capable guardians. The theory suggests that crime rates can be influenced by changing any of these three components. For example, increasing the presence of capable guardians (like police patrols) or making targets less suitable (through better locks and security measures) can reduce the likelihood of crimes occurring, even if motivated offenders are still present. L-RAT has been used to explain why certain individuals or locations are more susceptible to criminal activity. For instance, someone who lives alone in a poorly lit neighborhood and frequently travels may be perceived as a suitable target due to their predictable absence from home. But lately, L-RAT has been adapted to understand victimization in cyber contexts, where routine activities and lifestyles are increasingly conducted online. People follow regular, predictable patterns of behavior in their daily lives, such as commuting to work or school, participating in leisure activities, shopping, and socializing. According to the theory, engaging in these routine activities exposes individuals to potential opportunities for victimization. Criminals make calculated decisions based on their assessment of risks versus rewards. They tend to target individuals or places where they perceive a low risk of getting caught and a high probability of success.

Related Literature

Reyns BW [1] - "Online Routines and Identity Theft Victimization"

- Reyns BW [1] investigated how daily online routines influence the risk of identity theft. The study found that individuals who engage in high-risk online activities (e.g., online shopping, social networking) are more likely to become victims of identity theft. It also validated L-RAT by demonstrating that exposure to potential offenders and target suitability significantly impact victimization rates.

Holt TJ, et al. [2] - "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization"

- Holt and Bossler explored the relevance of L-RAT in explaining the victimization of individuals who engage in online activities. The study highlighted that routine activities such as frequent use of the internet and participation in social networking sites increase exposure to cyber threats.It supported L-RAT by showing a positive correlation between risky online behaviors and cybercrime victimization.

Mesch GS (2009) - "Parental Mediation, Online Activities, and Cyberbullying"

- Mesch examined the role of parental mediation in adolescents' online activities and their exposure to cyberbullying. The results indicated that adolescents who spend more time on social media and engage in risky online behaviors are more likely to experience cyberbullying. This study reinforced L-RAT by linking the frequency and nature of online activities with increased victimization risk.

Ngo FT, et al. [3] - "Cybercrime Victimization: An Examination of Individual and Situational Level Factors"

- Ngo and Paternoster analyzed individual and situational factors contributing to various forms of cybercrime victimization. They found that personal characteristics (e.g., age, gender) and online routines (e.g., social networking, online shopping) are significant predictors of victimization. Their findings supported L-RAT, emphasizing the importance of routine activities in understanding cybercrime victimization.

Leukfeldt ER, Yar M (2016) - "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis"

- Leukfeldt and Yar conducted a theoretical and empirical analysis of L-RAT's application to cybercrime. The study confirmed that online routine activities, such as frequent internet use and engagement in social networks, increase the risk of becoming a victim of various cybercrimes. It validated L-RAT's applicability to cyber contexts by demonstrating how routine activities create opportunities for cybercriminals.

The Lifestyle Routine Activity Theory (LRAT), which stems from criminology, posits that the likelihood of becoming a victim of crime is influenced by everyday activities and lifestyle choices. Applying this framework to social media oversharing can help explain why certain individuals are more prone to disclosing excessive personal information online. According to LRAT, the more frequently individuals engage in activities that expose them to potential threats, the higher their risk of victimization. On social media, individuals who spend a significant amount of time online and frequently share updates about their lives are more exposed to the risks associated with oversharing. This constant online presence increases the chances of sharing sensitive information inadvertently [4].

LRAT also suggests that individuals who possess valuable or desirable characteristics are more likely to be targeted by offenders. In the context of social media, users who share information about their wealth, possessions, or personal achievements may become attractive targets for criminals seeking opportunities for theft, fraud, or other malicious activities [5].

The theory emphasizes the importance of capable guardians, people or mechanisms that can protect potential victims from harm. On social media, the absence of such guardians can lead to oversharing. For instance, without proper privacy settings, guidance on safe online behavior, or awareness of the risks, users are more likely to share personal information freely. It considers the physical or virtual proximity to potential offenders. Social media platforms bring users into closer virtual proximity with a vast array of individuals, including those with malicious intent. This increased interaction heightens the likelihood of encountering someone who might misuse the shared information [6].

It is observed Individuals daily routines and habits influence their patterns of social media use. Those with routines that include frequent social media check-ins, updates, and interactions are more likely to develop habits of oversharing. This consistent behavior can make it easier for malicious actors to predict and exploit vulnerabilities [7-10].

Understanding LRAT and its implications for social media behavior can help users navigate online interactions more safely and reduce the likelihood of negative consequences from oversharing. Sharing personal Information on Social Media platforms like Facebook, Twitter, Instagram, and LinkedIn are vital for communication, self-expression, and networking. However, the increasing tendency to overshare personal information on these platforms brings with it significant risks. These risks include threats to privacy, identity theft, professional consequences, mental health issues, data exploitation, security risks, and strained relationships. One of the primary concerns of oversharing on social media is the threat to personal privacy. Users frequently post sensitive details such as home addresses, phone numbers, and daily routines without fully considering the potential risks. This information can be easily accessed by malicious individuals or organizations, leading to privacy breaches and exposing users to unwanted attention or harm. Once shared, the digital footprint is challenging to erase, making it vital for users to carefully consider what they post online [11].

Another severe consequence of oversharing is identity theft. Cybercriminals can compile seemingly innocuous details shared on social media to steal identities, leading to financial loss, damaged credit scores, and a long, arduous process to reclaim one's identity. For example, sharing information such as birthdates, mother's name, or pet names—often used in security questions—can provide criminals with the information needed to access personal accounts [12].

Oversharing can also have significant professional repercussions. Security threats are also heightened by oversharing. Announcing vacations or significant purchases on social media can alert burglars to opportunities. For instance, posting about an upcoming trip can signal that a home will be unoccupied, making it an easy target for theft. Similarly, sharing photos of expensive new gadgets can attract the attention of criminals [13-16].

Inadequate cybersecurity practices can greatly compromise the security of systems and sensitive data. A common issue is the use of weak passwords, which are often easy to guess or reused across different sites, making it easier for cybercriminals to gain unauthorized access. Another significant vulnerability is the absence of two-factor authentication, which adds an essential layer of security [17,18]. Without this, accounts are more prone to being breached through password attacks. Failing to keep software and applications up to date is another major risk, as outdated software can have known vulnerabilities that cybercriminals can exploit. Furthermore, not maintaining regular backups can worsen the effects of ransomware attacks, potentially forcing victims to pay ransoms to regain access to their data [19,20].

User behavior also significantly contributes to cybersecurity risks. Users who frequently click on unverified links are at a higher risk of phishing and malware attacks. Similarly, downloading software from unofficial or untrusted sources can lead to the installation of malicious programs like malware or spyware. Ignoring security warnings from browsers or systems about potential threats can also result in exposure to harmful websites and software. To address these issues, organizations need to implement robust cybersecurity policies, provide regular training, and maintain vigilance in following best practices.

Discussion

Victims of lifestyle routine activity cyber crimes can greatly reduce their risk by implementing several safety measures and protocols. Firstly use strong, complex passwords and avoid using the same password for multiple accounts. Utilizing a password manager can help securely store and generate these passwords. Activating two-factor authentication (2FA) provides an additional security layer, with authentication apps being preferred over SMS-based methods. Keeping software and applications up-to-date ensures that systems are protected with the latest security patches. Regularly backing up important data to external hard drives or secure cloud services, and periodically verifying these backups, can lessen the impact of ransomware attacks. Practicing safe browsing habits is essential: avoid clicking on suspicious links, only enter personal information on secure websites, and be aware of common phishing tactics. Enhancing online security includes using strong, unique passwords for Wi-Fi networks and utilizing a VPN when on public Wi-Fi. Installing reputable antivirus and anti-malware software, along with scheduling regular scans, helps defend against threats. Limiting the sharing of personal information online and adjusting privacy settings on social media to control who can see your information also reduce risks. Finally, having an incident response plan and recognizing signs of compromised accounts can enable swift responses to potential cyber threats. The lifestyle routine activity theory in cyber criminology provides a robust framework for exploring how everyday behaviors impact the likelihood of falling victim to cybercrime. According to this theory, cybercrime occurs when a motivated offender finds a suitable target in the absence of effective guardianship. In the digital realm, this manifests through common activities like frequent internet use, social media engagement, and online transactions, all of which can attract cybercriminals. Insufficient cybersecurity measures such as weak passwords, lack of two-factor authentication, and outdated software further exacerbate vulnerabilities. Additionally, behaviors such as clicking on suspicious links and downloading unverified software heighten the risk. Emphasizing the integration of cybersecurity practices into daily routines is crucial to mitigating these risks. Understanding how routine online behaviors contribute to cybercrime allows for the development of targeted prevention strategies that address individual actions and broader systemic weaknesses. This underscores the ongoing need for education and awareness to keep pace with the evolving landscape of cyber threats.

References

1. Reyns BW (2013) Examining situational mechanisms in the context of online victimization: A routine activity theory approach. Journal of Research in Crime and Delinquency 50(2): 216-238.
2. Holt TJ, Bossler AM (2008) Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior 30(1): 25-53.
3. Ngo FT, Paternoster R, Bachman R, Kendler KS (2017) Routine activities and victimization: The role of opportunity in explaining ongoing exposure to crime. Journal of Quantitative Criminology 33(1): 193-213.
4. Akbulut Y, Oğuz A (2014) Cyberbullying: A new face of workplace bullying. Procedia - Social and Behavioral Sciences 152: 299-304.
5. Bossler AM, Burruss GW (2011) Assessing the applicability of lifestyle-routine activities theory for cybercrime victimization. Western Criminology Review 12(3): 1-16.
6. Bossler AM, Holt TJ (2009) On-line activities, guardianship, and malware infection: An examination of routine activities theory. Journal of Research in Crime and Delinquency 46(1): 4-27.
7. Chon MG, Wilcox P, Lim H (2019) Routine activity theory and cybercrime: A meta-analysis. Journal of Contemporary Criminal Justice 35(1): 43-61.
8. Cohen LE, Felson M (1979) Social change and crime rate trends: A routine activity approach. American Sociological Review 44(4): 588-608.
9. Conklin WA, Broida J (2019) Understanding cybercrime: A guide for developing countries. Journal of Global Information Management 27(4): 61-86.
10. Holt TJ, Bossler AM (2016) Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior 37(3): 263-280.
11. Kaur K, Rani S (2020) Cyber victimization: An application of routine activities theory. Journal of Cybersecurity Education, Research and Practice 1(1): 28-42.
12. McKinnon L (2019) Cyberbullying and digital citizenship: A literature review. The Clearing House: A Journal of Educational Strategies, Issues and Ideas 92(1): 18-25.
13. Maimon D, Alper M (2019) The utility of a theoretical framework for understanding cyberbullying victimization. Crime & Delinquency 65(6): 727-757.
14. Reyns BW (2010) A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. Crime Prevention and Community Safety 12: 99-118.
15. Reyns BW (2019) Routine activities and internet fraud victimization. Cyberpsychology, Behavior, and Social Networking 22(7): 485-491.
16. Reyns BW, Burek MW, Henson B, Fisher BS (2011) The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. Journal of Criminal Justice 36(1): 1-17.
17. Reyns BW, Henson B, Fisher BS (2012) The cybercrime victimization–knowledge gap: Exploring the extent and correlates of online crime and harm awareness. Crime & Delinquency 58(6): 879-907.
18. Reyns BW, Henson B (2016) Techno-socialization and cyberbullying victimization: A routine activities approach. Journal of Criminal Justice 46: 160-170.
19. Yar M (2005) The novelty of 'cybercrime'An assessment in light of routine activity theory. European Journal of Criminology 2(4): 407-427.
20. Zhang L, Katsiyannis A (2017) Cyberbullying victimization: An examination of law enforcement reporting among high school students. Journal of School Violence 16(1): 71-88.