ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Information Security Awareness, Organisational Support and Job Performance of Secretarial Professionals in a Digital Workplace, a case of University of Ibadan, Oyo State, Nigeria.

Basit A. Waheed[1]; Virginia O. Onche (P.hD)[2]; Paul A. Adejumo[3]

[1]Division of Senate, Admissions and Affiliated Institutions, University of Ibadan

[2]Department of Educational Management, University of Ibadan

[3]Vice Chancellor's Office, University of Ibadan

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150700013

Received: 11 July 2026; Accepted: 16 July 2026; Published: 05 August 2026

ABSTRACT

This study explored how Information Security Awareness (ISA) and Organizational Support (OS) influence the job performance of secretarial professionals at the University of Ibadan's digital workspace. Grounded in the Protection Motivation Theory (PMT), Organizational Support Theory (OST), and the Ability–Motivation–Opportunity (AMO) framework, the study extended existing knowledge by addressing a gap in the Nigerian higher education sector through an assessment of the combined predictive roles of Information Security Awareness (ISA) and Organizational Support (OS) in influencing employee performance. A descriptive survey design was used, involving a complete census of 120 secretarial professionals. Data were gathered through a validated questionnaire (Cronbach's Alpha: 0.875–0.885) and analyzed with descriptive statistics and regression models. Results showed high job performance (weighted mean = 3.78), high ISA (3.66), and moderately high OS (3.13). Regression analysis revealed that ISA had a very strong, significant impact on performance ($R = 0.884$, $R^2 = 0.782$, $B = 0.920$, $p < 0.001$), while OS had a moderate but significant effect ($R = 0.462$, $R^2 = 0.214$, $B = 0.292$, $p < 0.001$). Together, ISA and OS explained 80.9% of the variance in performance ($R = 0.899$, $R^2 = 0.809$, $p < 0.001$), with ISA emerging as the dominant predictor ($\beta = 0.824$). The study concludes that ISA significantly enhances staff capacity to protect information, adhere to policies, and maintain operational efficiency, while OS improves performance through resources, policies, and recognition. It recommends providing secure digital tools, targeted ISA awareness programs, and integrated security–support strategies to safeguard institutional data and ensure sustainable productivity in the digital age.

Keywords: Information Security, Awareness, Organisational Support, Job performance, Secretarial Professionals, Digital Workspace

INTRODUCTION

In today's dynamic digital environment, information technology serves as a vital organizational resource for improving operational efficiency and minimizing the time and financial resources required to process large volumes of information. It comprises the design, development, implementation, support, and management of computer-based information systems, integrating both hardware and software components to enable effective information processing and management. Building on this, Indah, M. et al. (2022) emphasize that safeguarding company data and information is essential when using information technology. Security is a fundamental aspect of information systems, as they often contain personal and confidential data belonging to individuals or organizations. Unfortunately, vulnerabilities remain common, exposing systems to threats such as viruses, human error, and hacking.

Job performance is a vital factor in determining organizational success, as it drives the delivery of high-quality services that improve customer satisfaction. Strong performance enables employees to create value that meets

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

or exceeds stakeholder expectations, contributing to long-term sustainability and competitive advantage. In industrial and organizational psychology, it is consistently recognized as one of the most critical indicators of overall organizational effectiveness (Masood et al., 2020).

Essentially, job performance represents the results of an individual's efforts, influenced by their abilities and understanding of assigned roles or tasks, and reflects how effectively these tasks are executed. Information Communication plays a significant role here, being able to share information clearly and accurately, and jealously guide and guard the same without breaches, will not only enhance competitive advantage but also foster customer trust and confidence (Borman, 2014).

Job performance encompasses the tasks and activities employees carry out to help achieve organizational goals. According to Okorie (2015), it includes all work-related behaviors, which can be viewed through three dimensions: outcomes, behaviors, and personal attributes. Its measurement typically involves systematic evaluation to assess the quality, relevance, and impact of work, with the purpose of rating, improving, or making necessary adjustments (Abosede & Akintola, 2015).

Appelbaum et al. (2000) proposed the Ability–Motivation–Opportunity (AMO) Theory, which explains employee performance as the outcome of the combined influence of three mutually reinforcing components. These include employees' ability, reflected in their knowledge and competencies; motivation, representing their readiness to apply effort toward work objectives; and opportunity, denoting the extent to which the organization provides the necessary resources, support, and enabling work environment for effective performance. In this study, information security awareness, as informed by PMT, enhances the ability of secretarial professionals to manage sensitive digital data securely. Organizational support, as explained by OST, strengthens their motivation and provides the opportunity to excel in their duties. The AMO framework thus explains how the combined influence of ISA and organizational support can lead to improved job performance in the University of Ibadan's digital workspace

The increasing digitalisation of organisational processes and the evolving nature of cybersecurity threats have underscored the need for empirical research on the influence of information security awareness and organisational support on the performance of secretarial professionals operating in digital workplace environments. The evolution of digital workplaces, accelerated by remote work trends and digital transformation initiatives, has heightened vulnerabilities associated with human factors in cybersecurity (Muthuswamy & Nithya, 2023; Radha et al., 2024).

Hwang et al. (2021) defined Information Security Awareness (ISA) as the extent to which employees possess the knowledge, understanding, and appropriate attitudes required to safeguard an organization's information assets. When employees exhibit low levels of security awareness and fail to cooperate effectively, they are more likely to misuse or misinterpret security protocols, thereby increasing the likelihood of security breaches and establishing personnel as a major source of organizational information security risk (Khando et al., 2021). To address this, organizations should foster a security-oriented culture by increasing awareness of relevant principles, policies, and potential threats (Kő et al., 2023). Through strategic actions and informed decision-making, top management can shape this culture effectively. Employees cannot reasonably be held accountable for breaches if they have not been equipped with sufficient knowledge of risks and countermeasures. When leadership prioritizes security, higher ISA can significantly strengthen overall protection by improving the effectiveness of information security management (Kő et al., 2023; Halboob et al., 2023).

Information Security Awareness (ISA) refers to employees' level of knowledge and understanding of organizational security policies, procedures, and potential security threats (Alsboul, 2016). As the global information security environment continues to evolve, organizations face increasingly sophisticated challenges arising from insider threats, malicious actors, and emerging forms of cyberattacks. The widespread adoption of hybrid work arrangements has further expanded the attack surface, creating additional risks to data security and system accessibility. Information security within organizations therefore focuses on protecting sensitive information from unauthorized access, disclosure, modification, disruption, or destruction by implementing measures that ensure the confidentiality, integrity, and availability of information assets. Moreover, the growing

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

prevalence of ransomware attacks; many of which originate through phishing campaigns, underscores the critical role of employees as the first line of defense. Consequently, maintaining a high level of security awareness is essential for identifying and mitigating evolving threats, including zero-day vulnerabilities and data breaches (IBM, 2022). Evidence indicates that employees with high autonomy and accountability play a crucial role in managing risks, mitigating threats, and enhancing cyber resilience (NCSAM, 2019).

Lavelle (2022), citing a Gartner report, noted that more than 74% of organizations intend to maintain remote work arrangements for at least part of their workforce on a long-term basis. While this transition offers greater workplace flexibility, it also creates additional cybersecurity challenges that reshape the organizational threat landscape. According to Georgiadou (2022), cybercriminals can exploit weaknesses associated with employee practices as well as deficiencies in organizational security policies. Employees working remotely are particularly vulnerable when they access organizational systems through unsecured public Wi-Fi networks, rely on unauthorized software or shadow IT, or store confidential corporate information on personal or inadequately protected devices. Such practices significantly increase the risk of cyberattacks and unauthorized data exposure. In addition, remote work environments make it more difficult for organizations to identify, monitor, and respond effectively to threats such as phishing attacks, malware infections, and insider-related security incidents (Aakash, 2021).

Mitigating such threats requires a multi-layered cybersecurity strategy that addresses password management, infrastructure security, email protection, user training, and social network safeguards. While users often recognize the difference between strong and weak passwords, risky behaviors such as storing or sharing credentials persist. Additionally, mandatory password changes can sometimes encourage password reuse, highlighting the need for varied strategies (Tam, 2010). Infrastructure security depends on both technical measures, such as antivirus programs, firewalls, and anti-spyware, and responsible user practices, including locking devices, avoiding unsafe browsing, and limiting non-work social media use (Sanok, 2005). Email remains a primary attack vector, with risks mitigated through machine learning detection, encryption, clear policies, and targeted user training (Kruger, 2007).

Lastly, security education fosters compliance when built on collaboration, transparent policies, and balanced enforcement, with awareness of threats serving as a key driver of secure behavior (Safa, 2016). Social networks present additional privacy challenges, as research highlights vulnerabilities in user profiles and the need for tailored strategies to manage both voluntary and mandatory data sharing (Al-Molhem, 2019).

The Protection Motivation Theory (PMT), proposed by Rogers (1975), explains individuals' adoption of protective behaviours through two key cognitive evaluation processes: threat appraisal and coping appraisal. Threat appraisal involves assessing the perceived severity of and susceptibility to a potential threat, whereas coping appraisal focuses on evaluating the effectiveness of the recommended protective response, an individual's confidence in carrying out that response (self-efficacy), and the perceived costs associated with taking protective action (Chang et al., 2022; Ogbanufe et al., 2023). These evaluations collectively shape protection motivation, which represents an individual's intention to engage in behaviours that reduce or prevent security risks (Boss et al., 2015). Owing to its strong explanatory capacity, PMT has been extensively employed in information security research to investigate issues such as responses to computer virus threats, password security practices (Vedadi & Warkentin, 2020), and adherence to organizational information security policies (Alsaad & Al-Okaily, 2022). Within the context of the present study, PMT provides the theoretical basis for explaining how information security awareness influences the compliance behaviour of secretarial professionals in the digital work environment of the University of Ibadan.

Ameen et al. (2021) define perceived organizational support as “employees’ belief that their contributions are valued and their well-being matters to company leaders”. Beyond expecting performance, supportive organizations provide resources that balance employee welfare with business goals. Such support fosters organizational commitment, encourages proactive evaluation of technical infrastructure, and promotes the implementation of security measures for critical systems. Furthermore, it supports employees in successfully adopting and leveraging digital technologies, which enhances the resilience of critical infrastructure security and improves organizational performance in digitally enabled work environments (Kalischko & Riedl, 2021).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

A digital workplace can be defined as an integrated technological ecosystem that enables collaboration, communication, and coordinated work activities across traditional office, remote, and hybrid working environments (Marsh et al., 2022). It enables seamless interaction among colleagues through advanced mobile tools, allowing employees to access and share information from any location. Digital workplace adoption leverages technologies to enhance efficiency, optimize processes, and support stakeholders such as customers, suppliers, and employees Muthuswamy and Nithya (2023). Within the broader context of digital transformation, the digital workplace serves as a catalyst for innovation by transforming existing business processes, strengthening organizational culture, and enhancing stakeholder experiences to address emerging market expectations. The adoption of digital workplace solutions contributes to greater operational efficiency, higher levels of productivity, organizational growth, and the sustained achievement of organizational performance.

Kour and Karim (2021) study argues that when organizations adopt HR strategies that prioritize employees' social and economic well-being, they foster loyalty and cooperation, which in turn supports the implementation of critical infrastructure security. Such support can take the form of monetary and non-monetary benefits, access to resources, professional development, and emotional encouragement. These measures expand employees' digital knowledge, facilitate the adoption of tools like cloud resources, and improve interaction with secure cloud systems. With cloud security in place, employees can manage high-quality data more effectively (Klimburg-Witjes & Wentland, 2021) and engage stakeholders remotely. Ultimately, organizational backing for cloud security enhances both digital workplace quality and overall technological effectiveness (Rodríguez-Abitia & Bribiesca-Correa, 2021).

Organizational Support Theory (OST), introduced by Eisenberger et al. (1986), posits that employees who believe their organization appreciates their contributions and is genuinely concerned about their well-being, commonly referred to as Perceived Organizational Support (POS), are more inclined to reciprocate through increased commitment, enhanced work effort, and greater adherence to organizational policies and procedures. Within the context of this study, organizational support comprises initiatives such as information security training, the provision of secure technological resources, clearly communicated security policies, and timely IT support. These organizational practices foster employees' trust, strengthen compliance with information security requirements, and contribute to improved job performance. Perceived Organizational Support is typically assessed using the Survey of Perceived Organizational Support (SPOS), an instrument that evaluates employees' perceptions of organizational fairness, supervisory support, access to essential resources, opportunities for training and development, and recognition of their contributions.

Statement of Problem

Empirical evidence indicates that a considerable proportion of cybersecurity incidents stem from human-related factors, emphasizing the critical need to strengthen Information Security Awareness (ISA) and organizational support as essential measures for protecting institutional information assets (Blythe, 2013; Klein & Zwilling, 2023). Nevertheless, the growing digitalization of administrative operations at the University of Ibadan has intensified the demand for effective information security practices among secretarial professionals. Their ability to perform efficiently in a digital work environment may be constrained by inadequate organizational support, including insufficient security training, limited access to secure technological resources, and poorly communicated information security policies. Against this backdrop, the present study examines the influence of information security awareness and organizational support on the job performance of secretarial professionals within the digital workplace of the University of Ibadan

Aim and Objectives of The Study

The aim of this study is to examine the influence of information security and Organizational Supports on Job Performance of Secretarial Professionals in a Digital Workspace in the University of Ibadan. The subobjectives are to:

1. assess the level of Job Performance of Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

2. identify the level of organizational support given to Secretarial Professionals in University of Ibadan, Oyo State
3. identify the level of Information Security Awareness of Secretarial Professionals in University of Ibadan, Oyo State
4. evaluate the influence of Information Security Awareness on the Job Performance of the Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State
5. evaluate the influence of Organisational Support on the Job Performance of the Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State
6. evaluate the combined influence of both Information Security Awareness and Organisational Support on the Job Performance of the Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State

Research Questions

1. What is the level of Job Performance of Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State
2. What is the level of organizational support given to Secretarial Professionals in University of Ibadan, Oyo State
3. What is the level of Information Security Awareness of Secretarial Professionals in the University of Ibadan, Oyo State

Hypotheses

H_{01}: There is no influence of Information Security Awareness on the Job Performance of the Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State

H_{02}: There is no influence of Organisational Support on the Job Performance of the Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State

H_{03}: There is no combined influence of both Information Security Awareness and Organisational Support on the Job Performance of the Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State

METHODOLOGY

A cross-sectional survey design was employed in this study to facilitate the collection of data from respondents at a single point in time. This research design was considered suitable for investigating the relationships among Information Security Awareness (ISA), Organisational Support (OS), and job performance. However, because cross-sectional studies capture data only once, they are unable to establish causal relationships between variables. Therefore, the findings should be interpreted as indicating statistically significant associations rather than definitive cause-and-effect links. To provide stronger evidence of causality and to monitor changes in employees' information security awareness, organisational support, and job performance over time, future research should consider employing longitudinal or experimental research designs.

The population comprised 120 secretarial professionals at the University of Ibadan. Given the relatively small population, the study adopted a total enumeration approach.

Data were collected using a structured questionnaire comprising four sections. Section A elicited respondents' demographic information. Section B measured Information Security Awareness (ISA), Section C measured Organisational Support (OS), and Section D measured Job Performance (JP). Sections B, C, and D each consisted of ten items measured on a four-point Likert scale ranging from Very High (4) to Very Low (1).

The questionnaire used in this study was developed through a comprehensive review of relevant literature and by adapting items from established and validated measurement instruments. The Information Security Awareness (ISA) scale was adapted from the works of Ahsan et al. (2026) and Alshammari and Al-Mamary (2026), with its development informed by the Protection Motivation Theory (PMT) and related information security compliance

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

models. The Organisational Support (OS) scale was derived from the Survey of Perceived Organizational Support (SPOS) developed by Eisenberger et al. (1986), whereas the Job Performance scale was adapted from the Ability–Motivation–Opportunity (AMO) framework introduced by Appelbaum et al. (2000). To ensure the instrument was appropriate for the study context, slight revisions were made to the wording of selected items to improve clarity and reflect the experiences of secretarial professionals in Nigerian universities, while maintaining the conceptual integrity of the original constructs.

To ensure the instrument possessed adequate face and content validity, the initial questionnaire was subjected to expert review. Two specialists in Information Management and Information Security evaluated the instrument by assessing the relevance, clarity, and representativeness of the questionnaire items with respect to the research objectives and theoretical foundations. Feedback obtained from the reviewers guided the refinement and modification of the instrument before it was administered for pilot testing.

Prior to the main data collection, a pilot study was undertaken among secretarial professionals at Ladoke Akintola University of Technology, Ogbomoso, to assess the internal consistency of the research instrument. Reliability analysis produced Cronbach's Alpha values of 0.885 for the Information Security Awareness scale, 0.875 for the Organisational Support scale, and 0.883 for the Job Performance scale. Because each coefficient exceeded the recommended minimum threshold of 0.70, the instrument was judged to possess satisfactory reliability and was deemed appropriate for the main survey. Descriptive statistics (frequency, percentage, mean, and standard deviation) were used to answer the research questions, while regression analysis was employed to test the hypotheses.

Analysis and Interpretation of Data

Answering of Research Questions

Table One: Descriptive Statistics on the Job Performance of Secretarial Professionals at the University of Ibadan: What is the level of job performance of Secretarial Professionals at the University of Ibadan, Ibadan, Oyo State?

Job Performance	**VH**	**H**	**L**	**VL**	**Mean**
Ability (Knowledge and Skill) To what extent do you possess the skills needed to complete administrative tasks accurately and efficiently?	(94) 78.3%	(20) 16.7%	(6) 5.0%	(0) 0%	3.73
To what extent can you adapt quickly to new administrative technologies and software tools?	(94) 78.3%	(20) 16.7%	(6) 5.0%	(0) 0%	3.73
To what extent do you maintain accuracy and attention to detail in preparing documents, reports, and records?	(86) 71.7%	22 18.3%	12 10.0%	0 1.7%	3.62
Average Mean					**3.69**
Motivation (Willingness and Efforts) To what extent do you put in extra effort to ensure that all assigned tasks are completed on time?	(98) 81.7%	(18) 15.0%	(4) 3.3%	(0) 0%	3.78
To what extent do you actively seek ways to improve the quality of your work?	(102) 85.0%	(14) 11.7%	(4) 3.3%	(0) 0%	3.82

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

To what extent do you remain committed to safeguarding sensitive institutional information?	(102) 85.0%	(14) 11.7%	(4) 3.3%	(0) 0%	3.82
Average Mean					**3.80**
Opportunity (Resources & Support) To what extent do you have access to the digital tools and resources you need to perform your duties effectively?	(90) 75.0%	(26) 21.7%	(4) 3.3%	(0) 0%	3.72
To what extent can you organize and maintain both digital and physical records systematically with the resources available?	(90) 75.0%	(26) 21.7%	(4) 3.3%	(0) 0%	3.72
To what extent do you receive adequate support from your department to carry out your responsibilities?	(120) 100.0%	(0) 0%	(0) 0%	(0) 0%	4.0
To what extent can you manage multiple administrative tasks simultaneously without compromising quality?	(116) 78.7%	(2) 17.8%	(2) 3.6%	(0) 0%	3.95
Average Mean					**3.84**
Weighted Mean for Job Performance of Secretarial Staff in University of Ibadan					**3.78**

Source: Field Survey Result (2025)

Decision rule 1.00 – 1.49=VL, 1.50 – 2.49=L, 2.50 – 3.49= H, 3.50 – 4.00=H

Note: VL= Very Low, L= Low H=High, H= Very High

The findings from Table One indicate that the job performance of secretarial professionals at the University of Ibadan is high across all assessed dimensions, with a weighted mean score of 3.78. Specifically, their ability, encompassing knowledge, skill, and adaptability recorded an average mean of 3.69, suggesting strong competence in administrative tasks, attention to detail, and proficiency with emerging technologies. Their motivation scored even higher at 3.80, reflecting a consistent willingness to put in extra effort, maintain high-quality standards, and protect sensitive institutional information. The highest-rated dimension, opportunity, achieved an average mean of 3.84, underscoring the adequacy of institutional resources, departmental support, and the capacity to manage multiple tasks effectively. The results suggest that the combination of technical ability, strong motivation, and sufficient institutional support enables secretarial staff to perform their duties with a high level of efficiency and effectiveness.

Table Two: Descriptive Statistics on the Level of Organisational Supports for Secretarial Professionals at the University of Ibadan: What is the level of Organisational Supports given to Secretarial of Secretarial Professionals at the University of Ibadan, Ibadan, Oyo State?

Organisational Supports	VH	H	L	VL	Mean
Training & Development To what extent does the university provide adequate training on information security practices?	(100) 100.0%	(0) 0.0%	(0) 0.0%	(0) 0%	4.0

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

To what extent do you receive training that enhances your ability to perform administrative tasks?	(100) 100.0%	(0) 0.0%	(0) 0.0%	(0) 0%	4.0
To what extent does the university offer opportunities to upgrade your skills in digital administration?	(48) 40.0%	(70) 58.3%	(2) 1.7%	(0) 0%	2.38
Average Mean					**3.46**
Resources & Tools To what extent does the university provide secure and reliable digital tools for your work?	(88) 73.3%	(22) 18.3%	(10) 8.3%	(0) 0%	2.65
To what extent do you have access to updated software and systems needed for your duties?	(88) 73.3%	(22) 18.3%	(10) 8.3%	(0) 0%	2.65
To what extent is your work environment equipped with resources that ensure efficiency?	(88) 73.3%	(22) 18.3%	(10) 8.3%	(0) 0%	2.65
Average Mean					**2.65**
Policies & Assistance To what extent does the university have clear policies guiding information security practices?	(90) 75.0%	(26) 21.7%	(4) 3.3%	(0) 0%	3.72
To what extent is IT support readily available when you encounter technical or security issues?	(98) 81.7%	(20) 16.7%	(4) 1.7%	(0) 0%	3.80
Average Mean					**3.76**
Recognition & Value To what extent is your contribution to administrative work recognized by your department?	(88) 73.3%	(22) 18.3%	(10) 8.3%	(0) 0%	2.65
To what extent does the university value your role in maintaining information security?	(88) 73.3%	(22) 18.3%	(10) 8.3%	(0) 0%	2.65
Average Mean					**2.65**
Weighted Mean for Organisational Support to Secretarial Professionals in the University of Ibadan					**3.13**

Source: Field Survey Result (2025)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Decision rule 1.00 – 1.49=VL, 1.50 – 2.49=L, 2.50 – 3.49= H, 3.50 – 4.00=H

Note: VL= Very Low, L= Low H=High, H= Very High

The results in Table Two reveal that the overall level of organisational support provided to secretarial professionals at the University of Ibadan is high, with a weighted mean score of 3.13. Among the four measured dimensions, Policies and Assistance recorded the highest rating (average mean = 3.76), indicating that staff benefit from clear institutional policies and readily available IT support when addressing technical or security challenges. Training and Development also scored high (average mean = 3.46), largely due to strong provision of information security training and administrative task enhancement programmes; however, opportunities for upgrading digital administration skills were rated low (2.38), highlighting a critical area for improvement. Both Resources and Tools and Recognition and Value received identical lower-end high ratings (2.65 each), suggesting that while staff have some access to digital tools and acknowledgment of their contributions, these supports are not optimal. Overall, the findings indicate that while the University offers a solid baseline of organisational support, enhancing resource availability, recognition mechanisms, and digital upskilling opportunities could significantly strengthen the support system for secretarial professionals.

Table Three: Descriptive Statistics on the Level Information Security Awareness of Secretarial Professionals at the University of Ibadan: What is the level of Information Security Awareness of Secretarial Professionals at the University of Ibadan, Ibadan, Oyo State?

Information Security Awareness	**VH**	**H**	**L**	**VL**	**Mean**
Threat Appraisal To what extent are you aware of the possible consequences of a data breach in your work?	(100) 100.0%	(0) 0.0%	(0) 0.0%	(0) 0%	4.0
To what extent do you believe your role is vulnerable to information security threats?	(100) 100.0%	(0) 0.0%	(0) 0.0%	(0) 0%	4.0
To what extent do you consider security breaches a serious risk to the university's operations?	(64) 53.3%	(54) 45.0%	(2) 1.7%	(0) 0%	2.52
Average Mean					**3.51**
Coping Appraisal To what extent can you correctly follow the university's information security policies?	(94) 78.3%	(20) 16.7%	(6) 5.0%	(0) 0%	3.73
To what extent do you believe the university's security measures are effective?	(94) 78.3%	(20) 16.7%	(6) 5.0%	(0) 0%	3.73
To what extent is it worthwhile for you to follow security procedures even when they take extra effort?	(94) 78.3%	(20) 16.7%	(6) 5.0%	(0) 0%	3.73
Average Mean					**3.73**
Protective Motivation	(100)	(18)	(2)	(0)	3.82

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

what extent do you update your passwords and use secure authentication methods?	83.3%	15.0%	1.7%	0%	
To what extent do you avoid clicking unknown links or opening suspicious email attachments?	(94) 78.3%	(20) 16.7%	(6) 5.0%	(0) 0%	3.73
To what extent do you report suspicious activities or security incidents promptly to the IT department?	(94) 78.3%	(20) 16.7%	(6) 5.0%	(0) 0%	3.73
To what extent do you ensure that sensitive data is stored and shared only through approved secure channels?	(90) 75.0%	(26) 21.7%	(4) 3.3%	(0) 0%	3.73
Average Mean					**3.75**
Weighted Mean for Level of Information Security Awareness among Secretarial Professionals in the University of Ibadan					**3.66**

Source: Field Survey Result (2025)

Decision rule 1.00 – 1.49=VL, 1.50 – 2.49=L, 2.50 – 3.49= H, 3.50 – 4.00=H

Note: VL= Very Low, L= Low H=High, H= Very High

The results presented in Table Three show that the overall level of information security awareness among secretarial professionals at the University of Ibadan is high, with a weighted mean score of 3.66. Among the three measured dimensions, Protective Motivation recorded the highest average mean (3.75), indicating that staff regularly engage in good security practices, including updating passwords, avoiding suspicious links, reporting incidents promptly, and using approved secure channels for sensitive data. Coping Appraisal followed closely with an average mean of 3.73, reflecting strong adherence to institutional security policies, trust in the effectiveness of security measures, and commitment to following procedures even when inconvenient. Threat Appraisal was also rated high (3.51), with staff demonstrating excellent awareness of the consequences of a data breach and their personal vulnerability to threats; however, awareness of the broader operational risks posed by breaches scored notably lower (2.52), revealing a gap in institutional risk perception. Overall, the findings indicate a strong foundation of security awareness and behaviour, but also highlight the need for targeted sensitisation to deepen understanding of the systemic impact of information security breaches on the university's operations.

Hypotheses Testing

Table Five[a-c]: Regression Analysis for H_{01}

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.884[a]	.782	.780	.15948
a. Predictors: (Constant), Information Security Awareness				

ANOVA[a]

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.777	1	10.777	423.738	.000[b]
	Residual	3.001	118	.025		
	Total	13.779	119			

a. Dependent Variable: Job Performance

b. Predictors: (Constant), Information Security Awareness

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.407	.165		2.471	.015
	Information Security Awareness	.920	.045	.884	20.585	.000

a. Dependent Variable: Job Performance

The regression analysis tables above shows that information security awareness is a strong and statistically significant predictor of job performance R = 0.884, R^2 = 0.782, F(1,118) = 423.738,

p < 0.001R = 0.884, R^2 = 0.782, F(1,118) = 423.738, p < 0.001 R = 0.884, R^2 = 0.782, F(1,118) = 423.738, p <0.001. This model indicates that 78.2% of the variance in job performance among secretarial professionals can be explained by their level of information security awareness. The positive regression coefficient (B = 0.920, p < 0.001) suggests that for every one-unit increase in information security awareness, job performance increases by 0.920 units, highlighting a substantial and direct relationship between the two variables. Therefore, the null hypothesis is rejected it is concluded that Information Security Awareness has a significant influence on the Job Performance of the Secretarial Professionals in the University of Ibadan, Ibadan, Oyo State.

Table Six[a-c]: Regression Analysis for H_{02}

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.462[a]	.214	.207	.30303

a. Predictors: (Constant), Organisational_Support3

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.943	1	2.943	32.052	.000[b]
	Residual	10.835	118	.092		
	Total	13.779	119			

a. Dependent Variable: Job Performance

b. Predictors: (Constant), Organisational Support

Coefficients[a]

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Model		Unstandardized Coefficients		Standardized Coefficients	t
		B	Std. Error	Beta	
1	(Constant)	2.715	.191		14.189
	Organisational Support	.292	.052	.462	5.661
a. Dependent Variable: Job Performance					

The regression analysis revealed a moderate positive relationship between organisational support and job performance among secretarial professionals at the University of Ibadan ($R = 0.462$, $p < 0.001$). The model explains 21.4% of the variance in job performance ($R^2 = 0.214$, Adjusted $R^2 = 0.207$), indicating that while organisational support is a statistically significant factor, a substantial portion of performance variation is influenced by other variables. The unstandardized coefficient ($B = 0.292$, $p < 0.001$) suggests that for every one-unit increase in organisational support, job performance increases by 0.292 units. The standardized coefficient ($\beta = 0.462$) confirms a moderate effect size. The constant value ($B = 2.715$) indicates the baseline level of job performance when organisational support is absent. Overall, while organisational support contributes meaningfully to job performance, its influence is notably weaker than that of information security awareness in earlier models, suggesting that performance is shaped more strongly by other factors when considered independently.

Table Six: Regression Analysis for H_{03}

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.899[a]	.809	.805	.15011

a. Predictors: (Constant), Organisational_Support3, Information Security Awareness

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.142	2	5.571	247.241	.000[b]
	Residual	2.636	117	.023		
	Total	13.779	119			

a. Dependent Variable: Job Performance

b. Predictors: (Constant), Organisational_Support3, Information Security Awareness

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t
		B	Std. Error	Beta	

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

1	(Constant)	.237	.161		1.473
	Information Security Awareness	.856	.045	.824	19.075
	Organisational Support	.110	.027	.174	4.024
a. Dependent Variable: Job Performance					

The multiple regression analysis showed that the combination of information security awareness and organisational support significantly predicts job performance among secretarial professionals at the University of Ibadan ($R = 0.899$, $p < 0.001$). The model explains 80.9% of the variance in job performance ($R^2 = 0.809$, Adjusted $R^2 = 0.805$), indicating a very high explanatory power. Both predictors were statistically significant, but with differing magnitudes of influence. Information security awareness had the stronger effect ($B = 0.856$, $\beta = 0.824$, $p < 0.001$), meaning that for every one-unit increase in awareness, job performance rises by 0.856 units when controlling for organisational support. Organisational support, while still significant, had a smaller effect ($B = 0.110$, $\beta = 0.174$, $p < 0.001$), indicating that a one-unit increase in support raises job performance by 0.110 units when controlling for information security awareness. These results suggest that while both factors are important, information security awareness is the dominant predictor, contributing far more to variations in job performance than organisational support when both are considered together.

DISCUSSION OF FINDINGS

The first null hypothesis (H_{01}), which proposed that Information Security Awareness (ISA) has no significant effect on the job performance of secretarial professionals at the University of Ibadan, was not supported. The simple regression analysis demonstrated a strong positive and statistically significant relationship between Information Security Awareness and job performance ($R = 0.884$, $R^2 = 0.782$, $B = 0.920$, $\beta = 0.884$, $p < 0.001$). The coefficient of determination indicates that Information Security Awareness accounts for 78.2% of the observed variation in job performance. Furthermore, the regression coefficient ($B = 0.920$) suggests that a one-unit improvement in Information Security Awareness is associated with a corresponding increase of 0.920 units in job performance. These findings underscore the importance of cultivating employees' security awareness as a means of improving efficiency, effectiveness, and adherence to secure work practices in digitally enabled work environments. The outcome of this study corroborates the findings of Zhen, Dong, Xie, and Chen (2022) in their study, Factors Influencing Employees' Information Security Awareness in the Telework Environment, published in Electronics, 11(21), 3458. Employing the Knowledge–Attitude–Behavior (KAB) model alongside Knowledge Inertia Theory, the researchers examined the determinants of Information Security Awareness among 305 full-time teleworkers in China using purposive sampling and Partial Least Squares Structural Equation Modeling (PLS-SEM). Their findings revealed that employees' knowledge, behavioural practices, and learning inertia significantly enhanced Information Security Awareness, whereas attitude and experience inertia exerted no significant influence. The authors concluded that strengthening Information Security Awareness enables employees to identify potential security threats, comply with organizational security policies, and adopt secure work practices. This conclusion is consistent with the present study, which demonstrates that greater Information Security Awareness contributes significantly to improved job performance among secretarial professionals within the University of Ibadan's digital work environment.

The second null hypothesis (H_{02}), which stated that Organisational Support has no significant effect on the job performance of secretarial professionals at the University of Ibadan, was likewise rejected. The regression results

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

indicated a positive and statistically significant relationship between Organisational Support and job performance ($R = 0.462$, $R^2 = 0.214$, $B = 0.292$, $\beta = 0.462$, $p < 0.001$). The findings show that Organisational Support explains 21.4% of the variation in job performance, while the regression coefficient indicates that every one-unit increase in Organisational Support results in an estimated 0.292-unit increase in employees' job performance. These findings suggest that the provision of organizational resources, supportive policies, training opportunities, and recognition positively influences employees' ability to perform their responsibilities effectively. This finding is consistent with the study conducted by Xin Guan et al. (2014) on Perceived Organizational Support and Job Performance among faculty members in six Chinese universities. Using a cross-sectional survey of 700 randomly selected academic staff, of which 581 valid responses were analyzed, the researchers found that Perceived Organizational Support significantly influenced job performance through mediating variables such as job satisfaction, positive affectivity, and affective commitment. They further established that procedural and distributive justice contributed positively to employees' perception of organizational support. The present study similarly demonstrates that institutional support, including training, equitable policies, recognition, and adequate work resources, plays an important role in improving the performance of secretarial professionals within Nigerian universities.

The findings also agree with those reported by Popoola (2023) in the study titled Organizational Characteristics, Employee Commitment and Job Performance of Secretaries in Government-owned Tertiary Institutions in Oyo State, Nigeria. Adopting a descriptive survey design, the study investigated 248 secretaries selected from a population of 635 using the Krejcie and Morgan sample size table. Data collected through a structured questionnaire were analyzed using descriptive and inferential statistics. The results revealed that organizational characteristics significantly influenced job performance ($R = 0.594$, Adjusted $R^2 = 0.342$, $p < 0.05$), while employee commitment also had a significant positive effect ($R = 0.501$, Adjusted $R^2 = 0.239$, $p < 0.05$). Collectively, both variables accounted for a substantial proportion of the variation in employees' performance. These findings reinforce the current study's conclusion that supportive organizational practices, an enabling work environment, and employee commitment are critical drivers of improved job performance among secretarial personnel in tertiary institutions.

The third null hypothesis (H_{03}), which posited that Information Security Awareness and Organisational Support do not jointly predict job performance, was also rejected. The multiple regression analysis demonstrated that the combined model possessed substantial explanatory power ($R = 0.899$, $R^2 = 0.809$, Adjusted $R^2 = 0.805$, $F(2,117) = 247.241$, $p < 0.001$). Together, Information Security Awareness and Organisational Support explained 80.9% of the variance in job performance among the respondents. However, Information Security Awareness emerged as the strongest predictor of job performance ($B = 0.856$, $\beta = 0.824$, $p < 0.001$), whereas Organisational Support, although statistically significant, made a comparatively smaller contribution ($B = 0.110$, $\beta = 0.174$, $p < 0.001$). This finding indicates that while organizational support enhances employee performance, Information Security Awareness exerts a more pronounced influence on the effectiveness of secretarial professionals in a digital work environment. The result is consistent with the findings of Alkalbani, Deng, and Kam (2016) in their study, Investigating the Role of Socio-organizational Factors in Information Security Compliance in Organizations. Using survey data collected from 294 employees across different organizations, the researchers examined the influence of management commitment, awareness and training, accountability, and technological mechanisms on information security compliance. Their analysis demonstrated that these socio-organizational factors significantly improved employees' compliance with information security requirements. Similarly, the present study indicates that the integration of strong Information Security Awareness with adequate Organisational Support creates a favourable environment that enhances employees' performance. This finding further suggests that organizations seeking to improve performance in digital workplaces should not rely solely on technological controls but should also invest in continuous security awareness programmes and supportive organizational practices that encourage compliance, productivity, and effective job performance.

CONCLUSION

This study has demonstrated that both Information Security Awareness (ISA) and Organisational Support (OS) expressively influence the job performance of secretarial professionals in the University of Ibadan's digital workplace. The findings reveal that ISA exerts the strongest influence, accounting for the majority of

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

performance variance, while OS, though still significant, plays a more moderate role. High levels of ISA were associated with improved ability to identify, prevent, and respond to security threats, thereby enhancing efficiency, accuracy, and adherence to institutional policies. Organisational support, particularly in the form of clear policies, training, IT assistance, and recognition, further reinforced these outcomes by providing the resources, guidance, and motivation necessary for optimal performance. The combined predictive strength of ISA and OS underscores the interdependence between individual competence and institutional backing in achieving sustainable digital workplace performance. This alignment not only safeguards sensitive institutional data but also promotes operational effectiveness, employee satisfaction, and institutional trust. Hence, organisations must cultivate a comprehensive culture of information security awareness while reinforcing organisational support frameworks to sustain high levels of productivity and strengthen resilience against the dynamic challenges posed by the evolving digital threat landscape.

RECOMMENDATION

Considering the empirical findings of this study, the following recommendations are offered to enhance information security awareness, organisational support, and job performance among secretarial professionals:

1. The University of Ibadan should sustain high job performance among secretarial professionals by providing continuous professional development programs and periodic performance audits based on clear KPIs.
2. Organisational support should be improved through investment in modern secure digital tools, expanded advanced digital administration training, and formal recognition systems for exceptional contributions.
3. Information security awareness should be deepened through targeted sensitisation workshops on the broader institutional consequences of security breaches and scenario-based drills to strengthen readiness.
4. Mandatory ISA modules should be integrated into annual training and induction programs, complemented by regular cyber threat updates and an ISA certification scheme for secretarial staff.
5. Perceived organisational support should be enhanced by fostering open supervisor-staff communication, ensuring timely IT assistance, and creating career development pathways linked to skills and performance.
6. An integrated strategy should be adopted that combines ISA initiatives with organisational support measures, pairing security training with secure tools, clear policies, and recognition programs.

REFERENCES

1. Aakash J., (2021). “COVID-19 Security Impact: Rise of Shadow IT.” Arista Community Central. Accessed on 13 August, 2025. https://arista.my.site.com/AristaCommunity/s/article/COVID-19-Security-Impact-Rise-of-Shadow-IT
2. Abosede, S. C. & Akintola, O. A. (2015). Information and Communication Technology Facilities' Utilization and Job Performance of Secretaries in Public and Private Universities in Ogun State International Journal of Managerial Studies and Research (IJMSR) 3(3), 44-52.
3. Ahsan, M. N., Alam, S., Kokash, H., & Ahmed, S. (2026). Employees cybersecurity compliance behaviour: Insight from PMT, TPB and OCT theories. Information Security Journal: A Global Perspective, 1-23.
4. AlKalbani, A., Deng, H., & Kam, B. (2016). Investigating the role of socio-organizational factors in the information security compliance in organizations. arXiv preprint arXiv:1606.00875.
5. Al-Molhem, N. R., Rahal, Y., & Dakkak, M. (2019). Social network analysis in Telecom data. Journal of Big Data, 6(1), 99.
6. Alsaad, A., Al-Okaily, M., 2022. Acceptance of protection technology in a time of fear: the case of Covid-19 exposure detection apps. Inf. Technol. People 35 (3), 1116–1135. https://doi.org/10.1108/ITP-10-2020-0719.
7. Alsboul, Y. (2016). Information Security Awareness: Antecedents and Satisfaction Perspective. In AMCIS.
8. Alshammari, M. M., & Al-Mamary, Y. H. (2026). Non-Technical Determinants of Information Security Policy Compliance: An Integrated PMT-TPB Model with Psychological Ownership, Trust, and Social Influence. Computers in Human Behavior Reports, 100947.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

9. Appelbaum, E. (2000). Manufacturing advantage: Why high-performance work systems pay off. Cornell University Press.
10. Blythe, J. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. Proceedings of CHItaly, 92-101.
11. Borman B. C. (2014). Introduction to the Special Issue: Personality and the Prediction of Job Performance: More Than the Big Five, Human Performance, 17(3), 267-269.
12. Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q.: Manag. Inf. Syst. 39 (4), 1–72. https://doi. org/10.25300/MISQ/2015/39.4.5
13. Chang, H.H., Wong, K.H., Lee, H.C., 2022. Peer privacy protection motivation and action on social networking sites: privacy self-efficacy and information security as moderators. Electron. Commer. Res. Appl. 54, 101176. https://doi.org/10.1016/j. elerap.2022.101176
14. Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. Journal of Applied Psychology, 71(3), 500–507. https://doi.org/10.1037/0021-9010.71.3.500
15. Georgiadou, A., Mouzakitis, S. & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur J 35, 486–505
16. Guan, X., Sun, T., Hou, Y., Zhao, L., Luan, Y., & Fan, L. (2014). The relationship between job performance and perceived organizational support in faculty members at Chinese universities: A questionnaire survey. BMC Medical Education, 14, 50. https://doi.org/10.1186/1472-6920-14-50
17. Halboob, W., Alakeel, A., & Derhab, A. (2023). Increasing continuous engagement with open government data. Journal of Global Information Management, 31(1), 1–21. DOI: 10.4018/JGIM.322437
18. Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. Journal of Computer Information Systems, 61(4), 345–356. DOI: 10.1080/08874417.2019.1650676
19. IBM. (2022). Definitive guide to ransomware 2022. Retrieved December 30, 2022, from https://www.ibm.com/downloads/ cas/EV6NAQR4
20. Indah, M., Angelina, A., Claudia, G., Sertivia, D., & Javelin, J. (2022). Analysis of factors affecting information system security behaviour in employees at it company. UltimaInfoSys: Jurnal Ilmu Sistem Informasinull, 29-36. https://doi.org/10.31937/si.v13i1.2660
21. Kalischko, T., & Riedl, R. (2021). Electronic performance monitoring in the digital workplace: conceptualization, review of effects and moderators, and future research opportunities. Frontiers in psychology, 12, 633031.
22. Khando, K., Gao, S., Islam, S., & Salam, A. (2021). Enhancing employees' information security awareness in private and public organizations: A systematic literature review. Computers & Security, 106, 102267. DOI: 10.1016/j.cose.2021.102267
23. Klein, G., & Zwilling, M. (2023). The weakest link: Employee cyber-defense behaviors while working from home. Journal of Computer Information Systemsnull, 1-15. https://doi.org/10.1080/08874417.2023.2221200
24. Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. Science, Technology, & Human Values , 46 (6), 1316-1339.
25. Kő, A., Tarján, G., & Mitev, A. (2023). Information security awareness maturity: Conceptual and practical aspects in Hungarian organizations. Information Technology & People, 36(8), 174–195. DOI: 10.1108/ITP-11-2021-0849
26. Kour, R., & Karim, R. (2021). Cybersecurity workforce in railway: its maturity and awareness. Journal of Quality in Maintenance Engineering, 27(3), 453-464.
27. Kruger, H.; Drevin, L.; Steyn, T. Email security awareness—A practical assessment of employee behaviour. In Proceedings of the Fifth World Conference on Information Security Education, West Point, NY, USA, 19–21 June 2007; Springer: New York, NY, USA, 2007; pp. 33–40.
28. Lavelle, J. (2020). "Gartner CFO survey reveals 74% intend to shift some employees to remote work permanently." Gartner. April 3. Online
29. Marsh, E., Vallejos, E. P., & Spence, A. (2022). The digital workplace and its dark side: An integrative review. Computers in Human Behavior, 128, 107118. https://doi.org/10.1016/j.chb.2021.107118

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

30. Masood H., Azmat, U., Sarwar, S., Adil, I. H., & Mustafa Gillani S. H., (2020) . Impact of Job Satisfaction, Job Stress and Motivation on Job Performance: A Case from Private Universities of Karachi, Kuwait Chapter of the Arabian Journal of Business and Management Review, 9(2), 31-41.
31. Muthuswamy, V. V., & Nithya, N. (2023). Role of cyber security on employees' digital workplace performance: Exploring the effects of employees' digital awareness and organizational support. https://doi.org/10.5281/zenodo.4766604
32. Muthuswamy, V. V., & Nithya, N. (2023). Role of cyber security on employees' digital workplace performance: Exploring the effects of employees' digital awareness and organizational support. International Journal of Cyber Criminology, 17(1), 54-71.
33. NCSAM. (2019). National cybersecurity awareness month. Retrieved April 19, 2021, from https://staysafeonline.org/ resource/ncsam19-report/
34. Ogbanufe, O., Crossler, R.E., Biros, D., 2023. The valued coexistence of protection motivation and stewardship in information security behaviors. Comput. Secur. 124, 102960. https://doi.org/10.1016/j.cose.2022.102960.
35. Okorie, N. C. (2015). Motivational factors and ICT skills as determinants of job performance of academic librarians in university libraries in South-West Nigeria. A dissertation submitted to the department of information resources management, Babcock University, Ilisan Remo.
36. Popoola, K. O. (2023). Organizational characteristics, employee commitment and job performance of secretaries in government-owned tertiary institutions in Oyo State, Nigeria [P.hD thesis, Lead City University]. Lead City University Repository. https://repository.lcu.edu.ng/handle/123456789/670
37. Radha, P., Sayyed, N., & Fathima, Y. (2024). The new normal: Navigating cyber security challenges in remote work policies. NPRC Journal of Multidisciplinary Research., 1 (8), 106-118. https://doi.org/10.3126/nprcjmr.v1i8.73042
38. Rodríguez-Abitia, G., & Bribiesca-Correa, G. (2021). Assessing digital transformation in universities. Future Internet, 13(2), 52.
39. Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 19 (1), 93–114. https://doi.org/10.1080/00223980.1975.9915803.
40. Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & security, 56, 70-82.
41. Saleem, Q. U. A., & Ameen, K. (2024). Exploring the role of library managers in supporting female professionals: Perspectives from Punjab Pakistan. Malaysian Journal of Library and Information Science, 29(2), 107-121.
42. Sanok, D.J., Jr. (2005). An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 23–24 September ; pp. 142–144.
43. Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology, 29(3), 233-244.
44. Vedadi, A., Warkentin, M., (2020). Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. J. Assoc. Inf. Syst. 21 (2), 3.
45. Zhen, J., Dong, K., Xie, Z., & Chen, L. (2022). Factors influencing employees' information security awareness in the telework environment. Electronics, 11(21), 3458.
46. Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Survey of perceived organizational support. Journal of Applied Psychology.
47. Appelbaum, E., Bailey, T., Berg, P., & Kalleberg, A. (2000). Manufacturing advantage: Why high-performance work systems pay off. London, UK: ILR Press.