



Ignatius Ajuru University of Education, Port Harcourt, Nigeria
Research and Development Centre

1st International Conference and Exhibition on Research, Innovation and Development (ICERID 2026)
Proceedings URL: <https://iauejournals.com/index.php/ICERID> Website: <https://icerid.online>



ISBN: 978-978-63205-1-9

June 2026; Page No. 545-555

Cybersecurity Skills Acquired by Business Education Learners for Effective Workplace Digital Records Management in Universities in Rivers State

*Ukata, P. F., & Sam-Eleyi, F. O.

Department of Business Education, Ignatius Ajuru University of Education, Port Harcourt, Nigeria.

*Corresponding author email: philip.ukata@iaue.edu.ng

Abstract

The indispensable need to know the skills acquired to protect digital records motivated this study, “Cybersecurity skills acquired by Business Education learners for effective workplace digital records management in Universities in Rivers State.” Two research questions guided the study, and two null hypotheses were tested. A descriptive survey research design was adopted. From a population of 554 Business Education learners, a census survey sampling was employed. A four-point response options questionnaire was used for data collection, and it was validated by three experts. The reliability of the instrument was established using Cronbach’s alpha, which yielded coefficients of 0.67 and 0.68. Mean and Standard Deviation were used to answer research questions and measure the spread in respondents’ opinions, while an independent t-test was used to test the null hypotheses at a 0.05 level of significance. Findings revealed that the types of cybersecurity skills mentioned were lowly acquired, and that there is a high level of benefits of cybersecurity skills to Business Education learners for effective workplace digital records management. Based on the findings, it was concluded that those types of cybersecurity skills were highly needed to be acquired for effective workplace digital records management. Therefore, among other things, it was recommended that Universities in Rivers State running Business Education programmes should ensure that learners are exposed to the different types of cybersecurity skills and their benefits for effective workplace digital records management.

Keywords: Cybersecurity Skills, Business Education, Business Education Learners, 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 Attack (DoS) and backdoor breaches, which can impede effective digital records management in workplaces by undergraduates (Geeks for Geeks, 2024).

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,

545 | Cite this paper as:

Ukata, P.F., & Sam-Eleyi, F.O. (2026). Cybersecurity skills acquired by business education learners for effective workplace digital records management in universities. In *Proceedings of the 1st International Conference and Exhibition on Research, Innovation and Development (ICERID)*, Ignatius Ajuru. University of Education, Port Harcourt, Nigeria. (Vol. 1, pp. 545-555).

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 skills 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 cyber-attacks (CNCS, 2026). Modern digital spaces have become more challenging than ever for any organisation trying to secure their most precious assets, sensitive data and operational infrastructure against advanced threat actors and malicious activities. What this means is skills and knowledge related to cybersecurity for managing digital records at work effectively.

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). The below stated and explained are some of the types of cybersecurity skills required for effective workplace digital records management (Certkiller, 2026; National Initiative for Cybersecurity Careers and Studies (NICCS), 2026; CNCS, 2026; Coursera, 2026).

1. **Business Impact Evaluation and Operational Consequences of Cybersecurity Skills**
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.
2. **Foundational Understanding of Digital Protection Imperatives of Cybersecurity Skills**
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 and cybersecurity skills for protecting digital records.
3. **Risk Assessment Techniques and Decision-Making Support of Cybersecurity Skills**
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.
4. **Risk Surveillance and Adaptive Risk Management Strategies of Cybersecurity Skills**
Risk management is a continual 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.
5. **Cloud Security Architecture and Implementation Excellence of Cybersecurity Skills**
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.

6. Artificial Intelligence and Security Applications of Cybersecurity Skills

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. In order 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.

7. Risk Evaluation and Strategic Management Approaches of Cybersecurity Skills

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.

8. Threat Analysis and Identification of Potential Vulnerabilities of Cybersecurity Skills

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.

9. Strategic Implementation and Organisational Integration of Cybersecurity Skills

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.

10. Blockchain Security and Distributed Ledger Protection of Cybersecurity Skills

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.

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; Ukata & Mekuri-Ndimele, 2025). Businesses need cybersecurity to protect confidential information, keep operations running smoothly, and adhere to stringent legal requirements for employees. Therefore, a strong cybersecurity posture acquired by learners reduces the possibility of catastrophic data loss, monetary losses, harm to one's reputation, and company interruption brought on by data breaches. 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. In order 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. It recovers and patches the attack, restores interrupted systems to normal operation, examines the assault's fundamental cause, and updates defences to prevent future attacks.

Digital Records Management (DRM) is a methodical strategy to capturing, organising, safeguarding, and managing digital data throughout their 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 include 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).

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. You can easily locate what you need on a computer or cloud-based system rather than sifting through mountains of paper (Ukata & Adejola, 2020a). Digital records make it possible for you 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 involves a systematic approach to capturing, organising, securing, and maintaining digital records throughout their lifecycle for effective decision-making in the workplace, which are skills required by learners 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). Effective workplace digital records management 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 undergraduates (Avery, 2026).

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 or Office Information Management (Ukata & Nmehielle, 2024a). Business Education is also an educational programme 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, knowledge about or usefulness in the business workplace (Ukata et al, 2017).

Business Education contents are an all-encompassing programme in which course contents are in the areas of Business Management, Business Administration, Office Information Management System, Office Technology and Management, and Information and Communication Technology or Information Management System, Purchase/Supply Education (Ukata & Udeh, 2022). Others are Accountancy 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 with cybersecurity skills (Ukata & Sila-Dikibo, 2020; Ukata, 2019).

It is an education that theoretically and practically prepares the learners with the required skills needed at the global workplace (Ukata, Adejola & Okoye, 2018). Business Education programme is offered as a course in universities, colleges of education and as an option in polytechnics by undergraduates.

Business Education learners include learners of different ages who enrolled for the Business Education programme in 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). The aim of Business Education to equip learners with the necessary 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 typically includes subject options such as accounting, marketing, finance, entrepreneurship, operations management, and economics, preparing students for various career paths in business and management. These learners in Universities in Rivers State require cybersecurity skills for effective workplace digital records management as employers and employees of the 21st-century workplace. Rivers State Universities are the two Rivers State-owned universities that run the Business Education Programme. They are Rivers State University and Ignatius Ajuru University of Education. These are universities that run the Business Education programme as designed by the National University Commission in a manner to equip Business Education learners with the required digital skills for a global work environment; as such, cybersecurity skills for effective workplace digital records management.

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 exceptional. This study is highly justified because it will fill a gap in the body of knowledge by revealing the level of the different types of cybersecurity skills acquired and their benefits to Business Education learners 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 skills acquired by Business Education learners for effective workplace digital records management.”

Over the years, improvements in information and communication technology have occasioned hasty changes in all aspects of human existence, including the 21st-century work environment. Cybersecurity, as an aspect of advancements in information and communication technology, requires knowledge of some level of the types of cybersecurity skills to nip any cracks in information security at the global workplace in time. 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, the need for some level of cybersecurity skills acquisition for effective workplace digital records management by learners of Business Education who will graduate to become information managers in the global workplace. The problem of this study is that, although there is different related literature on cybersecurity skills, none is on the level of types and benefits of cybersecurity skills acquired by Business Education learners for effective workplace digital records management. This is the reason for this timely investigation: ‘Cybersecurity Skills Acquired by Business Education Learners for Effective Workplace Digital Records Management in Universities in Rivers State.

The specific objectives of the study were to:

1. Determine the level of the types of cybersecurity skills acquired by Business Education learners for effective workplace digital records management.
2. Identify the benefits of the types of cybersecurity skills acquired by Business Education learners for effective workplace digital records management.

The following research questions guided the study:

1. What is the level of the types of cybersecurity skills acquired by Business Education learners for effective workplace digital records management?

2. What are the benefits of the types of cybersecurity skills acquired by Business Education learners for effective workplace digital records management?

Hypotheses

The following null hypotheses were formulated and tested at 0.05 level of significance:

H01: There is no significant difference in the mean responses of RSU and IAUE learners on the types of cybersecurity skills acquired for effective workplace digital records management.

H02: There is no significant difference in the mean responses of RSU and IAUE Business Education learners on the benefits of the types of cybersecurity skills acquired for effective workplace digital records management.

Methodology

The study adopted a descriptive survey research design. The population of the study was all 554 Business Education learners from Rivers State University (RSU) and Ignatius Ajuru University of Education (IAUE) (Heads of Department of Business Education, RSU & IAUE, 2026). Rivers State University (RSU, 110) and Ignatius Ajuru University of Education (IAUE, 444), comprising all four options in Business Education. Data from the Department of Business Education, University of Port Harcourt, was not accessible at the time of this study. The sample size of this study was 554, using a census sampling technique. The reason for using the entire population was that it was a manageable size for the researchers. The instrument used for data collection was a self-designed four-point response options questionnaire titled "Cybersecurity Skills Acquired by Business Education Learners for Effective Workplace Digital Records Management (CSABEL-EWDRM)". It contains two sections, A and B. Section A has 17 items, while Section B has 10 items, respectively, and 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 contents 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 internal consistency method was used to establish the reliability of the instrument. The instrument was administered to 20 Business Education learners from the University of Uyo who were not part of the population of the study. Cronbach's alpha was applied to compute the reliability coefficient, which yielded alpha values of 0.67 and 0.68. These high reliability coefficients show that the instrument was reliable for the study.

The researchers personally administered the 554 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 Department to distribute to the Business Education learners for completion and revisited after five working days to retrieve the completed copies. Four hundred and fifty-six (456) copies of the instrument, representing eighty-two per cent (82%), 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. An independent t-test was used to test the null hypotheses at a 0.05 level of significance. A null hypothesis was accepted where the calculated significance (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.

Results

Table 1: Respondents' mean ratings on the level of the types of cybersecurity skills acquired by Business Education learners for effective workplace digital records management, N = 456

SN	Items statement	$\bar{X}$	SD	Remarks
1	Understanding the basics of digital protection and cybersecurity skills in the workplace	3.07	.82	Lowly
2	Cloud security architecture and implementation excellence of cybersecurity skills	2.45	.75	Very lowly
3	Business impact evaluation and operational consequence analysis of cybersecurity skills	3.03	.81	Lowly
4	Artificial intelligence and security applications of cybersecurity skills	3.07	.70	Lowly
5	Comprehensive risk evaluation and strategic management approaches of cybersecurity skills	3.02	.74	Lowly
6	Threat analysis and identification of potential vulnerabilities of cybersecurity skills	3.04	.82	Lowly
7	Vulnerability identification and testing mechanisms of cybersecurity skills	3.01	.80	Lowly
8	Implementation and organisational integration of cybersecurity skills	3.02	.82	Lowly
9	Risk assessment techniques and decision-making support of cybersecurity skills	3.01	.81	Lowly
10	Professional development and career advancement strategies of cybersecurity skills	3.01	.71	Lowly
11	Risk surveillance and adaptive risk management strategies of cybersecurity skills	2.34	.79	Very lowly
12	Security domains and the future of cybersecurity skills	3.02	.81	Lowly
13	Integrating risk management into organisational governance and strategic planning of cybersecurity skills	2.44	.77	Very lowly
14	Blockchain security and distributed ledger protection of cybersecurity competency	3.02	.78	Lowly
15	Blockchain security and distributed ledger protection of cybersecurity skills	2.43	.73	Very lowly
16	Security education and awareness program development of cybersecurity skills	3.01	.81	Lowly
17	Business penetration testing and vulnerability assessment of cybersecurity skills	3.02	.73	Lowly
Aggregate Mean		2.88		Lowly

Table 1 shows that all 13 out of the 17 listed types of cybersecurity skills were lowly acquired by Business Education learners for effective workplace digital records management, with mean scores that ranged from 3.01 to 3.07, while 4 items were very lowly acquired with mean scores that ranged from 2.43 to 2.45. Also, the aggregated mean score of 2.88 indicates that Business Education learners acquired the types of cybersecurity skills for effective workplace digital records management to a low extent. The standard deviations for the 17 listed items ranged from 0.70 to 0.81, which shows that respondents were homogeneous in their opinions that Business Education learners had acquired the types of cybersecurity skills listed for effective workplace digital records management.

Table 2: Respondents' mean ratings on the level of benefits of the types of cybersecurity skills acquired by Business Education learners for effective workplace digital records management **N = 456**

SN	Items statement	$\bar{X}$	SD	Remarks
18	Cybersecurity skills assist users in relying on critical digital infrastructure and connected devices.	3.72	.72	Highly
19	Cybersecurity skills utilise 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 use cybersecurity skills to safeguard proprietary data, maintain operational uptime, and comply with strict legal regulations	3.75	.73	Highly
22	Cybersecurity skills minimise the risk of devastating digital records, financial losses, reputational damage, and business disruption caused by data breaches.	3.76	.71	Highly
23	Cybersecurity skills assist in identifying assets and risks by taking inventory of all hardware, software, and data to evaluate potential vulnerabilities, weaknesses, and potential threat vectors	3.74	.75	Highly
24	Cybersecurity skills are used to protect infrastructure by deploying security controls such as firewalls, encryption, data loss prevention, and access management to block unauthorised entry	3.59	.71	Highly
25	Cybersecurity skills also assist in detecting 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
26	Cybersecurity skills are used to promptly respond to incidents by executing pre-planned containment, isolation, and mitigation strategies immediately when a security breach or active threat is validated	3.69	.67	Highly
27	Cybersecurity skills assist in recovering, patching the attack, and restoring disrupted systems to normal operation.	3.70	.73	Highly
28	Cybersecurity skills are used to analyse the root cause of the attack and update defences to prevent future exploits.	3.71	.71	Highly
Aggregate Mean		3.69		Highly

Table 2 shows that all 10 listed items are of a high level of benefits of cybersecurity skills to Business Education learners for effective workplace digital records management, with mean scores that ranged from 3.59 to 3.71. Also, the aggregated mean score of 3.69 shows that all 10 listed items are of a high level of benefits of cybersecurity skills to Business Education learners for effective workplace digital records management. The standard deviations for the 10 listed items ranged from 0.67 to 0.73, which shows that respondents were homogeneous in their opinions that the listed items are of high benefit to Business Education learners for effective workplace digital records management.

Testing Hypotheses

Table 3: Independent t-test Analysis of RSU and IAUE learners on the types of cybersecurity skills acquired for effective workplace digital records management.

Group	N	$\bar{X}$	SD	t	df	Sig.	Decision
RSU Learners	90	3.18	0.65	0.40	452	0.590	Not Significant
IAUE Learners	364	3.13	0.71				

The result in Table 3 shows that RUS learners recorded a mean score of 3.18 (SD = 0.65), while IAUE learners recorded a mean score of 3.13 (SD = 0.71). The t-test analysis yielded a t-value of 0.40 with a degree of freedom of 452 and a p-value of 0.590. Since the p-value is greater than the 0.05 level of significance ($p > 0.05$), the null hypothesis is accepted. This means that there is no significant difference in the mean responses of RSU and IAUE learners on the types of cybersecurity skills acquired for effective workplace digital records management.

Table 4: Independent t-test analysis of RSU and IAUE Business Education learners on the level of benefits of the types of cybersecurity skills acquired for effective workplace digital records management

Group	N	$\bar{X}$	SD	T	Df	Sig.	Decision
RSU Learners	90	3.38	0.66	0.54	452	0.582	Not Significant
IAUE Learners	364	3.31	0.72				

The result in Table 4 shows that RSU learners recorded a mean score of 3.38 (SD = 0.66), while IAUE learners recorded a mean score of 3.31 (SD = 0.72). The t-test analysis yielded a t-value of 0.54 with a degree of freedom of 452 and a p-value of 0.582. Since the p-value is greater than the 0.05 level of significance ($p > 0.05$), the null hypothesis is not rejected. This means that a significant difference does not exist in the mean responses of RUS and IAUE learners on the level of benefits of the types of cybersecurity skills acquired by them for effective workplace digital records management.

Discussion

Findings of the study showed that Business Education learners had low levels of acquired cybersecurity skills for effective workplace digital records management. The findings agree 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 imperatives of cybersecurity skills, cloud security and implementation excellence of cybersecurity skills, business impact evaluation and operational consequence analysis of cybersecurity skills, artificial intelligence and security applications of cybersecurity skills are among the types of cybersecurity skills that are to be acquired by learners for effective workplace digital records management.

Findings of the study equally show that there is a high level of benefits of cybersecurity skills to Business Education learners for effective workplace digital records management. The findings see eye to eye with Sophos (2026); Cisco (2026), and CISA (2021), who expressed that cybersecurity skills, among other things assists users in relying on critical digital infrastructure and connected devices, utilises a combination of people, processes, and technology to build multiple layers of defence across computers, networks, and data clusters for users, safeguard proprietary data, maintain operational uptime, comply with strict legal regulations and minimises 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 RSU and IAUE learners on the low level of the types of cybersecurity skills acquired by learners for effective workplace digital records management. The findings concur with the postulations of Ukata and Okeke (2023) and Ukata and Nmihelle (2022) that previous experience, skills training and adequate attention in class are among the factors that influence learners' knowledge on the level of the types of cybersecurity skills acquired for effective workplace digital records management. For example, learners who had acquired the skills through informal training and those who paid serious attention in the classroom lessons are expected to do better by acquiring a very high level or high level of cybersecurity skills than those without previous training and who did not pay good attention during classroom sessions (Mekuri-Ndimele & Ukata, 2025; Ezenwafor & Ukata, 2022).

Furthermore, findings of the study showed that a significant difference does not exist in the mean responses of RUS and IAUE learners on the level of benefits of the types of cybersecurity skills acquired by them for effective workplace digital records management. The findings are also aligned with the thoughts of Ukata and Mekuri-Ndimele (2025); Mekuri-Ndimele and Ukata (2025); Ezenwafor and Ukata (2022), who averred that how well learners demonstrate their knowledge of the level of benefit of the cybersecurity skills depend on institutional ownership. Accordingly, Ukata and Okeke (2023) and Ukata and Nmihelle (2022) claimed that institutional ownership is among the factors that influence learners' level of knowledge and skills acquisition in cybersecurity skills related to effective workplace digital records management. This is because the level of attention given to ICT infrastructure and application of ICT-related materials during teaching and learning differs from institution to institution, which equally affects learners' skills acquisition.

Conclusion

Based on the findings that emanated from the discussions of the study, it was concluded that those types of cybersecurity skills listed in Table 1 were highly needed to be acquired for effective workplace digital records management, with a high level of benefits. There is no significant difference in the mean responses of RSU and IAUE learners on the low level of the types of cybersecurity skills acquired, and the level of benefits of the types of cybersecurity skills acquired by them for effective workplace digital records management. Also, previous experience through informal training and institutional ownership plays a vital role in the level of the different types of cybersecurity skills and the level of benefits of the types of cybersecurity skills acquired for effective workplace digital records management.

Recommendations

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

1. Universities in Rivers State running Business Education programmes should ensure that learners are exposed to the different types of cybersecurity skills for effective workplace digital records management.
2. Looking at the benefits of cybersecurity skills, and since whatever knowledge one acquires remains with the person, parents of Business Education learners should make personal sacrifices from their earnings and engage their children in informal cybersecurity skills training through online and offline courses to enable their children to acquire very high skills in cybersecurity before gaining admission into the universities. These can also assist the learners in making a little income with the skills since they can work on a part-time basis for some persons within and around the university communities.
3. Management of Universities in Rivers State running Business Education programmes should organise regular training on the various types and very high benefits of cybersecurity skills for lecturers so that they will acquire the skills and transmit the same to learners. Additionally, modern ICT infrastructures for teaching and learning cybersecurity skills should be adequately provided for Business Education departments for effective workplace digital records management.

References

- Alooba. (2026, January 10). *Digital records management*. Alooba. Retrieved May 27, 2026, from <https://www.alooba.com/skills/tools/filing-and-record-keeping-345/digital-records-management/>
- 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. (2026, February). *The benefits of digital records management in the modern workplace*. Modern Business Life. Retrieved May 28, 2026, from <https://modernbusinesslife.com/the-benefits-of-digital-records-management-in-the-modern-workplace/>
- Certkiller. (2026, January 20). *Complete guide to essential cybersecurity competencies for modern professionals*. Retrieved May 31, 2026, from <https://www.certkiller.com/blog/complete-guide-to-essential-cybersecurity-competencies-for-modern-professionals/>
- Cisco. (2026, April 10). *What is cybersecurity?* Retrieved May 27, 2026, from <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html>
- CNCS. (2026, March 1). *Cybersecurity competencies framework*. Retrieved May 12, 2026, from <https://cncs.gov.pt/docs/cybersecurity-competencies-framework-cnccs.pdf>
- Coursera. (2026, February). *Essential skills for cybersecurity analysts in 2026*. Retrieved May 5, 2026, from <https://www.coursera.org/articles/cybersecurity-analyst-skills>
- GeeksforGeeks. (2024). *Computer security – overview*. Retrieved June 10, 2025, from <https://www.geeksforgeeks.org/computer-security-overview/>
- 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.
- National Initiative for Cybersecurity Careers and Studies. (2026, February 15). *NICE workforce framework for cybersecurity*. Retrieved May 20, 2026, from <https://niccs.cisa.gov/tools/nice-framework>
- National Universities Commission. (2022). *Core curriculum and minimum academic standard for the Nigerian university system (CCMAS)*. National Universities Commission.

- Rashid, H. A. (2023, December 6). *Digital records management*. Retrieved May 30, 2026, from <https://limbd.org/digital-records-management/>
- Schulze, J. (2025, August 11). *What is information technology? 2025 guide*. Coursera. Retrieved May 10, 2026, from <https://www.coursera.org/articles/what-is-information-technology>
- Sophos. (2026, May 25). *Cybersecurity defined*. Retrieved May 30, 2026, from <https://www.sophos.com/enus/cybersecurity-explained/what-is-cybersecurity>
- Ukata, P. F. (2019). *Business education students' learning experiences and programme satisfaction*. Lap Lambert Academic Publishing.
- 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*, 5(2), 24–37.
- 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.
- 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 employment in selected Rivers State tertiary institutions. *IRASS Journal of Multidisciplinary Studies*, 2(3), 1–8.
- 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., & 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., & 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*, 5(2), 1–11.
- 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., & 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., 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.