ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr2024

Assessment of Cybersecurity Awareness and Data Protection Practices Among Remote Virtual Assistants

Romer M. Real[1]; Kristine T. Soberano[2]

[1;2]State University of Northern Negros, Philippines

Publication Date: 2026/05/13

Abstract: Cybersecurity has become a critical concern in modern digital work environments where sensitive information is routinely exchanged through online platforms. Virtual assistants (VAs), who perform administrative, operational, and technical tasks remotely, frequently handle confidential data such as financial records, client databases, and internal communications. Despite their growing presence in the digital labor market, limited research has examined cybersecurity awareness and data protection behaviors among virtual assistants.

This study aimed to assess cybersecurity awareness and examine its influence on data protection practices among remote virtual assistants. A quantitative cross-sectional survey design was used, with data collected from 232 virtual assistants through an online questionnaire. The study measured cybersecurity awareness, security training, and data protection practices using a five-point Likert scale. Data were analyzed using descriptive statistics, Pearson correlation, and multiple regression analysis. Results showed that cybersecurity awareness (M = 3.14) and data protection practices (M = 3.13) were at a moderate level. A strong positive relationship was found between cybersecurity awareness and data protection practices (r = 0.60), while security training showed a moderate relationship (r = 0.34). The findings suggest that improving cybersecurity awareness plays a significant role in enhancing secure practices among virtual assistants. Regression results further confirmed that cybersecurity awareness is a significant predictor of data protection practices. The regression model explained 41.6% of the variance in data protection practices.

Keywords: *Cybersecurity Awareness; Data Protection; Information Security; Remote Work; Virtual Assistant*

How to Cite: Romer M. Real; Kristine T. Soberano (2026) Assessment of Cybersecurity Awareness and Data Protection Practices Among Remote Virtual Assistants. *International Journal of Innovative Science and Research Technology*, 11(4), 4417-4420. https://doi.org/10.38124/ijisrt/26apr2024

I. INTRODUCTION

The rapid growth of remote work has significantly changed how organizations operate and communicate. With the help of cloud computing, digital platforms, and online collaboration tools, companies are now able to work with teams located in different parts of the world. One of the roles that has become more common in this setup is the virtual assistant (VA), who provides administrative, operational, and sometimes technical support remotely.

Because of the nature of their work, virtual assistants often handle sensitive information such as client databases, financial records, internal communications, and confidential project files. This positions them as an important component of maintaining data security. However, working outside a controlled office environment also exposes them to various cybersecurity risks, including phishing attacks, malware, data breaches, and unauthorized access to systems.

Cybersecurity awareness refers to an individual's understanding of online threats and the actions needed to prevent them (Bada et al., 2019; Hadlington, 2017). People who are more aware of these risks are generally more careful in their behavior (Ng et al., 2009), such as using strong passwords, avoiding suspicious links, and following secure communication practices. In remote work settings, where there is less direct supervision and fewer centralized security controls, this awareness becomes even more important (Parsons et al., 2014).

In addition to awareness, security training also plays a key role in shaping how individuals respond to cybersecurity risks. Organizations often provide training programs to help workers recognize threats like phishing and social engineering. Previous studies have shown that individuals who receive cybersecurity training are more likely to follow security policies and adopt safer practices (Ifinedo, 2012; Siponen et al., 2010; Herath & Rao, 2009).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr2024

Despite the growing number of virtual assistants in the digital workforce, there is still limited research that focuses specifically on their cybersecurity awareness and data protection practices in remote work environments. Most existing studies focus on traditional office-based employees, which creates a gap in understanding how independent remote workers manage digital security risks (Posey et al., 2015).

This study aims to address this gap by examining the level of cybersecurity awareness and data protection practices among remote virtual assistants, as well as the role of security training in influencing their behavior. Organizational security culture also plays a role in influencing secure behavior among remote workers (D'Arcy & Greene, 2014).

II. OBJECTIVES

The general objective of this study is to assess cybersecurity awareness and examine data protection practices among remote virtual assistants.
Specifically, the study aims to:

- Determine the level of cybersecurity awareness among virtual assistants.
- Determine the level of security training exposure among virtual assistants.
- Determine the level of implementation of data protection practices.
- Examine the relationship between cybersecurity awareness and data protection practices.
- Examine the relationship between security training and data protection practices.
- Determine whether cybersecurity awareness and security training significantly predict data protection practices.

III. MATERIALS AND METHODS

A. Research Design

This study employs a quantitative cross-sectional survey design to examine the relationships between cybersecurity awareness, security training, and data protection practices among virtual assistants.

B. Participants

The participants consisted of remote virtual assistants recruited from freelancer communities and professional virtual assistant networks. Participants had at least six months of experience working remotely.

C. Respondent Profile

The demographic profile of the respondents includes age, sex, educational attainment, work setup, and years of experience as virtual assistants. The respondents represent a diverse group of remote workers, reflecting the varied nature of the virtual assistant industry.

D. Sampling Technique

A purposive sampling method is used to recruit respondents who meet the study criteria. Recruitment is conducted through online remote work forums and social media groups dedicated to virtual assistants.

E. Data Collection Procedure

Data were collected through an online questionnaire distributed using a secure digital survey platform. Participants were informed of the study's purpose and assured of confidentiality before completing the survey.

F. Ethical Considerations

Participants were informed about the purpose of the study prior to data collection. Participation was voluntary, and respondents had the option to withdraw at any time. No personally identifiable information was collected, and all responses were kept confidential and used solely for academic purposes.

G. Research Instruments

Three measurement scales are used in the study:

- Cybersecurity Awareness Scale - Measures knowledge of cybersecurity threats and security practices.
- Security Training Scale - Measures participants' exposure to cybersecurity training programs.
- Data Protection Practices Scale - Measures implementation of protective behaviors including:

✓ Password management
✓ Two-factor authentication
✓ Secure file storage
✓ Encrypted communication

All items are measured using a five-point Likert scale.

H. Reliability Testing

Reliability testing was conducted using Cronbach's Alpha to assess the internal consistency of the measurement scales.

Table 1. Reliability Testing Results

Scale	Cronbach's Alpha	Interpretation
Cybersecurity Awareness	0.53	Acceptable
Security Training	0.41	Moderate
Data Protection Practices	0.65	Acceptable

The results showed that cybersecurity awareness ($\alpha = 0.53$) and data protection practices ($\alpha = 0.65$) demonstrated acceptable reliability, while security training ($\alpha = 0.41$) showed moderate reliability. These results indicate that the instrument is suitable for exploratory research.

I. Data Analysis

Data were analyzed using descriptive statistics to determine the overall levels of cybersecurity awareness, security training, and data protection practices. Pearson correlation analysis was used to examine the relationships between variables, while multiple regression analysis was

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr2024

applied to determine the predictive influence of cybersecurity awareness and security training on data protection practices.

IV. RESULTS AND DISCUSSION

A. Results

A total of 232 virtual assistants participated in the study. This sample size was considered sufficient for statistical analysis. Descriptive statistics were used to determine the levels of cybersecurity awareness, security training, and data protection practices.

The results showed that cybersecurity awareness had a mean score of 3.14, security training had a mean score of 3.10, and data protection practices had a mean score of 3.13, indicating moderate levels across all variables.

The mean scores were interpreted using a five-point Likert scale, where higher values indicate greater levels of awareness, training, and implementation of data protection practices.

Pearson correlation analysis revealed a strong positive relationship between cybersecurity awareness and data protection practices (r = 0.60). Security training showed a moderate positive relationship with data protection practices (r = 0.34). A weaker relationship was observed between cybersecurity awareness and security training (r = 0.27).

The results are summarized in Tables 2 and 3.

Table 2. Descriptive Statistics

Variable	Mean	Interpretation
Cybersecurity Awareness	3.14	Moderate
Security Training	3.10	Moderate
Data Protection Practices	3.13	Moderate

Table 3. Correlation Matrix

Variables	Awareness	Training	Practices
Awareness	1.00	0.27	0.60
Training	0.27	1.00	0.34
Practices	0.60	0.34	1.00

➢ *Multiple Regression Analysis*

Multiple regression analysis was conducted to determine the predictive influence of cybersecurity awareness and security training on data protection practices.

Table 4. Multiple Regression Analysis

Variables	Awareness	Training	Practices
Cybersecurity Awareness	0.457	8.94	$p < 0.001$
Security Training	0.249	4.52	$p < 0.001$

The model was statistically significant ($F = 81.63$, $p < 0.001$) and explained 41.6% of the variance in data protection practices ($R^2 = 0.416$). Cybersecurity awareness was found to be a strong predictor ($\beta = 0.457$, $p < 0.001$), while security training also showed a significant but weaker effect ($\beta = 0.249$, $p < 0.001$).

B. Discussion

These findings are consistent with the Theory of Planned Behavior, which suggests that awareness and attitudes significantly influence behavioral outcomes (Ajzen, 1991). The strong positive relationship between awareness and practices suggests that individuals who are more knowledgeable about cybersecurity risks are more likely to implement secure behaviors in their work. This is consistent with previous studies (Parsons et al., 2014), which highlight that higher awareness leads to better compliance with security practices.

On the other hand, security training showed only a moderate relationship with data protection practices. This may suggest that training alone is not always sufficient and that its effectiveness depends on how well it is applied in real-world situations. Some virtual assistants may rely more on experience or self-learning rather than formal training.

Overall, the results emphasize the importance of strengthening cybersecurity awareness alongside training to improve data protection practices in remote work environments. This suggests that awareness-based interventions may be more effective than traditional training programs in improving cybersecurity behavior among remote workers.

This highlights the need for more practical and experience-based cybersecurity learning approaches rather than relying solely on formal training programs. Industry reports also emphasize that human factors remain one of the leading causes of data breaches, highlighting the importance of user awareness in cybersecurity (Verizon, 2023).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr2024

V. CONCLUSION AND RECOMMENDATION

A. Conclusion

The study found that cybersecurity awareness has a strong influence on data protection practices among virtual assistants, while security training shows a moderate effect. These findings suggest that increasing awareness is essential in promoting secure behavior in remote work environments. Virtual assistants who are more knowledgeable about cybersecurity risks are more likely to apply protective measures when handling sensitive information.

B. Recommendation

Based on the findings of the study, it is recommended that organizations provide continuous cybersecurity awareness programs to virtual assistants. Training programs should be practical and regularly updated to address current threats. Virtual assistants are also encouraged to adopt best practices such as using strong passwords, enabling two-factor authentication, and verifying information before sharing sensitive data. Future studies may explore additional factors that influence cybersecurity behavior in remote work settings.

REFERENCES

[1]. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.
[2]. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.
[3]. D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security, 22(5), 474–489.
[4]. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346.
[5]. Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations. Information Systems Research.
[6]. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95.
[7]. Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825.
[8]. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire. Computers & Security.
[9]. Posey, C., Roberts, T., & Lowry, P. B. (2015). The impact of organizational commitment on cybersecurity behavior. Journal of Management Information Systems.
[10]. Siponen, M., Pahnila, S., & Mahmood, A. (2010). Compliance with information security policies: An empirical investigation. Computer, 43(2), 64–71.
[11]. Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Enterprise.