An Analytical Review of Factors Influencing Behavior

Alex Brown

Old Dominion University

CYSE 201: Cybersecurity and Social Sciences

An Analytical Review of Factors Influencing Behavior

Intro

Cybercrime has become one of the fastest growing forms of criminal activity in the modern age. It's a complex issue with far-reaching consequences. The methods used by cybercriminals are constantly evolving. Thus, making methods and opportunities for cybercrime more likely to occur more frequently. Therefore, making it relevant in the sphere of social sciences has become a societal issue with significant impact. The article under review delves into the multifaceted nature of cybercrime, examining its roots and manifestations through a social science lens. This review will break down the article's approach to understanding cybercrime, including its research questions, methodology, and the data it analyzes, and its connections to broader social science theories and real-world societal challenges. It will also explore how the study addresses the unique concerns and contributions of marginalized groups within the context of cybercrime, ultimately assessing the overall societal impact of the research.

Cybercrime in Social Science

The article is strongly rooted in social science while leaning on disciplines such as criminology, sociology, and psychology. It uses these disciplines more than the other because it focuses on the human element of cybercrime. This means that the study is less about the technical aspects of hacking or malware and more about the motivations, behaviors, and social contexts of individuals involved in cybercrime. The study applies these aspects of social sciences and its principles because it helps breakdown and analyze human behavior and motivation. These are elements to why an individual may choose to engage in cybercrime as many of these reasons can range from personal gain to general curiosity or just seizing the opportunity. It also analyzes social interaction and influence, such as peer pressure within online communities, and how these factors can normalize or encourage deviant online actions. Furthermore, the article touches upon deviance and social control by exploring how societal norms and laws are applied to digital spaces and how individuals respond to these regulations. This

approach highlights that cybercrime is not solely a technical problem, but a complex social phenomenon influenced by human behavior, motivation, and societal structures.

Research Questions and Methods

The study focuses on understanding the key factors that influence cybercrime behavior by asking several important research questions. Ones that stem from what motivates an individual to engage in cybercrime or how social factors influence or contribute to behaviors such as theses or also which groups are more likely to participate or be affected by cybercrime. Through these research questions the study proposed a hypothesis that furthermore suggested that individuals that engage in risky online behavior are most likely influenced by their peers or possess psychological traits that make them more likely to act in cybercrime. Thus, the independent variable would be factors such as online activity, peer influence, and personal traits. While the dependent variable is the level of involvement in cybercrime. The study then examined these relationships as the study uses quantitative research methods in the form of a survey to best collect data from the participants about their personal online experiences and behavior. Then the data is analyzed using statistical techniques to identify patterns and help determine how the independent variable influences cybercrime behavior.

Data and Analysis

The study uses primarily quantitative as discussed before to more accurately understand the data and cybercrime behavior. The data was collected through a survey where participants report their personal experiences and online activities. Doing this can help us understand attitudes and possible involvement that relate to cybercrime. Thus, the data is the main source of information, as it is gathered directly from everyone for the study. In another case, the researcher also conducted a second source of information through data of crime statistics to help support, analyze, and compare findings. Therefore, to analyze the data, the researcher applies statistical methods that include percentages that help average and summarize the info in addition to techniques that further help examine the data in relation

to independent and dependent variables. These methods help researchers identify patterns which helped determine which factors would be the most important or which ones would associate with cybercrime the best. Through this drawing, a conclusion on the several different factors that contribute to online criminal behavior.

Connection to Class Material

The study strongly connects with source concepts of cybercriminal subculture and empiricism. Both help explain and support its findings on cybercrime behavior. The idea of a cybercriminal subculture refers to online groups or communities where criminal behavior is shared, learned, and sometimes encouraged. The article reinforces this concept by showing that cybercrime is not only an individual act but can also be influenced by social environments in digital spaces. Individuals may learn hacking techniques, fraud methods, or deviant attitudes through interaction in online communities where such behavior is normalized. This supports the course idea that crime can be socially learned and sustained through group values, even in virtual environments. The study also reflects the principle of empiricism, which emphasizes that knowledge should be based on observable evidence and systematic data collection. The article reinforces this concept by using research methods such as surveys and statistical analysis to examine cybercrime behavior. Instead of relying on assumptions, the study gathers real-world data from participants to identify patterns, relationships, and contributing factors. This strengthens the validity of its findings and aligns with the scientific approach taught in the course.

Relation to Marginalized Groups

The topic of cybercrime is closely connected to the experience of marginalized groups. These groups of people are more at risk of unique challenges within the digital space. For example,

marginalized communities often face higher rates of cyber victimization, such as online harassment and scams, due to existing societal inequalities that are amplified online. Furthermore, marginalized groups may have less access to cybersecurity resources or education, making them more vulnerable. This underrepresentation and vulnerability also lead to underreporting cybercrimes, as these individuals may distrust law enforcement or lack awareness of available support systems. However, these communities also play a vital role in advocating better cyber safety policies and contributing to awareness campaigns, demonstrating their resilience and agency in the face of digital threats. Their contributions highlight the need for inclusive cybersecurity strategies that address the specific needs and concerns of all community members.

Overall Contributions to Society.

In conclusion, the study makes numerous relevant and important contributions to society by enhancing our understanding of cybercrime's social and psychological underpinnings. It provides valuable insights that can inform policy development, law enforcement strategies, and public awareness campaigns aimed at mitigating online risks and promoting safer digital practices. Furthermore, by highlighting the intersection of cybercrime with marginalized groups, the study contributes to a more equitable approach to digital safety and policy making, ensuring that vulnerable populations are adequately protected and included in societal efforts to combat online threats. The interdisciplinary nature of the research, drawing from criminology, sociology, and psychology, also fosters a more holistic approach to addressing this complex issue. This comprehensive understanding is crucial for developing effective strategies to combat cybercrime and ensure a safer digital environment for everyone. Ultimately, the study's contributions lie in its ability to bridge theoretical knowledge with practical applications, offering a roadmap for future research and interventions in the ever-evolving landscape of cybercrime.

References

Ghaleb, M. M. S., & Sattarov, A. (2025). *Perceived security risks and cybersecurity compliance attitude: Role of personality traits and cybersecurity behavior*. *International Journal of Cyber Criminology, 19*(1), 27–53. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/438/124

Footnotes

[1]For APA reports, add footnotes manually on their own page following references. Do not use the **Insert Footnotes** method on the **References** tab as they will not be formatted correctly. For APA formatting requirements, it's easier to type your own footnote references and notes. To format a footnote reference, select the number and then, on the **Home** tab, in the **Styles** gallery, click **Footnote Reference**. The body of a footnote, such as this example, uses the **Normal** text style. If you delete this sample footnote, don't forget to delete its in-text reference at the end of the sample Heading 2 paragraph on the first page of body content in this template.

Tables

Table 1

Table Title

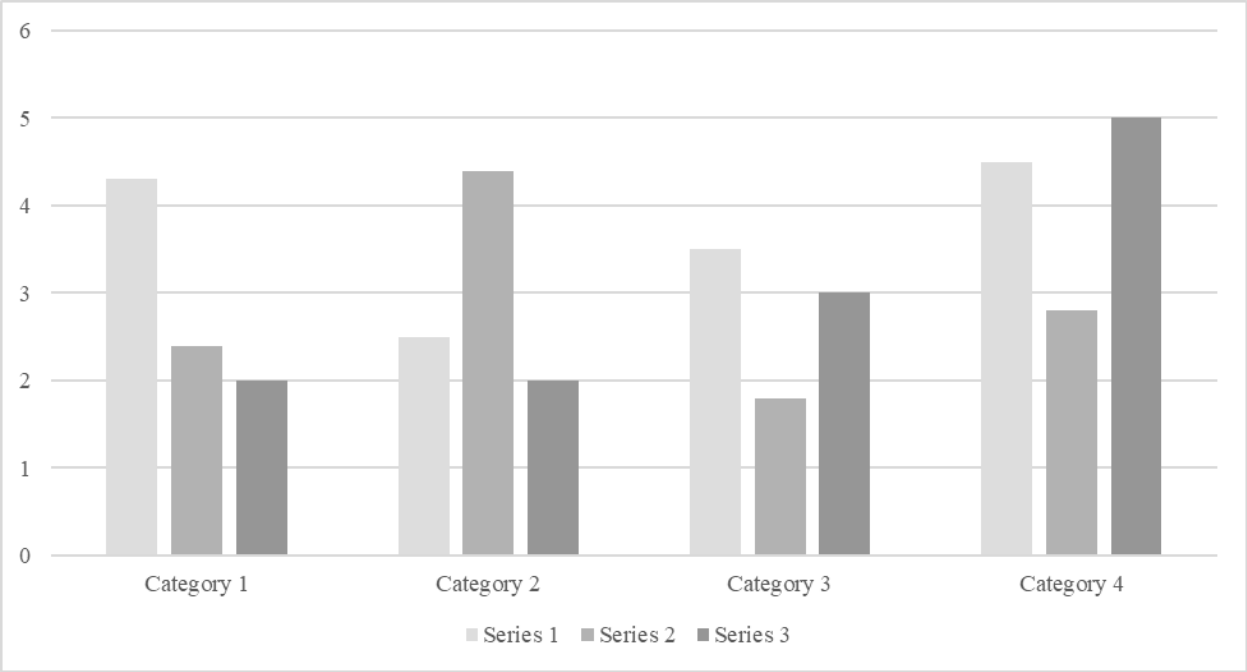
Column Head	Column Head	Column Head	Column Head	Column Head
Row Head	123	123	123	123
Row Head	456	456	456	456
Row Head	789	789	789	789
Row Head	123	123	123	123
Row Head	456	456	456	456
Row Head	789	789	789	789

Note: Place all tables for your paper in a tables section, following references and footnotes. Start a new page for each table, include a table number and table title for each, as shown. All explanatory text appears in a table note that follows the table, like this one. Use the **Table/Figure** style, available on the **Home** tab, in the **Styles** gallery, to get the spacing between table and note. Tables in APA format can use single or 1.5 line spacing. Include a heading for every row and column, even if the content seems obvious. A default table style has been set up for this template that fits APA guidelines. To insert a table, on the **Insert** tab, click **Table**.

Figures Title

Figure 1.

Include all figures in their own section, following references, footnotes, and tables. Include a numbered caption for each figure. Use the Table/Figure style for easy spacing between figure and caption.



For additional information on APA Style formatting, please consult the APA Style Manual, 7th Edition.