



## CYBERSECURITY COMPETENCIES REQUIRED BY BUSINESS EDUCATION LECTURERS FOR EFFECTIVE WORKPLACE DIGITAL RECORDS MANAGEMENT IN RIVERS STATE UNIVERSITIES

**Philip Festus Ukata (Ph.D.)\* and Anita Eberechi Amadi (Ph.D.).**

Department of Business Education, Faculty of Education,  
Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Rivers State, Nigeria.

\*Corresponding Author's Email: [philip.ukata@iaue.edu.ng](mailto:philip.ukata@iaue.edu.ng); [ukata4mephilip@yahoo.com](mailto:ukata4mephilip@yahoo.com);  
Tel.: +2348038877937

### Cite this article:

Philip Festus Ukata, Anita Eberechi Amadi (2026), Cybersecurity Competencies Required by Business Education Lecturers for Effective Workplace Digital Records Management in Rivers State Universities. British Journal of Contemporary Education 6(2), 34-51. DOI: 10.52589/BJCE-RMEUXSU3

### Manuscript History

Received: 7 Jun 2026

Accepted: 5 Jul 2026

Published: 16 Jul 2026

### Copyright © 2026 The Author(s).

This is an Open Access article distributed under the terms of Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0), which permits anyone to share, use, reproduce and redistribute in any medium, provided the original author and source are credited.

**ABSTRACT:** *The essential need to protect digital records motivated this study, "Cybersecurity competencies required by business education lecturers for effective workplace digital records management". Two research questions guided the study, and two null hypotheses were tested by comparing how years of teaching experience and educational attainment influenced cybersecurity competencies of the lecturers. A descriptive survey research design was adopted. From a population of 57 business education lecturers, a census survey sampling was employed. A four-point response options questionnaire was used for data collection, and three experts validated it. The reliability of the instrument was established using Cronbach's alpha, which yielded coefficients of 0.71 and 0.72. Mean and standard deviation were used to answer research questions and measure the spread in respondents' opinions, while one-way analysis of variance (ANOVA) was used to test the null hypotheses at a 0.05 level of significance. Findings revealed that foundational understanding of digital protection imperatives, cloud security architecture and implementation excellence, business impact evaluation and operational consequence analysis, artificial intelligence and machine learning security applications of cybersecurity competencies, among others, were highly required and that these cybersecurity competencies are highly beneficial to business education lecturers in public and private sectors for effective workplace digital records management. Based on the findings, it was concluded that those types of cybersecurity competencies were highly required and that cybersecurity competencies are highly beneficial for effective workplace digital records management. Therefore, among other things, it was recommended that business education lecturers should make personal sacrifices from their earnings and engage in cybersecurity competencies training to enable them to acquire very high knowledge and skills to perform on the job and sustain and remain relevant in their areas of operations.*

**KEYWORDS:** Cybersecurity competencies, Business Education, Business Education lecturers, digital records management, effective workplace digital records management.



## INTRODUCTION

Over the years, progress in information and communication technology has caused significant transformations in all facets of human life, particularly in the workplace. As new technologies are adopted in office settings, contemporary tools are being integrated and utilised, leading to innovative approaches to completing office tasks. In support of this, Amaewhule and Wolugbom (2021) observed that the emergence of digital technologies has initiated fresh methods for carrying out office responsibilities in various organisations globally. Nevertheless, the evolution of information and communication technology tools appears to be linked with several challenges, such as cyberattacks, including Denial of Service attacks (DoS) and backdoor breaches, which can impede effective digital records management in workplaces by business education lecturers (Geeks for Geeks, 2024).

Cybersecurity competencies and strategies serve as proactive measures to safeguard digital assets, particularly sensitive academic information. In educational contexts, robust cybersecurity mechanisms ensure the confidentiality, integrity, and availability of data. The introduction of AI into academic record management has brought both opportunities and risks (Nдалу & Nдалу, 2026). The application of automated records introduced complex challenges as cybercriminals increasingly exploit AI-driven techniques for more sophisticated attacks (Nwaiwu & Okoye, 2022). This duality underscores the need for universities to develop comprehensive cybersecurity frameworks that integrate technological, organisational, and human-centred strategies with competencies to prevent attacks.

Existing literature has documented the rising cases of cyberattacks targeting educational institutions worldwide. For example, Adebayo and Ibrahim (2021) noted that Nigerian universities experienced an upsurge in ransomware attacks between 2019 and 2021, exposing the weaknesses of institutional cybersecurity frameworks. Similarly, Alotaibi (2020) emphasised that inadequate security protocols and poor awareness among staff contribute significantly to the vulnerability of academic record systems. In the context of AI machines and blockchain, cybersecurity must evolve from traditional defence mechanisms to advanced intelligent solutions capable of predicting, preventing, and mitigating attacks in real time. For instance, Olagunju and Eze (2022) highlighted the potential of machine learning algorithms for intrusion detection systems, which can identify suspicious activities before they escalate into full-scale breaches.

The integration of AI into cybersecurity strategies with competencies provides opportunities for compliance automation, real-time monitoring, and enhanced auditing of academic records, yet it requires significant investment and technical expertise. Oladipo (2021) stressed that phishing attacks, insider threats, and weak password practices are often more detrimental than purely technical vulnerabilities. This suggests that any cybersecurity strategy must combine technological defences with competencies training, awareness, and institutional culture that prioritise security. AI-powered tools can assist in this regard by enabling adaptive authentication systems, real-time behavioural analysis, and proactive risk assessments (Oyekan & Adekunle, 2023).

In the context of this study, effective workplace digital records management by business education lecturers spans the public and private sectors.



Beyond securely managing students' digital grades, course materials, personal data, published academic documents; some business education lecturers are consultants in the areas of information and communication technology, office information technology, management information systems, digital skills in business education and business management, digital marketing, digital accounting system, website design and website management (Ukata & Nmehielle, 2024a; Ukata & Udeh, 2022). These high IT professional areas with different business dimensions that are usually prone to cybersecurity attacks require a high level of cloud security architecture, artificial intelligence and machine learning security, blockchain security, quantitative risk assessment, and enterprise-level cybersecurity competencies, among others, for effective workplace digital records management.

### **Cybersecurity**

According to Sophos (2026), cybersecurity involves the protection of systems, networks, programs, and data against digital threats. These cyberattacks typically target the unauthorised access, alteration, or destruction of sensitive information, seek to extort money from users, or disrupt regular business activities. Cybersecurity encompasses technologies and best practices aimed at safeguarding IT systems, networks, and data from unauthorised access, cyberattacks, and other security risks. It can be implemented through various means, including firewalls, antivirus software, encryption, authentication, intrusion detection systems, and established security policies (Schulze, 2025).

### **Cybersecurity Competencies**

Cybersecurity competencies comprise a broad set of skills, knowledge, characteristics, behaviours, and roles required to successfully protect hardware, software, and information against cybersecurity threats. These competencies are critical to the development of cybersecurity talent and addressing the growing threat posed by cyberattacks (CNCS, 2026). Modern digital spaces have become more challenging than ever for any organisation trying to secure its most precious assets, sensitive data, and operational infrastructure against advanced threat actors and malicious activities, which is the reason these competencies are required by business education lecturers in managing academic and administrative activities in their public and private sectors.

### **Types of Cybersecurity Attacks**

The following are some of the cybersecurity attacks: Denial of Service Attack (DoS), backdoor attacks, eavesdropping, phishing, spoofing, malware, social engineering, and polymorphic attacks, which means that cybersecurity competencies are taught to business education undergraduates for effective workplace digital records management (Geeks for Geeks, 2024).

### **Types of Cybersecurity Competencies**

The following are some of the cybersecurity strategies and competencies required by university staff to curb cyberattacks and protect digital academic records: encryption of data, authentication and access controls, regular system monitoring and intrusion detection, blockchain technology, cybersecurity awareness and training, artificial intelligence and machine learning, regulatory compliance and policy enforcement (Ndalul & Ndalul, 2026). The below stated and explained are some of the types of cybersecurity competencies required for



effective workplace digital records management (Certkiller, 2026; National Initiative for Cybersecurity Careers and Studies (NICCS), 2026; CNCS, 2026; Coursera, 2026).

### **Foundational Understanding of Digital Protection Imperatives of Cybersecurity Competency**

Digital protection has shifted from a peripheral information technology concern to a core business necessity affecting organisational sustainability, competitive differentiation, and stakeholder trust in a world where connectivity and data reliance continue to deepen. As businesses have embraced a spectrum of fully interconnected, user-facing digital technologies across all functions, the attack surfaces exposed are more expansive than ever before and require holistic protection strategies involving technical controls, process improvements, and human factor considerations. That is why one needs to have the basic contextual awareness of digital vulnerability imperatives of cybersecurity competency.

### **Cloud Security Architecture and Implementation Excellence of Cybersecurity Competency**

Adoption of cloud computing has significantly changed organisational IT infrastructures while posing new security risks, shared responsibility models, and architectural issues that call for specific expertise to properly handle. Identity and access management, data security, network security, compliance monitoring, and incident response in dispersed, multi-tenant systems are just a few of the domains that make up cloud security.

### **Business Impact Evaluation and Operational Consequence Analysis of Cybersecurity Competency**

Translating technical concerns into commercial language that executives and decision-makers can understand is one of the most important aspects of risk management. By assessing the possible effects of a successful cyberattack on the organisation's operations, financial stability, reputation, and compliance status, business impact analysis (BIA) plays a crucial part in this process.

### **Artificial Intelligence and Machine Learning Security Applications of Cybersecurity Competency**

With the ability to automate threat identification, behavioural analysis, and response coordination at scales and speeds that surpass human analytical capabilities, artificial intelligence technologies have become revolutionary tools for cybersecurity operations. To spot subtle trends, unusual behaviours, and new threats that conventional rule-based systems can miss or misunderstand, these technologies process enormous amounts of data from various sources.

### **Comprehensive Risk Evaluation and Strategic Management Approaches of Cybersecurity Competency**

Instead of depending on subjective opinions or marketing claims from security vendors, risk evaluation is a fundamental discipline that assists organisations in identifying and comprehending potential threats, identifying vulnerabilities within their systems, assessing the potential impacts of these risks, and prioritising their security efforts based on objective, data-driven analysis. Organisations must use methodical approaches that integrate quantitative and



qualitative analysis methodologies to produce actionable insights that guide resource allocation and strategic decision-making to effectively manage risk.

### **Structured Threat Analysis and Identification of Potential Vulnerabilities of Cybersecurity Competency**

Threat modelling is a crucial technique in the risk management framework that enables security professionals to methodically identify and assess possible attack vectors, comprehend the capabilities of potential adversaries, and anticipate different exploitation scenarios that could jeopardise organisational assets. These analytical methods are intended to predict how malevolent actors can take advantage of system flaws and accomplish their nefarious objectives.

### **Strategic Implementation and Organisational Integration of Cybersecurity Competency**

For cybersecurity programs to be successful, they must be strategically integrated with organisational culture, operational procedures, and business goals to maximise the return on security investments while promoting business success rather than obstructing operations or innovation projects. Cybersecurity experts who comprehend both technical security requirements and business contexts are needed for this integration.

### **Quantitative Risk Assessment Techniques and Decision-Making Support of Cybersecurity Competency**

Based on the probability of threats, the exploitability of vulnerabilities, and the possible consequences of a successful assault, risk quantification techniques are used to give identified security hazards numerical values. By providing a framework for comparing and analysing different security solutions, these quantifications help businesses determine which investments will reduce risk the most.

### **Ongoing Risk Surveillance and Adaptive Risk Management Strategies of Cybersecurity Competency**

Risk management is a continuous activity that necessitates constant observation of shifting vulnerabilities, increasing threats, and organisational shifts. Maintaining current risk assessments that take into account the dynamic nature of the working environment requires ongoing risk surveillance. In order to adapt their defences to new attack techniques, emerging technology, and changes in business goals, organisations must continuously monitor the threat landscape.

### **Blockchain Security and Distributed Ledger Protection of Cybersecurity Competency**

Blockchain technology has revolutionised data integrity, transaction verification, and decentralised trust mechanisms while posing new security risks that call for specific expertise and defensive tactics. Blockchain security includes infrastructure protection in distributed computing systems, consensus procedures, cryptography implementations, and smart contract security.



## Essential Benefits of Cybersecurity Competencies

Relying on vital digital infrastructure and connected devices is one of the key advantages of cybersecurity for putting into practice efficient workplace digital records management. For efficient workplace digital records management, cybersecurity builds many layers of protection across computers, networks, and data clusters using a combination of people, procedures, and technology (Sophos, 2026). Businesses need cybersecurity to protect confidential information, keep operations running smoothly, and adhere to stringent legal requirements. Therefore, a strong cybersecurity posture reduces the possibility of catastrophic digital records, monetary losses, harm to one's reputation, and company interruption brought on by data breaches (Ukata & Sila-Dikibo, 2020; Ukata, 2019). In essence, by inventorying all hardware, software, and data to assess potential vulnerabilities, weaknesses, and potential threat vectors, cybersecurity also helps identify assets and dangers. By implementing security measures like firewalls, encryption, data loss prevention, and access management to prevent unwanted access, it is utilised to safeguard infrastructure (Cisco, 2026). To spot suspicious activity, unauthorised modifications, or possible breaches in real time, cybersecurity can also identify anomalies through ongoing system and network traffic monitoring. When a security breach or active threat is confirmed, it quickly responds to occurrences by implementing pre-planned containment, isolation, and mitigation techniques.

Effective workplace digital records management necessitates cybersecurity competencies. Cybersecurity professionals, with the aid of automated protocols, recover and patch systems after an attack, restore interrupted systems to normal operation, examine the fundamental cause, and update defences to prevent future attacks (CISA, 2021).

## Digital Records Management (DRM)

Digital Records Management (DRM) is a methodical strategy to capture, organise, safeguard, and manage digital data throughout its existence, according to Rashid (2023). According to Ukata and Wechie (2019), this procedure is crucial for guaranteeing responsibility, openness, and adherence to legal and regulatory obligations. The process of arranging, storing, and monitoring crucial data in a digital format to support companies in making wise decisions is also known as digital records management. DRM facilitates effective document and data management for companies and organisations, guaranteeing quick access to records when action and decision-making are required (Alooba, 2026). Digital records management includes records imaging management, born-digital records management, e-mail management systems, and document management systems (DMS). Document Management Systems (DMSs) manage disorganised data, including spreadsheets and documents, and facilitate the creation, sharing, and control of digital records for use in a regular and productive workplace (Ukata & Wechie, 2019).

## Benefits of Digital Records Management

Aspects of legal and regulatory compliance, risk mitigation and security, operational efficiency and collaboration, cost reduction, and resource optimisation are all significantly impacted by digital records management. Organisations facilitate file organisation through digital records management. Organisations can easily locate required documents in the cloud-based system rather than sifting through mountains of paper (Ukata & Adejola, 2020a). Digital records make it possible for personnel to view crucial documents at any time and from any location. Teams that need to transmit information fast or operate remotely may find this particularly useful.



Compared to paper files, digital records require less physical space. This lowers the expense of storing paper documents while also keeping offices tidy. Lastly, improved security is made possible by the proper security of digital data management. To prevent unwanted access to sensitive data, you can utilise encryption and passwords (Alooba, 2026).

### **Effective Workplace Digital Records Management**

Effective workplace digital records management involves a systematic approach to capturing, organising, securing, and maintaining digital records throughout their lifecycle for effective decision-making in the workplace. Ensuring legal and regulatory compliance by making sure that companies fulfil the requirements of numerous laws and regulations controlling data and information is essential to effective workplace digital records management. Accountability, openness, and adherence to legal and regulatory standards are all dependent on efficient digital records management in the workplace. By putting strong security measures in place to prevent unauthorised access to sensitive information and guarantee data integrity, effective workplace digital records management may also help with risk reduction and security (Ukata & Adejola, 2020a). It helps in engaging in operational efficiency and collaboration by streamlining business operations and facilitating collaboration across teams, especially in remote and hybrid work environments, to achieve success.

Demonstrating best practices such as assessing needs, implementing a classification system, establishing retention schedules, utilising automation, investing in secure storage, training employees, conducting audits, leveraging technology, and developing clear policies and procedures, which require essential cybersecurity competencies through business education by business education lecturers (Avery, 2026).

### **Business Education**

The National Universities Commission (2022) posited that business education is a specialised profession designed to provide students with knowledge, skills, and competence leading to employability and advancement in office occupations; pedagogical skills in teaching business subjects at different levels of the educational system; as well as self-employment or being an employer of labour. As an aspect of vocational education and training, business education is designed to fill the gap between knowledge and practice by exposing students to general education as well as specialised areas in accounting, entrepreneurship, marketing, and office technology and management (Ukata & Nmehielle, 2024b). Business education is also an educational program offered in higher institutions such as universities and colleges of education, with options in the polytechnics, which prepares students for careers in business, both in the private and public sectors, through inculcating in them practical skills and knowledge about usefulness in the business workplace (Ukata et al., 2017). Business education content is an all-encompassing program in which course content is in the areas of business management, business administration, office information management systems, Office Technology and Management, information and communication technology, or Information Management System, Purchase/Supply Education. Others are accounting education, communication skills, English language, distributive education, entrepreneurship education, management/marketing, educational psychology, philosophy and sociology of education, business law, research methodology, etc., which require the application of artificial intelligence (AI). It is an education that theoretically and practically prepares the learners with the required skills needed in the global workplace (Ukata et al., 2018).



## **Business Education Lecturers**

Business education lecturers include teachers of business education of different ages who lecture the business education program courses in the universities, colleges of education, and polytechnics with a choice of different options designed to provide a comprehensive understanding of effective classroom management principles and practices, business principles, office practices, and management systems (Ukata & Amini, 2022). They aim to equip learners with the necessary digital skills to function effectively in the business world as an employer and employee, improve decision-making abilities, and understand management theories and leadership. The curriculum contents typically include subject options such as accounting, marketing, finance, entrepreneurship, operations management, and economics, preparing students for various career paths in business and management. These lecturers require cybersecurity competencies for effective workplace digital records management, as employees and consultants of the global workplace who work with different academic files, such as results files (online and offline), email management, and hosting sites of publications.

## **Justification/Gap of the Study**

Although there is related literature to this study, there is no literature that has the exact purpose of the study, specific objectives, moderating variables, and methodology as in the current study, which makes this study unique. This study is highly justified because it will fill a gap in the body of knowledge by revealing the different types of cybersecurity competencies and their essential benefits required by business education undergraduates for effective workplace digital records management. The findings and recommendations will provide empirical data for stakeholders at different levels to make useful decisions on related problems to this topic: “Cybersecurity competencies required by business education lecturers for effective workplace digital records management in Rivers State Universities.”

## **Subjects and Moderating Variables of the Study**

The subjects for this study are male and female lecturers of the business education program. The lecturers will be of different levels of educational attainment, years of teaching experience, and from different institutions of the Rivers State Universities. Studies have shown that how well lecturers demonstrate their knowledge of cybersecurity competencies and teaching experience required by Business Education undergraduates for effective workplace digital records management depends on their level of educational qualification, training and retraining, age, teaching experience and institutional ownership (Ukata & Mekuri-Ndimele, 2025). For example, lecturers with higher degrees, such as a PhD and an M.Sc./M.Ed., are expected to possess higher knowledge and skills with cybersecurity competencies related to teaching experience than those with HND/B.Sc./B.Ed. (Mekuri-Ndimele & Ukata, 2025; Ezenwafor & Ukata, 2022).

Accordingly, Ukata and Okeke (2023) and Ukata and Nmiehelle (2022) claimed that teaching experience, age, and institutional ownership are among the factors that influence lecturers' knowledge and skills in cybersecurity competencies-related teaching experience for effective workplace digital records management because younger and more experienced lecturers are more likely to possess them than older and less experienced ones. Also, lecturers who have spent 10 years or more teaching cybersecurity competencies-related courses, such as information management technology, management information systems, and advanced word processing, are expected to possess higher knowledge and skills to be able to identify the types



and extent of cybersecurity competencies for effective workplace digital records management than those with less than 10 years of teaching experience (Ukata & Obinichi-Aaron, 2025).

### **Statement of the Problem**

Over numerous years, advancements in information and communication technology have resulted in rapid changes in all aspects of human existence, including the global work environment. Cybersecurity, as an aspect of advancements in information and communication technology, may require knowledge of some types of cybersecurity competencies to nip any breach of information security in the workplace in time by workers like lecturers who work with academic and administrative-related information, such as results files online and offline. Digital records management, as a process of organising, storing, and keeping track of important information in a digital format, may sometimes be prone to cybersecurity attacks; as such, there is a need for cybersecurity competencies for effective workplace digital records management by staff like lecturers. Currently, lecturers are involved in working with different online and offline academic files, such as results files (results coding, upload, and download), email management, and hosting publication sites, including consultancy, which may be prone to cybersecurity attacks.

The problem of this study is that, although there is different literature on cybersecurity competencies, the different types and essentials of cybersecurity competencies required by business education lecturers in the public and private sector for effective workplace digital records management, like results coding, upload and download, email management, hosting publication sites management, and consultancy, remain unknown. This is the reason for this timely investigation, ‘Cybersecurity Competencies Required by Business Education lecturers for Effective Workplace Digital Records Management in Rivers State Universities.’

### **METHODOLOGY**

The study adopted a descriptive survey research design. The population of the study was all 57 business education lecturers from Rivers State University (RSU) and Ignatius Ajuru University of Education (IAUE) (Department of Business Education, RSU & IAUE, 2026). Rivers State University (RSU, 31) and Ignatius Ajuru University of Education (IAUE, 26). Data from the Department of Business Education, University of Port Harcourt, was not accessible at the time of this investigation. The census survey technique was adopted to sample all 57 business education lecturers because it is a manageable size. The instrument used for data collection was a self-designed four-point response options questionnaire titled “Cybersecurity Competencies Required by Business Education Lecturers for Effective Workplace Digital Records Management.” The questionnaire contains two sections, A and B. Section A has 17 items, while Section B has 10 items, respectively, and they were rated as very highly (4.50 – 5.00), highly (3.50 – 4.49), lowly (2.50 – 3.49), and very lowly (1.50 – 2.49). The questionnaire was subjected to face and content validation by three experts from the Faculty of Education, Ignatius Ajuru University of Education (two from the Department of Business Education and one from Educational Psychology). The measure of internal consistency method was used to establish the reliability of the instrument. The instrument was administered to 16 lecturers from the University of Uyo who were not part of the population of the study. The Cronbach’s alpha was applied to compute the reliability coefficient, which yielded alpha values of 0.71 and 0.72. These high reliability coefficients show that the instrument was reliable for the study. The



researchers personally administered the copies of the questionnaire to the respondents in their schools with the help of two research assistants who were adequately briefed on the modalities to follow. The researchers first visited each of the universities and sought consent from the relevant heads of department for the study. Thereafter, the researchers and assistants visited each school and handed over the required number of copies of the instrument to the heads of the department to distribute to the business education lecturers for completion and revisited after five working days to retrieve the completed copies. Fifty-five copies of the instrument were correctly filled, retrieved, and used for data analysis. The arithmetic mean and standard deviation were used to answer the two research questions and ascertain how homogeneous or heterogeneous the respondents' opinions were relative to the questionnaire items and the aggregated mean. The one-way analysis of variance (ANOVA) was used to test the two null hypotheses at a 0.05 level of significance. The ANOVA was used for the two null hypotheses because it measured one categorical independent variable with three levels of moderating variables. A null hypothesis was accepted where the calculated significant (Sig.) value (p-value) was greater than or equal to ( $\geq$ ) the alpha value of 0.05. Otherwise, the null hypothesis was rejected. The data analysis was carried out using Statistical Package for Social Sciences (SPSS) version 25.

## Result Presentation, Analysis and Discussion

### Research Question 1

What are the types of cybersecurity competencies required by business education lecturers for effective workplace digital records management?

**Table 1: Respondents' mean ratings on the types of cybersecurity competencies required by Business Education lecturers for effective workplace digital records management**

| SN | Items statement                                                                                        | $\bar{X}$ | SD  | N = 55<br>Remarks |
|----|--------------------------------------------------------------------------------------------------------|-----------|-----|-------------------|
| 1  | Foundational understanding of digital protection imperatives of cybersecurity competency               | 3.57      | .82 | Highly            |
| 2  | Cloud security architecture and implementation excellence of cybersecurity competency                  | 3.61      | .75 | Highly            |
| 3  | Business impact evaluation and operational consequence analysis of cybersecurity competency            | 3.70      | .81 | Highly            |
| 4  | Artificial intelligence and machine learning security applications of cybersecurity competency         | 3.67      | .70 | Highly            |
| 5  | Comprehensive risk evaluation and strategic management approaches of cybersecurity competency          | 3.71      | .74 | Highly            |
| 6  | Structured threat analysis and identification of potential vulnerabilities of cybersecurity competency | 3.58      | .82 | Highly            |
| 7  | In-Depth vulnerability identification and testing mechanisms of cybersecurity competency               | 3.61      | .80 | Highly            |
| 8  | Strategic implementation and organisational integration of cybersecurity competency                    | 3.67      | .82 | Highly            |
| 9  | Quantitative risk assessment techniques and decision-making support of cybersecurity competency        | 3.71      | .81 | Highly            |



|                       |                                                                                                               |             |     |               |
|-----------------------|---------------------------------------------------------------------------------------------------------------|-------------|-----|---------------|
| 10                    | Professional development and career advancement strategies for cybersecurity competency                       | 3.71        | .71 | Highly        |
| 11                    | Ongoing Risk Surveillance and Adaptive Risk Management Strategies of Cybersecurity Competency                 | 3.76        | .79 | Highly        |
| 12                    | Emerging security domains and the future of cybersecurity competency                                          | 3.72        | .85 | Highly        |
| 13                    | Integrating risk management into organisational governance and strategic planning of cybersecurity competency | 3.58        | .80 | Highly        |
| 14                    | Blockchain security and distributed ledger protection of cybersecurity competency                             | 3.60        | .78 | Highly        |
| 15                    | Digital marketing security protection, cybersecurity competency                                               | 3.77        | .73 | Highly        |
| 16                    | Security education and awareness program development of cybersecurity competency                              | 3.71        | .81 | Highly        |
| 17                    | Advanced penetration testing and vulnerability assessment of cybersecurity competency                         | 3.75        | .73 | Highly        |
| <b>Aggregate Mean</b> |                                                                                                               | <b>3.66</b> |     | <b>Highly</b> |

Table 1 shows that all 17 listed types of cybersecurity competencies were highly required by business education lecturers for effective workplace digital records management, with mean scores that ranged from 3.57 to 3.77. Also, the aggregated mean score of 3.66 shows that all the listed types of cybersecurity competencies were highly required by business education lecturers for effective workplace digital records management.

The standard deviations for the 17 listed items ranged from 0.78 to 0.88, which shows that respondents were homogeneous in their opinions that all the listed types of cybersecurity competencies were highly required by business education lecturers for effective workplace digital records management.

## Research Question 2

What are some of the essential benefits of cybersecurity competencies to business education lecturers for effective workplace digital records management?

**Table 2: Respondents' Mean Ratings on Some of the Essential Benefits of Cybersecurity Competencies to Business Education lecturers for effective workplace digital records management**

| SN | Item's statement                                                                                                                                                       | $\bar{X}$ | SD  | N = 55<br>Remarks |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----|-------------------|
| 18 | Cybersecurity assists users in relying on critical digital infrastructure and connected devices.                                                                       | 3.62      | .72 | Highly            |
| 19 | Cybersecurity utilises a combination of people, processes, and technology to build multiple layers of defence across computers, networks, and data clusters for users. | 3.65      | .71 | Highly            |



|                       |                                                                                                                                                                                               |             |     |               |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----|---------------|
| 20                    | Organisations implement cybersecurity to safeguard proprietary data, maintain operational uptime, and comply with strict legal regulations                                                    | 3.75        | .73 | Highly        |
| 21                    | A cybersecurity posture minimises the risk of devastating digital records, financial losses, reputational damage, and business disruption caused by data breaches.                            | 3.77        | .71 | Highly        |
| 22                    | Cybersecurity assists in identifying assets and risks by taking inventory of all hardware, software, and data to evaluate potential vulnerabilities, weaknesses, and potential threat vectors | 3.72        | .75 | Highly        |
| 23                    | Cybersecurity protects infrastructure by deploying security controls such as firewalls, encryption, data loss prevention, and access management to block unauthorised entry                   | 3.58        | .74 | Highly        |
| 24                    | Cybersecurity also detects anomalies via continuous monitoring of systems and network traffic to identify suspicious behaviour, unauthorised changes, or potential intrusions in real time.   | 3.60        | .68 | Highly        |
| 25                    | Cybersecurity promptly responds to incidents by executing pre-planned containment, isolation, and mitigation strategies immediately when a security breach or active threat is validated      | 3.67        | .67 | Highly        |
| 26                    | Cybersecurity recovers, patches the attack, and restores disrupted systems to normal operation.                                                                                               | 3.74        | .73 | Highly        |
| 27                    | Cybersecurity analyses the root cause of the attack and updates defences to prevent future exploits.                                                                                          | 3.71        | .71 | Highly        |
| <b>Aggregate Mean</b> |                                                                                                                                                                                               | <b>3.68</b> |     | <b>Highly</b> |

Table 2 shows that all 10 listed items are highly essential benefits of cybersecurity competencies to business education lecturers for effective workplace digital records management, with mean scores that ranged from 3.58 to 3.77. Also, the aggregated mean score of 3.68 shows that all 10 listed items are highly essential benefits to business education undergraduates for effective workplace digital records management.

The standard deviations for the 10 listed items ranged from 0.67 to 0.74, which shows that respondents were homogeneous in their opinions that all the listed items are highly essential benefits to cybersecurity competencies for business education lecturers for effective workplace digital records management.

### Testing Hypotheses

**H0<sub>1</sub>:** There is no significant difference in the mean responses of lecturers on the types of cybersecurity competencies required for effective workplace digital records management based on their years of experience.



**Table 3: ANOVA summary of lecturers' responses on the types of cybersecurity competencies required for effective workplace digital records management based on their years of experience.**

| Sources of Variance | Sum of Squares | Df        | Mean Square | F-cal. | Sig. | Decision        |
|---------------------|----------------|-----------|-------------|--------|------|-----------------|
| Between Groups      | 2.458          | 2         | 1.229       | 1.815  | .283 | Accept $H_{01}$ |
| Within Groups       | 55.357         | 53        | .677        |        |      |                 |
| <b>Total</b>        | <b>57.815</b>  | <b>55</b> |             |        |      |                 |

Table 3 shows a calculated F-value of 1.81 with a significant (sig.) p-value of 0.28, which is greater than the alpha value of 0.05 ( $0.28 > 0.05$ ) at degrees of freedom of 2 and 53. Therefore, the null hypothesis ( $H_{01}$ ) was accepted. This means that there is no significant difference in the lecturers' responses on the types of cybersecurity competencies required for effective workplace digital records management based on their years of experience.

**H02:** A significant difference does not exist in the mean responses of male and female lecturers on the essential benefits of cybersecurity competencies required for effective workplace digital records management based on their educational attainment.

**Table 4: ANOVA summary of lecturers' responses on some of the essential benefits of cybersecurity competencies for effective workplace digital records management based on their educational attainment.**

| Sources of Variance | Sum of Squares | Df        | Mean Square | F-cal. | Sig. | Decision        |
|---------------------|----------------|-----------|-------------|--------|------|-----------------|
| Between Groups      | 2.558          | 2         | 1.279       | 1.889  | .293 | Accept $H_{02}$ |
| Within Groups       | 56.357         | 53        | .677        |        |      |                 |
| <b>Total</b>        | <b>58.915</b>  | <b>55</b> |             |        |      |                 |

Table 4 shows a calculated F-value of 1.27 with a significant (sig.) p-value of 0.29, which is greater than the alpha value of 0.05 ( $0.29 > 0.05$ ) at degrees of freedom of 2 and 53. Therefore, the null hypothesis ( $H_{02}$ ) was accepted. This means that a significant difference does not exist in the lecturers' responses on the essential benefits of cybersecurity competencies required for effective workplace digital records management based on their educational attainment.

## DISCUSSION OF FINDINGS

Findings of the study showed that all the listed types of cybersecurity competencies were highly required by business education lecturers for effective workplace digital records management. The findings are in agreement with the views of Certkiller (2026); National Initiative for Cybersecurity Careers and Studies (2026), CNCS (2026); and Coursera (2026), who argued that, foundational understanding of digital protection imperative, cloud security architecture and implementation excellence, business impact evaluation and operational consequence analysis, artificial intelligence and machine learning security applications of cybersecurity



competency are among the types of cybersecurity competencies that are highly required by business education lecturers for effective workplace digital records management.

The findings as well see eye to eye with the assertions of Ndalu and Ndalu (2026) who noted that some of the cybersecurity strategies and competencies required by university staff to curb cyberattacks and protecting digital academic records include but not limited to; encryption of data, authentication and access controls, regular system monitoring and intrusion detection, blockchain technology application, cybersecurity awareness and training, artificial intelligence and machine learning, regulatory, and compliance and policy enforcement. Furthermore, Olagunju and Eze (2022) highlighted the potential of machine learning algorithms for intrusion detection systems, which can identify suspicious activities before they escalate into full-scale breaches. The integration of AI into cybersecurity strategies provides opportunities for compliance automation, real-time monitoring, and enhanced auditing of electronic academic records, which require significant investment and technical expertise.

Findings of the study also indicate highly essential benefits of cybersecurity competencies for business education lecturers for effective workplace digital records management. The discoveries see eye to eye with Sophos (2026), Cisco (2026), and CISA (2021), who expressed that cybersecurity, among other things, assists users in relying on critical digital infrastructure and connected devices; utilizes a combination of people, processes, and technology to build multiple layers of defence across computers, networks, and data clusters for users; safeguards proprietary data; maintains operational uptime; complies with strict legal regulations; and minimizes the risk of devastating digital records, financial losses, reputational damage, and business disruption caused by data breaches. Additionally, findings of the study showed that there is no significant difference in the mean responses of lecturers on the types of cybersecurity competencies required by business education lecturers for effective workplace digital records management based on their years of experience. The findings agreed with the studies by Chukwu and Umeh (2023), which indicate that universities need adequate funding, experienced staff, trained personnel, and raised infrastructure to meet standards, integration of AI machines into cybersecurity strategies, which provides opportunities for compliance automation, making significant investments to raise their technical expertise to have competencies in real-time, monitoring, and enhanced auditing of digital academic records. The findings also concur with the postulations of Ukata and Okeke (2023) and Ukata and Nmihelle (2022) that teaching experience and age are among the factors that influence lecturers' knowledge and skills in cybersecurity competencies related to effective workplace digital records management, because younger and more experienced lecturers are more likely to possess them than older and less experienced ones.

Years of experience in artificial intelligence and machine learning as AI-driven tools are increasingly deployed to detect anomalies, predict cyberattacks, and automate responses to emerging threats. These technologies enhance proactive security for academic institutions managing large volumes of digital records (Eze et al., 2022). Likewise, training students, faculty members, and administrators with good experience in cybersecurity best practices significantly reduces risks associated with phishing, weak passwords, and accidental data exposure (Bada et al., 2019). Also, lecturers who have spent 10 years or more teaching cybersecurity competencies-related courses, such as information management technology, information technology, management information systems, and advanced word processing, are expected to possess higher knowledge and skills to be able to identify the types and extent of benefits of cybersecurity competencies for effective workplace digital records management



than those with less than 10 years of teaching experience (Ukata & Obinichi-Aaron, 2025). This means that teaching experience and age are among the factors influencing lecturers' knowledge and skills in cybersecurity-related teaching for effective workplace digital records management.

Furthermore, the study's findings showed that there is no significant difference in the mean responses of lecturers regarding the essential benefits of cybersecurity competencies for business education lecturers in effective workplace digital records management, based on their educational attainment.

The findings aligned with the thoughts of Ndalul and Ndalul (2026) posited that training and education on Artificial Intelligence (AI) have emerged as a transformative tool in enhancing cybersecurity by enabling proactive detection, prevention, and response to evolving threats. Additionally, unlike traditional security systems that rely on predefined rules, AI-powered tools such as machine learning (ML), deep learning, and natural language processing (NLP) can analyse vast amounts of data in real time to identify patterns, anomalies, and potential intrusions (Buczak & Guven, 2016). AI helps security systems adapt dynamically, thereby improving the detection of zero-day attacks and sophisticated malware that conventional methods often miss (Zhang et al., 2022). The findings similarly harmonise with the thoughts of Mekuri-Ndimele and Ukata (2025) and Ezenwafor and Ukata (2022), who averred that how well lecturers demonstrate their knowledge of cybersecurity competencies and teaching experience required by business education lecturers for effective workplace digital records management depends on their level of educational qualification, training, and retraining. For example, lecturers with higher degrees, such as a PhD and an M.Sc./M.Ed., are expected to possess higher knowledge and skills with cybersecurity competencies related to teaching experience than those with HND/B.Sc./B.Ed. This means that educational qualifications play a vital role in demonstrating knowledge of cybersecurity competencies required by Business Education lecturers for effective workplace digital records management.

## CONCLUSION

Based on the findings that emanated from the discussions of the study, it was concluded that different types of cybersecurity competencies were highly required by Business Education lecturers in public and private sectors for effective workplace digital records management. Cybersecurity competencies are also highly beneficial to Business Education lecturers for effective workplace digital records management. Correspondingly, teaching experience and educational qualifications are among the factors that influence lecturers' knowledge and skills in cybersecurity competencies in demonstrating knowledge of cybersecurity competencies required by business education undergraduates for effective workplace digital records management.

## RECOMMENDATIONS

Based on the findings and conclusions of the study, the following recommendations were made:



1. Since whatever knowledge one acquires remains with the person, the business education lecturers should make personal sacrifices from their earnings and engage in cybersecurity competencies training through online and offline short courses to enable them to acquire very high knowledge and skills to perform on the job as well as sustain and remain relevant in their areas of operations. Tertiary institutions running the business education program should send lecturers for specialised training in types of cybersecurity competencies to aid them in gaining the needed skills, since the training may be expensive for lecturers to bear.
2. Rivers State Universities running business education programs should organise regular training on the highly essential benefits of cybersecurity competencies to business education undergraduates for effective workplace digital records management.
3. Since the level of educational attainment and years of experience play vital roles in identifying the types and essential benefits of cybersecurity competencies needed by business education undergraduates for effective workplace digital records management, business educators with the required academic qualifications and years of experience should be employed by institutions running the business education program. These will assist in the implementation of the cybersecurity competencies curriculum and transfer cybersecurity competencies skills to learners to acquire the needed employability skills.

## REFERENCES

- Adebayo, O., & Ibrahim, M. (2021). Ransomware threats and cybersecurity challenges in Nigerian universities. *Journal of Information Security and Digital Research*, 9(2), 55–67.
- Alooba, (January 10, 2026). Digital records management <https://www.alooba.com/skills/tools/filing-and-record-keeping-345/digital-records-management/>, May 27<sup>th</sup>, 2026.
- Alotaibi, B. (2021). Cybersecurity challenges in higher education institutions: A systematic review. *Education and Information Technologies*, 26(5), 6271–6290.
- Amaewhule, W., & Wolugbom, K. R. (2021). Competencies required of office management and technology graduating students for effective performance in modern office. *International Journal of Innovative Education Research*, 9(2), 37–49.
- Avery, K. (February, 2026). The benefits of digital records management in the modern workplace. <https://modernbusinesslife.com/the-benefits-of-digital-records-management-in-the-modern-workplace/> on May 28<sup>th</sup>, 2026.
- Bada, A., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.
- Certkiller, (January 20, 2026). Complete guide to essential cybersecurity competencies for modern professionals. <https://www.certkiller.com/blog/complete-guide-to-essential-cybersecurity-competencies-for-modern-professionals/>, May 31<sup>st</sup>, 2026.
- Cisco, (April 10, 2026). What is cybersecurity? <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html> on May 27<sup>th</sup>, 2026.
- CNCS, (January 1, 2026). Cybersecurity-competencies-framework. <https://cncs.gov.pt/docs/cybersecurity-competencies-framework-cnccs.pdf> on May 30<sup>th</sup>, 2026.



- CNCS, (March 1, 2026). Cybersecurity competencies framework. <https://cncs.gov.pt/docs/cybersecurity-competencies-framework-cnccs.pdf>, May 12th, 2026.
- Coursera, (February, 2026). Essential skills for cybersecurity analysts in 2026. <https://www.coursera.org/articles/cybersecurity-analyst-skills?msocid=2b761493ff4168682c120073fe666988>, May 5th, 2026.
- Eze, S. C., Chinedu-Eze, V. C., Bello, A. O., & Inegbedion, H. (2022). Digital transformation and cybersecurity in higher education institutions: An empirical investigation. *International Journal of Educational Management*, 36(6), 795–814.
- Geeks for Geeks, (2024). Computer security – overview. Retrieved from <https://www.geeksforgeeks.org/computer-security-overview/> on the 10th June, 2025.
- Mekuri-Ndimele, J. A. & Ukata, P. F. (2025). Application of artificial intelligence (AI) on lecturers' job performances in selected Rivers State tertiary institutions. *The Nigerian Academy of Management Journal*, 20 (1), 9-21.
- Nwaiwu, J., & Okoye, P. (2022). Artificial intelligence and cybersecurity in higher education: A new frontier. *Journal of Digital Transformation in Africa*, 4(1), 41–57.
- Ndal, J. U. & Ndal, T. C. (2026). Cybersecurity Strategies for Protecting Digital Academic Records in the Era of Artificial Intelligence: A Literary Analysis. *International Journal of Educational Management*, 2 (2), 253-264.
- National Universities Commission (2022). Core curriculum and minimum academic standard for the Nigerian university system (CCMAS). A publication of the National Universities Commission, Abuja, Nigeria.
- National Initiative for Cybersecurity Careers and Studies (NICCS), (February 15, 2026). NICE workforce framework for cybersecurity. <https://niccs.cisa.gov/tools/nice-framework>, May 20<sup>th</sup>, 2026.
- NIST, (April 2, 2026). Cybersecurity skills and workforce frameworks. <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/cybersecurity-skills-and>, May 21st, 2026.
- Oladipo, T. (2021). Human factors in cybersecurity: An assessment of Nigerian higher education institutions. *Nigerian Journal of Information and Communication Technology*, 6(2), 29–44.
- Olagunju, K., & Eze, V. (2022). Artificial intelligence and machine learning applications for cybersecurity in academic institutions. *Journal of Computer Science and Innovation*, 10(4), 88–101.
- Oyekan, J., & Adekunle, B. (2023). AI-driven strategies for academic data protection in developing countries. *Journal of Emerging Trends in Educational Technology*, 12(3), 66–79.
- Rashid, H. A. (December 6, 2023). Digital records management. <https://limbd.org/digital-records-management/> on the May 30<sup>th</sup>, 2026.
- Schulze, J. (August 11, 2025). What is information technology? 2025 Guide. <https://www.coursera.org/articles/what-is-information-technology?msocid=2b761493ff4168682c120073fe666988>, May 10, 2026.
- Sophos, (May 25, 2026). Cybersecurity defined. <https://www.sophos.com/en-us/cybersecurity-explained/what-is-cybersecurity> on May 30, 2026.
- Ukata, P. F. & Adejola, B. C. (2020a). Indigenous Knowledge Database Management System and Employment Generation: A Case of South - South Nigeria. *Research Journal of Humanities and Cultural Studies (RJHCS)*, 5 (2), 24 – 37.



- Ukata, P. F. & Adejola, B. C. (2020b). Using Modern Information and Communication Technologies in Curbing Academic Libraries Crimes in Rivers State Tertiary Institutions. *World Journal of Innovation and Modern Technology (WJIMT)*, 3 (1), 23 – 38.
- Ukata P. F. Wechie, N. & Nmehielle, E. L. (2017). Instructional strategies and teaching of business education in Rivers State. *International Journal of Education and Evaluation*, 3 (9), 20-36.
- Ukata P. F., Nmehielle, E. L. (2024a). Office technology and management (OTM) curriculum development and review in Nigeria: Opportunities, challenges and trends in tertiary institutions in Rivers State. *NAU Journal of Technology and Vocational Education*, 9, (2), 43-55.
- Ukata P. F., Nmehielle, E. L. (2024b). Information and communication technology instructional competencies possessed by lecturers for implementing office management and technology curriculum in tertiary institutions in Rivers State. *Nigerian Journal of Business Education*, 11(2), 318-325.
- Ukata, P. F. & Amini, M. C. (2022). Digital entrepreneurial skills acquired by business education undergraduates for decent work in tertiary institutions in Rivers State. *International Journal of Innovative Education Research*, 10(2), 99-108.
- Ukata, P. F. & Mekuri-Ndimele, J. A. (2025). Teaching students artificial intelligence tools required for digital entrepreneurship to acquire decent employments in selected Rivers State Tertiary Institutions, *IRASS Journal of Multidisciplinary Studies*, 2 (3), 1-8.
- Ukata, P. F. & Obinichi-Aaron, E. O. (2025). Teaching artificial intelligence tools required of undergraduates for communication and digital entrepreneurship in Public Tertiary Institutions in Rivers State. *GRS Journal of Multidisciplinary Research and Studies*, 2 (4), 21-27.
- Ukata, P. F. & Wechie, N. (2019). Electronic records management and national development: A Case of Nigeria. *International Journal of Social Science and Management*, 5 (2), 35 – 57.
- Ukata, P. F. & Udeh, C. P. (2022). Utilisation of new technologies by business education lecturers for teaching accounting courses in tertiary institutions in Rivers State. *International Journal of Innovative Information Systems & Technology Research*, 10(2), 29-38.
- Ukata, P. F. (2019). *Business education students' learning experiences and programme satisfaction*. Germany: Lap Lambert Academic Publishing.
- Ukata, P. F. Silas-Dikibo, I. D. (2020). Extent of students' satisfaction with business experiences acquired through business education programme in Rivers State universities. *World Journal of Entrepreneurial Development Studies (WJEDS)*, 5 (2), 1- 11.
- Ukata, P. F., Adejola, B. C. & Okoye, A. J. C (2018). Business education students' learning experience and programme satisfaction in Rivers State University. *World Journal of Innovation and Modern Technology*, 2 (1), 9-34.