Cybersecurity Awareness, and Cybersecurity Behavior of High School Students in Davao City: A Mediation Role of Perceived Behavioral Control

Neil Bryan B. Booc
Graduate School Department, School of Teacher Education, Faculty, Holy Cross of Davao College, Davao City, Philippines

Kenneth Budiongan
Graduate School Department, Holy Cross of Davao College, Davao City, Philippines

Ramil Carballo
Graduate School Department, Holy Cross of Davao College, Davao City, Philippines

ABSTRACT:
This study aims to determine the mediating effect of perceived behavioral control in the relationship between cybersecurity awareness and cybersecurity behavior of high school students in Davao City, Philippines drawing on the Theory of Planned Behavior (TPB). Using a quantitative approach, data were collected through a survey questionnaire distributed to 100 high school students in a private school in Davao City. Established measures were used to assess cybersecurity awareness, perceived behavioral control, and cybersecurity behavior, with strict adherence to ethical considerations and data confidentiality. The study discovered a significant positive correlation among students' cybersecurity awareness, perceived behavioral control, and cybersecurity behavior. Both awareness and perceived control were found to be strong predictors of cybersecurity behavior, indicating that students with higher awareness and confidence in their abilities are more likely to engage in positive cybersecurity practices. These findings underscore the importance of educational efforts in promoting cybersecurity behavior among high school students. By enhancing cybersecurity awareness and promoting a sense of control among students, educators, and policymakers can better prepare them to navigate the digital landscape safely. Future research should explore the effectiveness of different educational interventions and assess their long-term impacts on students' cybersecurity behavior.

Keywords: Cybersecurity awareness, perceived behavioral control, cybersecurity behavior, high school students, theory of planned behavior, Davao City, Philippines.

INTRODUCTION
Cybersecurity issues can have widespread and significant impacts on various aspects of individuals. Junior high school students should not overlook the importance of cybersecurity, as this can lead to serious problems. If they do not create strong passwords, their personal information could be easily accessed by others. Not keeping their software updated may result in their devices being vulnerable to viruses [1]. If they are not careful about the websites they visit, they could accidentally download...
harmful software. Not being cautious with personal information online might lead to identity theft. And, if they do not log out of accounts on shared computers, someone else might access their private information [2]. It can compromise the national security and privacy of individuals. A study found that while internet users understand cyber threats well, they often fail to take adequate protective measures [3][4]. Moreover, despite increased risk perception at the University of Michigan, low baseline concerns about cybersecurity and the resistance to change in online behavior [5]. The Midwestern region of the United States adds to this by suggesting that individual differences in personality and risk-taking behavior can also predict cybersecurity behaviors [6]. These findings underscore the need for more effective cybersecurity training programs that take into account the interplay between knowledge, behavior, and personal characteristics. In the Philippines has one study highlighted the need for improved cybersecurity awareness and practices among the population [7][8]. These findings underscore the importance of targeted education and training programs to enhance cybersecurity behavior in the not only Philippines but internationally.

Statement of the Problem
The primary goal of this research is to explore and answer the following questions:

1. What is the level of cybersecurity awareness, perceived behavioral control, and cybersecurity behavior of high school students?

2. Is there a significant relationship between cybersecurity awareness and perceived behavioral control of the cybersecurity behavior of high school students?

3. Is there a mediating effect of perceived behavioral control in the relationship between cybersecurity awareness and cybersecurity behavior of high school students?

Hypotheses
The result will be tested at 0.05 and 0.01 alpha level:

H₀₁: There is no significant relationship between cybersecurity awareness and perceived behavioral control of the cybersecurity behavior of high school students.

H₀₂: There is no mediating effect of perceived behavioral control in the relationship between cybersecurity awareness and cybersecurity behavior of high school students.

Theory
This theory is anchored in the Theory of Planned Behavior (TPB), developed by Icek Ajzen (1991). Effective in cybersecurity, TPB examines the link between knowledge of cyber threats, attitudes towards cybersecurity measures, and individuals’ perceived control in implementing these measures. “Attitudes, social norms, and perceived control are all important factors in shaping cybersecurity behavior, with perceived control being particularly influential” [10][11].

METHODS
This research utilized a non-experimental quantitative design using a descriptive-correlational approach with mediating effect analysis. The method used for collecting data in this study is simple random sampling, in which 100 random high school students are given an adopted survey questionnaire [9]. A questionnaire is a research instrument composed of a list of questions for the respondents. This survey will be used to ask students how they would respond to specific security-related questions and situations. In this study, ethical consideration was given importance and thoroughly followed. The researchers used mean, Pearson-R, and mediating analysis to analyze the data.

RESULTS AND DISCUSSION
This section presented the results of the statistical analysis. A detailed discussion follows the presentation of results to provide meaning and implication to numerical data.
SOP 1. What is the level of cybersecurity awareness, perceived behavioral control, and cybersecurity behavior of high school students?

Table 1. Level of Cybersecurity Awareness Perceived Behavioral Control, and Cybersecurity Behavior of High School Students

<table>
<thead>
<tr>
<th>Variables</th>
<th>Mean</th>
<th>Descriptive Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Awareness</td>
<td>3.61</td>
<td>High</td>
</tr>
<tr>
<td>Perceived Behavioral Control</td>
<td>3.64</td>
<td>High</td>
</tr>
<tr>
<td>Cybersecurity Behavior</td>
<td>3.27</td>
<td>Average</td>
</tr>
<tr>
<td>Overall</td>
<td>3.51</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 1 shows the level of cybersecurity awareness of high school students with M = 3.61 and a high descriptive level. This suggests that high school students nowadays have a high level of awareness of their cybersecurity. The perceived behavioral control of students has M = 3.64, with a descriptive level of High. This suggests that high school students generally believe they have a high level of control over their behavior in their cybersecurity both online and offline, both in terms of their efficacy and the perceived controllability of the situation. In terms of cybersecurity behavior, students have M = 3.27 with an average descriptive level. This means that students fall within an average level in terms of their cybersecurity behavior. With an overall M = 3.51, the overall descriptive level is rated as high, indicating that high school students exhibit a high level of cybersecurity awareness, perceived control, and behavior, though there is still some room for enhancement in cybersecurity behavior. While internet users generally possess adequate cyber threat awareness, they often apply minimal protective measures, with different behavior across countries [3].

SOP 2. Is there a significant relationship between cybersecurity awareness and perceived behavioral control of the cybersecurity behavior of high school students?

Table 2. Significance of the Relationship Between Cybersecurity Awareness and Cybersecurity Behavior Among High School Students

<table>
<thead>
<tr>
<th>Cybersecurity Awareness</th>
<th>Cybersecurity Behavior</th>
<th>r</th>
<th>p-value</th>
<th>Decision H₀</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>.632</td>
<td>.000</td>
<td>Reject</td>
<td>Significant</td>
</tr>
</tbody>
</table>

Note: *p < 0.01

The significant relationship between cybersecurity awareness and cybersecurity behavior among high school students is reflected in Table 2. The result exhibits that the relationship between cybersecurity awareness and cybersecurity behavior among high school students exists with an overall p-value of 0.000, hence significant at 0.01 alpha significance level. Thus, the null hypothesis is rejected. Moreover, looking at the overall correlation coefficient, the computed r of 0.632, it shows that there is a moderate positive correlation between cybersecurity awareness and cybersecurity behavior. In practical terms, it suggests that individuals who are more aware of cybersecurity concerns tend to exhibit more secure behaviors in cyberspace.

A study suggests a need for increased or maintained education, information drive, and awareness-raising activities to help students better understand the various forms of cybercrime and the associated risks [12]. On the contrary, studies found that while internet users understand cyber threats, they often fail to take adequate protective measures [3][4].

Table 3. Significance on the Relationship Between Perceived Behavioral Control and Cybersecurity Behavior Among High School Students

<table>
<thead>
<tr>
<th>Perceived Behavioral Control</th>
<th>Cybersecurity Behavior</th>
<th>r</th>
<th>p-value</th>
<th>Decision H₀</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>.616</td>
<td>.000</td>
<td>Reject</td>
<td>Significant</td>
</tr>
</tbody>
</table>

Note: *p<.01
The significant relationship between perceived behavior control and cybersecurity behavior among high school students is also shown in Table 3. It was also found that there is a significant relationship between perceived behavior and cybersecurity behavior or a moderate positive connection, with a number ($r = 0.616$, $p = 0.000 < 0.01$). This finding also suggests that a higher level of perceived behavior in terms of self-efficacy and controllability will again adopt positive cybersecurity behavior of high school students. We can say that individuals who perceive a greater sense of control over their cybersecurity behavior are more likely to engage in cybersecurity practices or behaviors.

A study suggests that highly motivated employees with high severity, vulnerability, response efficacy, and self-efficacy exercise cybersecurity enhance the understanding of cybersecurity behavior’s role in addressing cybersecurity threats [13]. A study highlighted the influence of cyber security perception on attitudes towards using a learning management system, moderated by Internet security awareness [14].

SOP 3: Is there a mediating effect of perceived behavioral control in the relationship between cybersecurity awareness and cybersecurity behavior of high school students?

Table 3. Mediating Effect of Perceived Behavioral Control in the Relationship Between Cybersecurity Awareness and Cybersecurity Behavior of High School Students

<table>
<thead>
<tr>
<th></th>
<th>Estimate</th>
<th>Std. Error</th>
<th>p-val</th>
<th>Decision on $H_0$</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>PB → CB</td>
<td>.274</td>
<td>.076</td>
<td>&lt;.001</td>
<td>Reject</td>
<td>Significant</td>
</tr>
<tr>
<td>CA → CB</td>
<td>.384</td>
<td>.094</td>
<td>&lt;.001</td>
<td>Reject</td>
<td>Significant</td>
</tr>
<tr>
<td>CA → PB</td>
<td>.818</td>
<td>.093</td>
<td>&lt;.001</td>
<td>Reject</td>
<td>Significant</td>
</tr>
</tbody>
</table>

Legend: CA – Cybersecurity Awareness, PB – Perceived Behavior Control, CB – Cybersecurity behavior

As shown in Table 3, the effect of perceived behavior control on cybersecurity behavior has an estimated value of 0.274, a standard error of 0.076, and a p-value of <0.01. This means that there is a significant effect of perceived behavior control of high school students on their cybersecurity behavior. Moreover, the effect of cybersecurity awareness on cybersecurity behavior has an estimated value of 0.384, a standard error of 0.094, and a p-value of <0.01. This means that there is a significant effect of cybersecurity awareness of high school students on their cybersecurity behavior. Also, cybersecurity awareness significantly influences the perceived behavioral control of students. There is a 0.818 unit increase in the effect of cybersecurity awareness on perceived behavior control. Overall, there is a partial mediating effect of perceived behavioral control in the relationship between cybersecurity awareness and cybersecurity behavior of high school students. It is shown in the path analysis in Figure 1.
Moreover, there is a mediating effect of perceived behavior control on cybersecurity awareness and cybersecurity behavior of high school students. This suggests that perceived behavior control partially mediates the relationship between cybersecurity awareness and cybersecurity awareness. This means that while there is a significant direct effect of cybersecurity awareness and cybersecurity awareness, part of the relationship is also explained by the mediator effect of perceived behavior control.

The provided results align with the Theory of Planned Behavior (TPB). Increased cybersecurity awareness leads to higher perceived behavior control, akin to a positive attitude toward cybersecurity behavior. While not explicitly mentioned, perceived behavior control can encompass social influence, reflecting subjective norms [9]. Research consistently shows that perceived behavior control is a key determinant of cybersecurity behavior among high school and college students [10] [15] [16]. This aligns with the Theory of Planned Behavior (TPB), which emphasizes the role of perceived control in shaping behavior. Specifically, higher perceived control is associated with better cybersecurity behavior, while perceived vulnerability to cybersecurity risks can also influence behavior [17].

CONCLUSION

Based on the results and discussions, it can be concluded that high school students generally demonstrate a high level of cybersecurity awareness, perceived behavioral control, and cybersecurity behavior. However, there remains room for improvement, particularly in enhancing cybersecurity behavior. Furthermore, the study reveals a significant and moderate positive relationship between cybersecurity awareness and cybersecurity behavior, indicating that as awareness increases, so does responsible cybersecurity behavior. Additionally, a significant relationship exists between perceived behavioral control and cybersecurity behavior, suggesting that students who feel more control over their cybersecurity actions tend to exhibit better cybersecurity behavior. Moreover, the findings highlight the mediating effect of perceived behavioral control in the relationship between cybersecurity awareness and cybersecurity behavior. This suggests that perceived behavioral control plays a crucial role in influencing how cybersecurity awareness translates into actual behavior among high school students.

RECOMMENDATIONS

Based on mediation analysis, stakeholders can enhance cybersecurity behavior outcomes in high school students by prioritizing interventions targeting perceived behavior control and strengthening its influence on cybersecurity awareness and cybersecurity behavior relationships. This involves providing training, resources, or support to improve PB. Additionally, an integrated approach can be adopted addressing both direct and indirect pathways. This could involve designing interventions that simultaneously target cybersecurity awareness and perceived behavior control to maximize effectiveness. However, challenges such as resource constraints and resistance to change may arise. To overcome these, tailored interventions should be implemented, anticipating and addressing resistance through stakeholder engagement and education. Monitoring should focus on short-term goals while evaluating sustained impact in the long term, ensuring interventions effectively address challenges and lead to improved outcomes. Further research could explore additional mediators or moderators to better understand the complex relationship between cybersecurity awareness and cybersecurity behavior.

CONFLICT OF INTERESTS

No conflict of interest.
REFERENCES


