International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

The relationship between cybersecurity awareness and secretaries' job performance in university of Ibadan

Basit Adebayo. Waheed [1,*], Virginia Ochanya Onche [2] and Oluwatoyin Omotayo Oguntayo [3]

[1] *Division of Senate, Admissions and Affiliated Institutions, University of Ibadan, Nigeria.*
[2] *Department of Educational Management, Faculty of Education, University of Ibadan, Nigeria.*
[3] *Department of Office Technology and Management, Faculty of Business and Communication Studies, The Polytechnic, Ibadan, Nigeria.*

International Journal of Science and Research Archive, 2025, 16(01), 662-674

Publication history: Received on 31 May 2025; revised on 05 July 2025; accepted on 08 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2068

Abstract

This study examines the relationship between cybersecurity awareness and secretaries' job performance at the University of Ibadan, focusing on four key objectives: assessing the level of job performance, evaluating cybersecurity awareness, exploring the relationship between the two variables, and determining the impact of cybersecurity awareness on job performance. A descriptive survey design was adopted, utilizing total enumeration sampling of 80 secretaries. Data were collected using a structured questionnaire on a 4-point Likert scale, validated through content validity, and tested for reliability with Cronbach Alpha coefficients ranging from 0.823 to 0.973. Descriptive and inferential statistics, including Pearson correlation and regression analysis, were employed for data analysis. Findings revealed a generally high level of job performance (mean = 3.67) and a moderately high level of cybersecurity awareness (mean = 3.66). The study established a very strong positive correlation (r = 0.938, p = 0.000) between cybersecurity awareness and job performance, indicating that secretaries with higher cybersecurity awareness tend to perform better. Regression analysis further demonstrated that cybersecurity awareness significantly impacts job performance, accounting for 88% of the variance (R^2 = 0.880). The t-value (23.920) and p-value (0.000) confirmed the statistical significance of this impact. The study concludes that cybersecurity awareness is a critical factor in enhancing secretaries' job performance, though other variables may also contribute. It recommends regular training on cybersecurity practices, improved access to reliable security tools, and integration of cybersecurity awareness into professional development programs to address emerging threats and maintain high performance levels. These findings underscore the importance of fostering a culture of cybersecurity to optimize secretarial roles in the digital era.

Keywords: Cybersecurity; Awareness Secretaries; Job Performance; Cybercrime; Cyerstalking

1 Introduction

Modern organizations rely heavily on digital platforms and systems for daily operations, increasing their vulnerability to cybersecurity breaches. These breaches, which are becoming more frequent, have severe implications for organizations, the national economy, and security. The relationship between cybersecurity awareness and secretaries' job performance is significant, as enhanced awareness improves their ability to handle sensitive information responsibly (Nurse, 2021). Cybersecurity awareness training fosters a culture of security, enabling secretaries to effectively use digital tools in their tasks (Corradini, 2020). However, studies show that without proper training, the benefits of digital tools on job performance are limited. For instance, Oyerinde etal. (2023) found that secretaries in government offices did not significantly benefit from these devices due to inadequate training. Therefore, integrating

* Corresponding author: Basit A. Waheed

comprehensive cybersecurity training into secretaries' professional development is crucial for boosting performance and ensuring organizational security (Corradini, 2020; Oyerinde etal., 2023).

The International Telecommunications Union (ITU) explained that cybersecurity involves a combination of tools, policies, security frameworks, safeguards, guidelines, risk management strategies, actions, training, best practices, assurance measures, and technologies designed to secure the cyber environment and protect organizational and user assets. These assets include computing devices, personnel, infrastructure, applications, services, telecommunications systems, and all transmitted or stored information. The primary goals of cybersecurity are to uphold availability, integrity (including authenticity and non-repudiation), and confidentiality against cyber threats.

Cybersecurity awareness refers to an individual's understanding and ability to implement security practices while using internet networking sites. It involves recognizing the importance of safeguarding personal or organizational data when engaging with websites

For organizations, businesses, and individuals to protect themselves from potential cyberthreats, assaults, or disruptions in the current digital era, cybersecurity awareness and expertise are crucial. In order to lower risks and mitigate potential security breaches, it is essential to improve one's understanding of cybersecurity, including safeguarding data, preserving personal information, and assuring device safety through practices like using strong passwords.

Cybersecurity awareness is increasingly recognized as a critical component in mitigating cyber threats, particularly in organizational settings. The Integrated Cybersecurity Awareness Training (iCAT) model emphasizes innovative training methods, such as gamification and micro-learning, to enhance engagement and knowledge retention among participants (Taherdoost, 2024). Qualitative studies indicate that tailored training programs significantly improve employees' ability to recognize phishing attempts, although continuous reinforcement is necessary to maintain vigilance (Khan and Muntaha, 2024). Furthermore, research on students highlights the importance of understanding various cybersecurity aspects, including password security and data protection, revealing a correlation between educational background and awareness levels (Gardenia and Gani, 2024) (Nimkar and Kumar, 2024). The Cybersecurity Awareness Inventory (CAIN) serves as a reliable tool for assessing knowledge of cyber threats, demonstrating predictive validity about security behaviors (Nocera et al., 2024). Collectively, these studies underscore the necessity for adaptive, scenario-based training to foster a culture of cybersecurity awareness across diverse populations.

The importance of cybersecurity awareness in reducing cyberthreats is becoming more widely acknowledged, especially in corporate contexts. To improve participant engagement and knowledge retention, the Integrated Cybersecurity Awareness Training (iCAT) approach places a strong emphasis on cutting-edge training techniques, including gamification and microlearning (Taherdoost, 2024). According to a qualitative study, employees' capacity to identify phishing attempts is greatly enhanced by customized training programs; nonetheless, ongoing reinforcement is required to sustain alertness (Khan and Muntaha, 2024). Additionally, studies on students emphasize the significance of learning many cybersecurity facets, such as data protection and password security, and show a relationship between awareness levels and educational background (Gardenia and Gani, 2024) (Nimkar and Kumar, 2024). As a trustworthy instrument for evaluating awareness of cyberthreats, the Cybersecurity Awareness Inventory (CAIN) exhibits predictive validity with regard to security practices (Nocera et al., 2024).

2 Cybercrime

Cybercrime, according to Halder and Jaishankar (2011), is characterized as behaviors committed to harm a person or a group, either directly or indirectly, by causing bodily or psychological damage or by tarnishing their name. Modern telecommunication networks, including cell phones and the internet (such as chat rooms, emails, notice boards, and online groups), are used to facilitate these crimes.

Cybercrime significantly impacts secretaries in Nigeria, primarily through prevalent scams such as the infamous 419 scams, which have evolved with technological advancements. These scams often target individuals in administrative roles, exploiting their access to sensitive information and financial resources. Secretaries may receive fraudulent emails promising lucrative business opportunities or lottery winnings, employing persuasive language and emotional appeals to manipulate victims into providing personal information or funds (Falade, 2023) (Schaffer, 2012). The rise of phishing and identity theft further complicates the landscape, as cybercriminals increasingly use sophisticated tactics to deceive unsuspecting secretaries, leading to financial losses and reputational damage for organizations (Bello, 2017) (Afolabi and Esoso, 2021). The Nigerian government's struggle to combat cybercrime is compounded by socio-economic pressures, including widespread unemployment and poverty, which fuel the motivations for cyber offenses. This

highlights the urgent need for a coordinated strategy combining cybersecurity infrastructure, social reorientation, and economic reform (Afolabi & Esoso, 2021; Ojedokun & Eraye, 2012)

Cyberstalking is the term used to describe online harassment in which the victim is bombarded with messages, emails, or other correspondence from the perpetrator, who typically involves someone they know. Cyberstalking, as opposed to traditional offline stalking, uses technology, including the internet, email, text messages, websites, and webcams to instill dread and emotional distress in the victim. Harassment of this kind has the potential to turn into grave physical threats.

Spamming is the practice of haphazardly sending unsolicited, frequently commercial emails to a large Spamming is the practice of haphazardly sending unsolicited, frequently commercial emails to a large number of recipients. This can also apply to other platforms, such as blogs, web forums, mobile phones, and chat rooms. In addition to clogging inboxes, it may direct users to malicious websites that aim to steal private data, such as credit card numbers or login credentials. Typically, spam is used to promote questionable goods or services (Hazen, 2020; The Free Dictionary, n.d.).

Hacking occurs when an individual gains illegal access to a victim's computer system, frequently without the victim's knowledge, and uses techniques like IP spoofing or brute force attacks to take advantage of system flaws. To find new weaknesses and create programs for their illicit operations, hackers depend on a community (Monkshouts, 2019). Intellectual property theft involves the unlawful taking of a creator's intellectual property, like trademarks, intellectual property rights, and copyright. Software piracy and the unauthorised distribution of copyrighted works are frequent infractions (Jrank, 2021).

In an attempt to perpetrate fraud or theft, identity theft happens when someone illegally obtains another person's personal information, such as social security numbers or bank account information. The victim of this kind of cybercrime may suffer significant financial losses and have their credit reputation destroyed (FBI, 2021). Malicious software, sometimes known as malware, is developed to get infiltrate networks and potentially destroy systems or steal confidential information. This program frequently infiltrates a system to take advantage of weaknesses and interfere with regular operations (Monkshouts, 2019).

Predators target children in chat rooms to take advantage of them, which can result in child pornography (Helpline Law, n.d.). This is known as child soliciting and abuse online.

The term “cyberterrorism” emphasizes the use of the internet for terrorist purposes, such as widespread computer network disruptions and virus attacks to achieve political or social goals. The goal of this type of terrorism is to threaten or pressure governments and their populace (Denning, 2000).

2.1 Statement of the Problem

In the current digital era, cybersecurity has become a major concern for organizations globally, including educational institutions. As universities increasingly rely on digital systems and platforms for administrative and academic purposes, their vulnerability to cybersecurity threats has also risen. Secretaries, who are essential in managing sensitive information, communications, and data, are particularly exposed to this challenge. While cybersecurity awareness has gained significant attention in the corporate sector, where employees regularly undergo cybersecurity training, such awareness is less emphasized in government institutions. Despite the growing dependence on digital tools, secretaries in many government offices, including universities, often lack access to thorough cybersecurity training. This training gap is concerning, as a secretary’s ability to perform their duties effectively is closely tied to their knowledge and understanding of cybersecurity practices.

Objectives of the Study

The main objective of this study is to evaluate the relationship between Cybersecurity Awareness and Secretaries Job Performance in University of Ibadan. Sub objectives are to

- Know the level of Secretaries Job Performance in University of Ibadan
- Assess the level of cybersecurity awareness among secretaries in in University of Ibadan.
- Explore the relationship between cybersecurity awareness and Secretaries’ job effectiveness in University of Ibadan.
- Evaluate the impact of cybersecurity awareness on Secretaries’ job effectiveness in University of Ibadan.

2.2 Research Questions

- What is the level of Secretaries' Job Performance of Secretaries in University of Ibadan?
- What is the level of Cybersecurity Awareness among Secretaries in University of Ibadan?
- What is the relationship between Cybersecurity awareness and secretaries Job performance in University of Ibadan.
- What is the impact of Cybersecurity awareness on Secretaries Job Performance?

2.3 Research Hypotheses

- **H_{01}**: There is no relationship between Cybersecurity and Secretaries Job Performance in University of Ibadan
- **H_{02}**: Cybersecurity does not have any impact on Secretaries Job Performance in University of Ibadan

3 Methodology

The study adopted a descriptive survey design to investigate the relationship between cybersecurity awareness and secretaries' job performance at the University of Ibadan. Given the small population size, total enumeration sampling was employed, involving all 80 secretaries in the institution. Data were collected through a structured questionnaire designed on a 4-point Likert scale, with response options such as Very High (4), High (3), Low (2), Very Low (1), and Strongly Agree (4), Agree (3), Disagree (2), Strongly Disagree (1). Reliability status was confirmed using Cronbach Alpha, yielding coefficients of 0.928 for Secretaries' Job Performance, 0.973 for Cybersecurity Awareness, 0.823 for the relationship between Cybersecurity Awareness and Secretaries' Job Performance, and 0.973 for the Impact of Cybersecurity Awareness on Secretaries' Job Performance. Data analysis incorporated both descriptive and inferential statistics. Descriptive statistics, including frequency, percentage, mean, and standard deviation, were utilized to address Research Questions One and Two, which focused on determining the levels of secretaries' job performance and cybersecurity awareness, respectively. Pearson correlation was applied to Research Question Three to establish the relationship between cybersecurity awareness and secretaries' job performance. To evaluate the impact of cybersecurity awareness on job performance (Research Question Four), a One-Sample T-Test was employed. Hypotheses were tested using inferential methods, with Pearson correlation applied to Hypothesis One to assess the relationship between cybersecurity awareness and job performance, and regression analysis employed for Hypothesis Two to determine the significance of the impact of cybersecurity awareness on job performance.

3.1 Presentation of Data and Data Analysis

3.1.1 Research Questions

Table 1 Research Question One: What is the level of secretaries' job effectiveness in University of Ibadan?

S/N	Questions	Very High	High	Low	Very Low	Mean
	Information Management Efficiency					
1	What is your level of effectiveness in organizing and securing sensitive data using appropriate cybersecurity tools?	60 (75%)	14 (17.5%)	6 (7.5%)	0 (0%)	3.68
2	What is the level of your use encrypted storage or secure file-sharing platforms to manage sensitive information?	62 (77.5%)	14 (17.5%)	4 (5%)	0 (0%)	3.73
3	What is your level of reliance on backup systems to ensure the safety of critical data in case of a cyber threat?	58 (72.5%)	16 (20%)	6 (7.5%)	0 (0%)	3.65
	Average Mean for Information Management Efficiency					**3.69**
	Confidentiality and Discretion	**Very High**	**High**	**Low**	**Very Low**	**Mean**
4	What is your level of effectiveness ensuring confidentiality of sensitive information when communicating digitally (e.g., emails, cloud storage)?	58 (72.5%)	16 (20%)	6 (7.5%)	0 (0%)	3.65

5	At what level do you take measures to prevent unauthorized access to confidential data, such as using strong passwords and two-factor authentication?	60 (75%)	16 (20%)	4 (5%)	0 (0%)	3.70
6	How well do you follow organizational guidelines for handling confidential information, ensuring it's kept secure from cyber threats?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
	Average mean for Confidentiality and Discretion					**3.66**
	Crisis Management and Incident Response	**Very High**	**High**	**Low**	**Very Low**	**Mean**
7	What is your level of effectiveness in securing digital platforms to complete administrative tasks while ensuring data protection?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
8	What is your level of proficiency in using cybersecurity tools (e.g., VPNs, encrypted emails, anti-malware software) in your daily work	58 (72.5%)	16 (20%)	6 (7.5%)	0 (0%)	3.65
9	How comfortable are you in handling confidential data without compromising its security?	60 (75%)	16 (20%)	4 (5%)	0 (0%)	3.70
	Average mean for Confidentiality and Discretion					**3.66**
	Weighted mean for Secretaries Job Effectiveness					**3.67**

Decision rule 1.00 – 1.49=Very Low, 1.50 – 2.49=Low, 2.50 – 3.49= High, 3.50 – 4.00=Very High

From Table One above, it was discovered that cybersecurity awareness among respondents rated high level of proficiency across the three key dimensions: confidentiality, integrity, and availability, as indicated by the weighted mean score of 3.66, demonstrates. Notably, the strongest performance was observed in the integrity dimension, with a mean score of 3.70, highlighting respondents' confidence in ensuring data accuracy, reliability, and protection against unauthorized modifications. However, a small proportion of respondents rated their familiarity as low, particularly in areas such as understanding encryption methods and reporting system downtime. The findings reflect strong cybersecurity awareness, which enhances the respondents' effectiveness in maintaining secure, reliable, and accessible data systems.

3.1.2 Descriptive Statistic

Table 2 Descriptive Statistics of Research Question One: What is the level of secretaries' job effectiveness in University of Ibadan?

	N	**Mean**	**Std. Deviation**	**Skewness**		**Kurtosis**	
	Statistic	**Statistic**	**Statistic**	**Statistic**	**Std. Error**	**Statistic**	**Std. Error**
Level of Secretaries Job Performance	80	3.6667	0.47766	-1.335	0.269	0.829	0.532
Valid N (listwise)	80						

The level of secretaries' Job Performance at the University of Ibadan is generally positive, as indicated by the mean score of 3.67 out of 4. This suggests that, on average, secretaries perceive themselves to be effective in their roles. The standard deviation of 0.48 reveals that while most respondents rate their job performance highly, there is some variability in the responses, though not significantly. The negative skewness of -1.335 further supports this, showing that more respondents tend to rate their job performance positively, with fewer reporting lower levels of effectiveness. Additionally, the kurtosis value of 0.829 indicates a relatively flat distribution, meaning that the responses are spread out rather than tightly clustered around the mean. These findings suggest that secretaries at the University of Ibadan exhibit above-average job effectiveness, with a tendency toward more favorable ratings, but some variation exists in individual perceptions of their effectiveness.

Table 3 Research Question Two: What is the level of Cybersecurity awareness among secretaries?

	Confidentiality	**Very High**	**High**	**Low**	**Very Low**	**Mean**
10	How familiar are you with protecting sensitive data from unauthorized access?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
11	How would you rate your knowledge of encryption methods for securing confidential documents?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
12	How well do you understand the risks associated with sharing passwords or sensitive information with unauthorized personnel?	58 (72.5%)	16 (20%)	6 (7.5%)	0 (0%)	3.65
	Average mean for Confidentiality and Discretion					**3.64**
	Integrity	**Very High**	**High**	**Low**	**Very Low**	**Mean**
13	How confident are you in verifying the accuracy and authenticity of data before sharing or using it?	60 (75%)	16 (20%)	4 (5%)	0 (0%)	3.70
14	How well do you understand how to detect and prevent unauthorized changes to organizational data?	62 (77.5%)	14 (17.5%)	4 (5%)	0 (0%)	3.70
15	How familiar are you with methods to ensure the reliability and consistency of the data you handle?	60 (75%)	16 (20%)	4 (5%)	0 (0%)	3.70
	Average mean for Integrity					**3.70**
	Availability	**Very High**	**High**	**Low**	**Very Low**	**Mean**
16	How confident are you in identifying and reporting system downtime or potential cybersecurity breaches?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
17	How familiar are you with the importance of maintaining backups to ensure availability of important documents?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
18	How well do you understand strategies to ensure uninterrupted access to critical systems or files in your daily work?	60 (75%)	16 (20%)	4 (5%)	0 (0%)	3.70
	Weighted Mean for Availability					**3.65**
	Weighted Mean for Level of Cybersecurity Awareness					**3.66**

Decision rule 1.00 – 1.49=Very Low, 1.50 – 2.49=Low, 2.50 – 3.49= High, 3.50 – 4.00=Very High

The results of the survey reveal a strong overall level of cybersecurity awareness among respondents, as indicated by the average means and weighted mean across the key dimensions. For Confidentiality and Discretion, the average mean is 3.64, suggesting that respondents generally have a solid understanding of protecting sensitive data and managing risks related to unauthorized access and sharing. The Integrity dimension scored the highest, with an average mean of 3.70, demonstrating respondents' confidence in ensuring data accuracy, preventing unauthorized changes, and maintaining the reliability and consistency of the information they handle. In terms of Availability, the weighted mean is 3.65, reflecting respondents' strong competence in identifying and addressing system downtimes, recognizing the importance of backups, and ensuring uninterrupted access to critical files.

The weighted mean for cybersecurity awareness stands at 3.66, indicating a high level of competence across all three dimensions. This suggests that respondents are well-equipped to safeguard confidentiality, ensure the integrity of data, and maintain the availability of critical systems in their professional roles.

3.1.4 Descriptive Statistics

Table 4 Descriptive Statistics of Research Question Two: What is the level of Cybersecurity awareness among secretaries?

	N	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Cyber Security Awareness	80	3.6583	0.54684	-1.406	0.269	0.971	0.532
Valid N (listwise)	80						

The Level of cybersecurity awareness among secretaries at the University of Ibadan has a mean score of 3.66 (out of 4), indicating a moderately high level of awareness. The standard deviation of 0.55 indicates that, while most respondents report similar levels of cybersecurity awareness, there is some variability in their responses. The skewness value of -1.406 indicates a slight negative skew, meaning more respondents rated their cybersecurity awareness on the higher side, with fewer reporting low levels of awareness. The kurtosis value of 0.971 suggests a relatively normal distribution of responses, with a moderate concentration around the mean. In conclusion, the data indicate that secretaries at the University of Ibadan generally have a strong awareness of cybersecurity, but there are individual differences in the perceived level of awareness.

Table 5 Research Question Three: What is the relationship between Cybersecurity Awareness and Secretaries' Job performance in University of Ibadan?

	(Risk Management Framework) **Risk Identification**	**SA**	**A**	**D**	**SD**	**Mean**
19	I am aware of potential cybersecurity risks that could disrupt my job performance.	79 (98.8%)	1 (1.3%)	0 (0%)	0 (0%)	4.0
20	My ability to identify and report cybersecurity threats enhances my overall productivity at work.	80 (100%)	0 (0%)	0 (0%)	0 (0%)	4.0
21	I regularly apply cybersecurity best practices (e.g., avoiding phishing scams) to reduce risks in my daily tasks.	0 (0%)	34 (42.5%)	44 (55%)	2 (2.5%)	2.40
	Weighted Mean for Risk Identification					**3.47**
	Risk Assessment	**SA**	**A**	**D**	**SD**	**Mean**
22	Adhering to the University's cybersecurity policies positively impacts the efficiency of my job performance.	58 (72.5%)	18 (22.5%)	4 (5%)	0 (0%)	3.68
23	I believe that regular updates and compliance with security guidelines help me maintain optimal performance in my role	58 (72.5%)	18 (22.5%)	4 (5%)	0 (0%)	3.68
24	My knowledge of incident response protocols (e.g., reporting breaches or system failures) contributes to seamless task completion during security disruptions.	60 (75%)	14 (17.5%)	6 (7.5%)	0 (0%)	3.73
	Weighted Mean for Risk Assessment					**3.69**
	Risk Mitigation	**SA**	**A**	**D**	**SD**	**Mean**
25	Being prepared to recover from cybersecurity incidents (e.g., restoring lost data) improves my ability to meet job deadlines	62 (77.5%)	14 (17.5%)	4 (5%)	0 (0%)	3.73
26	Implementing multiple layers of security (e.g., passwords, firewalls, and antivirus) in my tasks boosts my confidence and job efficiency	58 (72.5%)	18 (22.5%)	4 (5%)	0 (0%)	3.65
27	Collaboration with IT staff and adherence to security protocols helps me complete tasks effectively without compromising cybersecurity standards.	58 (72.5%)	16 (20%)	6 (7.5%)	0 (0%)	3.65
	Weighted Mean Risk Mitigation					**3.68**
	Weighted mean for relationship between Cybersecurity Awareness and Secretaries Job performance in University of Ibadan					**3.61**

Decision rule 1.00 – 1.49=Strongly Disagree, 1.50 – 2.49=Disagree, 2.50 – 3.49= Agree, 3.50 – 4.00=Strongly Agree

The results show that respondents generally agree on the importance of cybersecurity in their roles. For Risk Identification, there is strong agreement on being aware of potential risks and the ability to report threats, though there is less agreement on consistently applying best practices, as seen in the lower mean score of 2.40. In terms of Risk Assessment, respondents strongly agree that adherence to cybersecurity policies and knowledge of incident response protocols enhance job performance, reflected in a mean score of 3.69. Similarly, for Risk Mitigation, respondents are in agreement about the value of preparedness, multiple security layers, and collaboration with IT staff, with a mean score of 3.68. The weighted mean of 3.61 suggests a moderate to strong belief in the positive relationship between cybersecurity awareness and secretaries' job performance, though there is room for improvement in the regular application of cybersecurity practices.

Table 6 Correlations for Research Question Three: What is the relationship between Cybersecurity Awareness and Secretaries Job performance in University of Ibadan?

		Level of Secretaries' Job Performance	**Cyber Security Awareness**
Level of Secretaries Job Performance	Pearson Correlation	1	0.938**
	Sig. (2-tailed)		0.000
	N	80	80
Cyber Security Awareness	Pearson Correlation	0.938**	1
	Sig. (2-tailed)	0.000	
	N	80	80

The correlation between Secretaries' Job Performance and Level of Cyber Security Awareness is 0.938, which indicates a very strong positive relationship between the two variables. This suggests that higher levels of cybersecurity awareness are closely associated with better job performance among secretaries. The correlation is statistically significant at the 0.01 level, as shown by the p-value of 0.000, meaning the relationship is highly unlikely to be due to chance. With a sample size of 80, this finding suggests that improving cybersecurity awareness could potentially enhance the job effectiveness of secretaries at the University of Ibadan.

Table 7 Research Question Four: What is the impact of Cybersecurity Awareness on Secretaries' Job Performance in University of Ibadan?

	Defense in Depth (Multi-Layered Security)	**Very High**	**High**	**Low**	**Very Low**	**Mean**
	Perimeter Security					
28	How effectively are firewalls implemented in your organization to monitor and control incoming and outgoing network traffic?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
29	How well do intrusion prevention systems (IPS) detect and prevent unauthorized access attempts in your network?	58 (72.5%)	16 (20%)	6 (7.5%)	0 (0%)	3.65
	Average Mean for Perimeter Security					**3.64**
	Endpoint Security	**Very High**	**High**	**Low**	**Very Low**	**Mean**
30	How has implementing cybersecurity best practices (e.g., secure passwords, avoiding suspicious links) has improved my overall productivity?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63

31	What is the level at which Cybersecurity awareness gives me the confidence to handle sensitive organizational data securely?	60 (75%)	16 (20%)	4 (5%)	0 (0%)	3.70
	Average Mean for Endpoint Security					**3.67**
	Data Security	**Very High**	**High**	**Low**	**Very Low**	**Mean**
32	How effectively are encryption protocols implemented in your organization to safeguard sensitive data?	62 (77.5%)	14 (17.5%)	4 (5%)	0 (0%)	3.73
33	How frequently do you perform secure backups of critical organizational data?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
	Average Mean for Data Security					**3.68**
	Human Layer	**Very High**	**High**	**Low**	**Very Low**	**Mean**
34	How confident are you in recognizing and responding to suspicious emails, calls, or messages that may pose a security threat?	56 (70%)	18 (22.5%)	6 (7.5%)	0 (0%)	3.63
35	How easily do you adapt to changes in cybersecurity protocols or policies in your organization?	58 (72.5%)	16 (20%)	6 (7.5%)	0 (0%)	3.65
	Average Mean for Human Security					**3.64**
	Weighted Mean for Impact of Cybersecurity Awareness on Secretaries Job Performance					**3.66**

Decision rule 1.00 – 1.49=Very Low, 1.50 – 2.49=Low, 2.50 – 3.49= High, 3.50 – 4.00=Very High

The table shows the effectiveness of various cybersecurity layers, particularly Perimeter Security, Endpoint Security, Data Security, and Human Layer. For Perimeter Security, respondents expressed strong effectiveness in firewalls and intrusion prevention systems, with an average mean of 3.64, suggesting that these measures are generally well-implemented. In Endpoint Security, respondents rated the impact of cybersecurity best practices and confidence in handling sensitive data highly, with an average mean of 3.67, indicating that these practices are perceived as enhancing productivity and security. For Data Security, encryption protocols and secure backups received positive ratings, with an average mean of 3.68, reflecting effective safeguards for sensitive organizational data. Finally, in the Human Layer, respondents were confident in recognizing security threats like suspicious emails and adapting to changes in cybersecurity policies, yielding an average mean of 3.64. The weighted mean for the impact of cybersecurity awareness on secretaries' job performance is 3.66, suggesting a high level of confidence in the multi-layered security approach and its positive influence on job performance.

Table 8 One-Sample Test Research Question Four: What is the impact of Cybersecurity Awareness on Secretaries' Job Performance in University of Ibadan?

	Test Value = 0					
	t	**df**	**Sig. (2-tailed)**	**Mean Difference**	**95% Confidence Interval of the Difference**	
					Lower	**Upper**
Impact of Cybersecurity Awareness on Secretaries Job Performance	59.570	79	0.000	3.65714	3.5349	3.7793

The results of the One-Sample t-test for the Impact of Cybersecurity Awareness (CA) on Secretaries' Job Performance (SJP) demonstrate a highly significant relationship. The t-value of 59.570 with 79 degrees of freedom yields a p-value of 0.000, which is well below the 0.05 significance level, indicating that the impact of cybersecurity awareness on job performance is statistically significant. The mean difference of 3.65714 suggests a notable positive effect, and the 95% confidence interval of 3.5349 to 3.7793 confirms that the true mean difference is likely to fall within this range. These

findings imply that increased cybersecurity awareness is strongly associated with improved job performance among secretaries at the University of Ibadan, with the results being both meaningful and reliable.

3.1.3 Testing of Hypotheses

Table 9 H_{01} There is no relationship between Cybersecurity and Secretaries Job Performance in University of Ibadan

		Level of Secretaries Job Performance	Cyber Security Awareness
Level of Secretaries Job Performance	Pearson Correlation	1	0.938**
	Sig. (2-tailed)		0.000
	N	80	80
Cyber Security Awareness	Pearson Correlation	0.938**	1
	Sig. (2-tailed)	0.000	
	N	80	80

The Pearson correlation coefficient of 0.938 indicates a very strong positive relationship between Cybersecurity Awareness and Secretaries' Job Performance. The p-value is 0.000 and significance value is 0.05. Since the p-value is 0.000, which is smaller than the significant value 0.05, we reject the null hypothesis (H_0). Therefore, there is sufficient evidence to conclude that there is a significant relationship between Cybersecurity Awareness and Secretaries' Job Performance at the University of Ibadan.

H_{02}: Cybersecurity does not have any impact on Secretaries' Job Performance in the University of Ibadan

Table 10 Model Summary for H_{02}

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.938[a]	0.880	0.878	0.16650

a. Predictors: (Constant), Cyber Security Awareness

Table 11 ANOVA[a] for H_{02}

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	15.862	1	15.862	572.184	0.000[b]
	Residual	2.162	78	0.028		
	Total	18.025	79			

a. Dependent Variable: Level of Secretaries' Job Performance; b. Predictors: (Constant), Cyber Security Awareness

Table 12 Coefficients[a] for H_{02}

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.669	0.127		5.280	0.000
	Cyber Security Awareness	0.819	0.034	0.938	23.920	0.000

a. Dependent Variable: Secretaries' Job Performance

The regression analysis results indicate a strong and significant relationship between cybersecurity awareness and secretaries' job performance at the University of Ibadan. The Model Summary shows a correlation coefficient (R = 0.938) and a high coefficient of determination (R^2 = 0.880), indicating that 88% of the variance in secretaries' job performance

can be explained by cybersecurity awareness. The Adjusted R^2 value of 0.878 confirms the model's robustness, while the Standard Error of the Estimate (0.16650) suggests minimal error in predictions.

The ANOVA results confirm the model's statistical significance, with a very high F-value (572.184) and a p-value of 0.000, highlighting that the regression model is a good fit for the data.

The Coefficients table provides further insights, showing an unstandardized coefficient (B = 0.819) and a standardized coefficient (Beta = 0.938) for cybersecurity awareness. This means that a one-unit increase in cybersecurity awareness leads to a 0.819-unit increase in secretaries job performance. The t-value (23.920) and p-value (0.000) confirm the statistical significance of this relationship. Since the p-value is 0.000 (less than 0.05), we reject the null hypothesis and conclude that cybersecurity has a significant and positive impact on Secretaries' job performance at the University of Ibadan.

4 Discussion of Findings

The findings of research question one revealed that secretaries at the University of Ibadan exhibit a generally high level of job performance, with an average mean score of 3.67 out of 4. This suggests that, on average, secretaries perceive themselves as highly effective in their roles. This result aligns with the findings of Onche (2023), who conducted a survey on "Employee Coordination Practices and Job Performance of Secretaries in Federal Universities in South-West Nigeria," which included the University of Ibadan. Using a stratified proportionate sampling technique, Onche selected 217 participants based on Krejcie and Morgan's sample size table and achieved a 99% response rate (215 responses). With a questionnaire reliability coefficient of 0.93, descriptive statistics and regression analysis revealed a moderate level of job performance among secretaries, with a mean score of 2.14.

The findings for research question two indicated a moderately high level of cybersecurity awareness among secretaries at the University of Ibadan, with an overall mean score of 3.66 (on a 4-point scale). While confidentiality and discretion also ranked moderately high, their mean score was slightly below that of integrity (3.70). To address this gap, secretaries are encouraged to participate in consistent training and retraining to enhance their skills in confidentiality and discretion. Supporting this finding, Zwilling et al. (2020) conducted research across Israel, Slovenia, Poland, and Turkey, demonstrating that while internet users are aware of cyber threats, they often take only minimal and basic precautions.

For research question three, the findings revealed a very strong positive relationship between cybersecurity awareness and secretaries' job performance at the University of Ibadan. This indicates that higher levels of cybersecurity awareness significantly correlate with better job performance. However, secretaries are encouraged to engage in continuous training to address emerging cyber threats that accompany advancements in technology. The study by Tripathy et al. (2023) supports this result. Their research on how employees' cybersecurity behavior is influenced by knowledge of cybersecurity policy, which surveyed 579 corporate managers and professionals, found that employees with a thorough understanding of company cybersecurity policies are better equipped to handle cybersecurity-related tasks compared to those with limited knowledge.

Finally, the findings for research question four demonstrated that cybersecurity awareness has a significant impact on secretaries' job performance at the University of Ibadan. While cybersecurity awareness is a key factor, it is acknowledged that other variables also contribute to determining secretaries' job performance.

The first hypothesis, which posits that there is no relationship between cybersecurity and secretaries' job performance at the University of Ibadan, was rejected because the p-value (0.000) was less than the significance level (0.05). This indicates a strong positive relationship between cybersecurity and secretaries' job performance at the University of Ibadan.

The second hypothesis, which states that cybersecurity does not impact secretaries' job performance at the University of Ibadan, was also rejected. The t-value (23.920) and p-value (0.000) confirmed the statistical significance of this relationship. Since the p-value is less than 0.05, it is concluded that cybersecurity has a significant and positive impact on secretaries' job performance at the University of Ibadan.

These findings align with the study conducted by Akinwande (2023), which examined Artificial Intelligence and Cybersecurity as predictors of 21st-century secretaries' job efficiency at the University of Ibadan. Using a descriptive research design, total enumeration of 80 secretaries, a structured questionnaire as the research instrument, and Cronbach's alpha for reliability testing, the study employed multiple regression and correlation analyses to test the

hypotheses. The results revealed a statistically significant, albeit weak, relationship between the level of cybersecurity and job efficiency.

Recommendations

Based on the findings, the following recommendations are made

- University of Ibadan should carry out performance appraisal and identify areas where the secretaries need improvement. Workshops on cybersecurity and other areas should be organized for secretaries to improve and maintain their job performance.
- Secretaries shall be regularly trained on issues of cybersecurity involving new threats and practices of data security. Items on cybersecurity awareness shall be added to the universities' professional development programs to ensure that secretaries are kept abreast of current trends in cybersecurity.
- Secretaries ought to have access to reliable tools like firewalls, encryption software, and multi-factor authentication. Therefore, management of University of Ibadan should avail the secretaries with all of them.
- The university should make policy which will enforce adherence to cybersecurity measures by the secretaries

5 Conclusion

This study examined the relationship between cybersecurity awareness and secretaries' job performance at the University of Ibadan. The findings revealed that secretaries demonstrate a high level of job performance (mean = 3.67) and a moderately high level of cybersecurity awareness (mean = 3.66). The study also established a very strong positive correlation (r = 0.938) between cybersecurity awareness and secretaries' job performance, suggesting that enhanced cybersecurity awareness significantly contributes to better performance. Also, regression analysis confirmed that cybersecurity awareness accounts for 88% of the variance in job performance, with a notable impact validated by a highly significant t-value (23.920) and p-value (0.000). It has been shown that, among other things, cybersecurity significantly influences how well secretaries at the University of Ibadan perform on the job, particularly in in this era of digitalization.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Afolabi, M. B., & Agbor, J. E. (2021). Cybercrime ordeal in Nigeria security firmament. *Sapientia Global Journal of* Arts, Humanities and Development Studies (SGOJAHDS), 4(1), 257–268. https://sgojahds.com/index.php/SGOJAHDS/article/view/181

[2] Akinwande R. A. (2023). Artificial Intelligence and Cybersecurity as Predictors of 21st Century Secretaries Job Efficiency in University of Ibadan. Final Year Project submitted to the Department of Office Technology and Management, The Polytechnic, Ibadan, Ibadan.

[3] Bello, T. (2017). Anatomy of cybercrime in Nigeria: The legal chronicle. Available at SSRN 3055743.

[4] Corradini, I. (2020). Redefining the Approach to Cybersecurity. In: Building a Cybersecurity Culture in Organizations. Studies in Systems, Decision and Control, vol 284. Springer, Cham. https://doi.org/10.1007/978-3-030-43999-6_3

[5] Denning, D. (2000). Cyberterrorism: The new threat. Retrieved from https://www.ssrc.org

[6] Di Nocera, F., Tempestini, G., & Presaghi, F. (2024). Reliability and validity of the Cybersecurity Awareness INventory (CAIN). Behaviour & Information Technology, 44(7), 1417–1428. https://doi.org/10.1080/0144929X.2024.2355362

[7] Falade, P. V. (2023). Trend and Emerging Types of 419 Scams. arXiv preprint arXiv:2308.12448.

[8] FBI. (2021). Identity theft overview. Retrieved from https://www.fbi.gov

[9] Gardenia, Y., and Gani, A. G. (2024). Cybersecurity Awareness Model with Methods: Analytical Hierarchy Process and Structural Equation Model. EAI Endorsed Transactions on Scalable Information Systems, 11.

[10] Gardenia, Y., and Gani, A. G. (2024). Cybersecurity Awareness Model with Methods: Analytical Hierarchy Process and Structural Equation Model. EAI Endorsed Transactions on Scalable Information Systems, 11.

[11] Halder, D., and Jaishankar, K. (Eds.). (2011). Cybercrime and the victimization of women: Laws, rights and regulations: Laws, rights and regulations. Igi Global.

[12] Hazen, S. (2020). Spam definition and examples. Retrieved from https://www.thefreedictionary.com/spamming

[13] Helpline Law. (n.d.). Cyber crimes in India. Retrieved from http://www.helplinelaw.com

[14] International Telecommunications Union (ITU). (n.d.). Definition of cybersecurity. ITU-T X.1205, Overview of cybersecurity. Retrieved November 25, 2024, from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[15] Jrank Articles. (2021). Intellectual property theft and its impact. Retrieved from http://law.jrank.org

[16] Khan, M. H., & Muntaha, S. T. (2024). Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks: A qualitative study. World Journal of Advanced Research and Reviews, 23(2), 1663–1673. https://doi.org/10.30574/wjarr.2024.23.2.2538

[17] Monkshouts. (2019). Types of cybercrime and prevention tips. Retrieved from http://www.monkshouts.org

[18] Nimkar, S., & Kumar, S. (2024). An analytical study on cyber security awareness level. In 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET) (pp. 1–6). IEEE. https://doi.org/10.1109/ICICET59348.2024.10616311

[19] Nurse, J. R. C. (2021). Cybersecurity Awareness. In Encyclopedia of Cryptography, Security and Privacy. Springer. DOI: 10.1007/978-3-642-27739-9_1596-1

[20] Ojedokun, A. U., & Eraye, C. M. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. International Journal of Cyber Criminology, 6(2), 1001.

[21] Onche, V. O. (2023). Employee Coordination Practices and The Job Performance of Secretaries in Federal Universities in South-West, Nigeria. British Journal of Multidisciplinary and Advanced Studies, 4(6), 65-78.

[22] Oyerinde, D. O., Aina, M. A., & Adeniran, A. O. (2023). Digital Devices and Job Performance of Secretaries in Government Parastatals in Ekiti State, Nigeria. Shodh Sari-An International Multidisciplinary Journal, 02(02), 270–281. https://doi.org/10.59231/SARI7586

[23] Schaffer, D. (2012). The language of scam spams: linguistic features of" Nigerian fraud" e-mails. ETC: A Review of General Semantics, 157-179.

[24] Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. Information, 15(9), 512.

[25] The Free Dictionary. (n.d.). Spam definition. Retrieved from https://www.thefreedictionary.com

[26] Tripathy, S., Rao, C. L., Kumar, V., Adity, P. H., Kumar, D., and Jindal, M. (2023). Investigating How Employees' Cybersecurity Behaviour is Affected by Their Knowledge of Cybersecurity Policy. In 2023 IEEE International Conference on ICT in Business Industry and Government (ICTBIG) (pp. 1-6). IEEE.

[27] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269