

Impact of Information Security on Digital Economy in Uganda: A Case Study of Selected Public and Private Institutions in Kampala Central Business District

Henry Mulindwa^{1*}; Dr. Mubanga Mpundu²

¹Author; ²Co-Author

¹Institute of Distance Learning University of Zambia Lusaka, Zambia

²University of the Western Cape, Department of Economics, P/Bag X17, Robert Sobukwe Drive, Bellville, 7535, Cape Town, South Africa.

¹ORCID: <https://orcid.org/0009-0007-8670-8040>

²ORCID: <https://orcid.org/0000-0002-4009-9151>

Corresponding Author: Henry Mulindwa^{1*}

Publication Date: 2026/09/28

Abstract: This study investigated the impact of information security on the digital economy within the Kampala Central Business District-Uganda. A mixed-methods approach was adopted, surveys, interviews were used. A sample of 384 respondents were engaged. Data analyzed using the Statistical Package for Social Sciences and thematic methods respectively. Findings revealed that there was an impact of information security practices on performance and competitiveness [$r = 4738.143$, $p < .001$, $\eta^2 = .995$], information security vulnerabilities and breaches had a significant effect on digital economy [$r = 3266.254$, $p < .001$, $\eta^2 = .995$], there no significant effect for challenges and opportunities encountered [$r = 0.500$, $p = .966$] and a positive correlation existed about fostering a secure and thriving digital economy in Uganda ($r = 0.127$, $p = 0.030$). It was concluded that the performance and competitiveness of institutions in Uganda's public and private sectors of the digital economy have been greatly influenced by information security standards, information security vulnerabilities and breaches affect public and commercial organizations. The study recommends that Kampala Central Business District should investment in cyber security infrastructure, technology, and human resources.

Keywords: Digital Economy, Cybercrime, Information Security, and Cyber Attacks.

How to Cite: Henry Mulindwa; Dr. Mubanga Mpundu (2026) Impact of Information Security on Digital Economy in Uganda: A Case Study of Selected Public and Private Institutions in Kampala Central Business District. *International Journal of Innovative Science and Research Technology*, 11(9), 1602-1613. <https://doi.org/10.38124/ijisrt/26sep591>

I. INTRODUCTION

In Uganda, as in many other developing countries, the digital economy holds immense promise, with its potential to revolutionize industries, create jobs, and improve overall living standards (Mutula, 2008). Information security encompasses the strategies and measures implemented to protect digital assets, systems, and data from unauthorized access, breaches, and cyber threats (Whitman & Mattord, 2019). The rapid digitization of economic activities and the ever-increasing reliance on digital platforms by both public and private institutions in Uganda have amplified the importance of robust information security measures (Katebire, 2015). As these organizations digitize their

operations, they create a vast amount of sensitive and valuable data, including financial records, customer information, intellectual property, and government records, which are crucial for their functioning and competitiveness (Chakraborty, 2017). In Uganda, the Kampala Central Business District (CBD) serves as the epicenter of various public and private institutions that are instrumental in the country's digital economy (Ng & Yi, 2016). Public institutions include government agencies, while private institutions comprise a wide array of businesses, ranging from financial services to e-commerce and technology startups. The confluence of these entities within the CBD makes it a prime location for studying the impact of information security on the digital economy, as well as assessing the vulnerabilities

and practices of these organizations in protecting their digital assets.

➤ *Purpose of the Study*

The purpose of this study was to investigate and comprehensively understand the impact of information security on the digital economy within the Kampala Central Business District of Uganda, focusing on selected public and private institutions. By examining the interplay between information security practices, vulnerabilities, and the economic performance of these institutions, the research aimed at providing valuable insights that can contribute to the sustainable growth and competitiveness of Uganda's digital economy.

➤ *Problem Investigated*

The rapid growth of Uganda's digital economy, particularly in the Kampala Central Business District (CBD), presents both opportunities and challenges. While the digital economy can drive economic growth, efficiency, and innovation, it is increasingly vulnerable to information security threats. The critical issue is that as the digital landscape evolves, there is a growing need for effective information security measures, yet it's unclear to what extent public and private institutions in the Kampala CBD are addressing this need. Public and private institutions in the Kampala CBD handle vast amounts of sensitive data, but they face numerous information security vulnerabilities, including data breaches, cyber-attacks, and insider threats (Hugbo, 2019). Understanding the nature and scope of these vulnerabilities is essential for mitigating risks and protecting digital assets. The digital economy plays a crucial role in Uganda's economic growth, but the impact of information security on its performance, competitiveness, and contribution to the national Gross Domestic Product (GDP) hasn't been thoroughly studied in the local context. This knowledge gap hinders the development of tailored solutions and best practices for mitigating information security risks. This research project is vital because Uganda's digital economy has the potential to significantly boost national economic development. Understanding the role of information security is crucial for harnessing the full potential of the digital economy and ensuring its long-term sustainability (Blimpo & Cosgrove-Davies, 2019). By identifying information security vulnerabilities and challenges, this study provides valuable insights to mitigate risks, prevent financial losses, and enhance information security practices in public and private sectors. It also enriches academic understanding, informs policymakers, and encourages a thriving digital economy in Uganda.

➤ *Theoretical Framework*

This study was founded upon the theoretical framework of the digital economy, which provides a comprehensive perspective on various aspects of economic activities in the digital age. Some of the notable research studies have significantly contributed to this framework, exploring how digital technologies have the potential to reshape industries, drive innovation, and enhance productivity, ultimately leading to economic growth (Brynjolfsson & McAfee, 2014; Tapscott & Tapscott, 2016). In parallel, the theoretical

foundation of information security is pivotal. The CIA triad (confidentiality, integrity, and availability) and threat modeling (Pfleeger & Pfleeger, 2015) form the basis for understanding how information security practices safeguard digital assets and mitigate risks in a constantly evolving digital landscape.

Information security is a multi-faceted discipline that seeks to comprehend and lessen the dangers associated with safeguarding information systems, data, and digital assets (Banalieva, 2019). Trust, innovation, economic growth, and ecosystem stability are all affected by how secure information is in the digital economy. The theoretical framework known as the CIA Triad is based on the three cornerstones of information security: confidentiality, integrity, and availability. People's personally identifiable information must be kept private if a person values their privacy and wishes to prevent data breaches. Data integrity protects information against manipulation or corruption, ensuring that it is accurate and unaffected. A firm must always have access to all data and systems for it to run efficiently. To ensure the continuous security of the digital environment, Safiullin (2019) claims that the CIA Triad sets forth three principles that should be balanced and utilized as a foundation for information security policies and procedures in all sectors. Information security also emphasizes the need to use many levels of protection. Using many layers of security is essential to defending against a wide variety of threats. This approach recognizes that no security measure is 100% successful and works to build redundant and resilient systems. By putting in place different security measures, businesses may defend themselves against possible risks and lessen the effects of security breaches on the digital economy. These techniques include multitiered access controls, intrusion detection systems, firewalls, encryption, and more.

II. LITERATURE REVIEW

Globally, the importance of information security practices has gained increasing recognition. As Brynjolfsson and McAfee (2014) emphasizes, the digital economy's growth is intrinsically tied to the effective protection of digital assets. This notion is further supported by a global survey by PwC (2019), which highlighted that organizations with robust information security practices tend to experience fewer data breaches and, consequently, exhibit stronger economic performance. Effective information security practices play a pivotal role in safeguarding digital assets and ensuring the confidentiality, integrity, and availability of data. Kooper, Maes, and Lindgreen (2011) says that staff members' and security teams' skills and competencies would enable good performance in the area of ICT security and governance issues. Furthermore, Laswell and Allen (2007) provides that such workers with training will enhance their information security performance. Therefore, it should be underlined that this type of training must be institutionalized in order for all employees to receive it whenever necessary. Piccoli and Pigni (2018) states that it has become a discipline that many ICT managers and teams in companies and enterprises are highly worried about because it affects their competitiveness.

On a regional level, various studies have examined the impact of information security practices in different parts of the world. For example, research conducted by European Network and Information Security Agency (2018) shows that European businesses have reaped economic benefits by investing in advanced security technologies and fostering a culture of cyber security. These findings align with the European Union's strategic focus on cyber security as a driver of digital economic growth. At the core of these studies is the understanding that information security practices significantly influence the economic performance of organizations and their competitiveness in the digital economy. In East African countries, the notion that cyber security and cyber resilience are merely technical issues that can be resolved by closing the technological gap with more developed countries. Instead, Gagliardone and Sambuli (2015) notes that it highlights the political nature of cyber security and the possibility that, in the lack of sufficient checks and balances, the growing securitization of domestic and international politics may necessitate expensive trade-offs with individual and collective freedoms

Kanyesigye and Mwesigwa (2016) identifies the specific information security challenges faced by institutions in Uganda's digital landscape. These challenges include resource constraints, the need for tailored security strategies, and the presence of vulnerabilities that may lead to data breaches and cyber-attacks. The recognition of these challenges within the local context underscores the importance of evaluating information security practices for their impact on the economic performance of institutions.

The reviewed literature underscores the global consensus on the significance of information security practices in the digital economy. While global and regional studies provide general insights, the local context in Uganda introduces specific challenges and opportunities that demand consideration. Recognizing the importance of information security practices, this study aims to contribute to the existing body of knowledge by evaluating their impact on the economic performance of selected institutions in the Kampala Central Business District, taking into account variables such as "Economic performance," "Information security practices," "Information security vulnerabilities," "Information security breaches," "Challenges in information security implementation," and "Opportunities in information security implementation."

In Uganda, Ahimbisibwe and Nabende (2023) says that a national information security policy, and security standards including technical risk assessment, risk management and accreditation, security classification, personnel security, physical security, and incident management are all included in the national information security framework (NISF). Uganda now has more options thanks to the expansion of its ICT infrastructure, Internet usage, and online access. But, as eservices become more widely used, cyber security protection becomes essential to prevent cybercrime and preserve user confidence. By safeguarding vital national sectors and information infrastructure, information security also advances larger objectives related to national security.

The Uganda Cyber Security Strategy 2022 offers policy, technical guidance, and development pathways to fulfil Uganda's Vision 2040, which seeks to make Uganda a competitive upper middleincome nation. Adesuyi (2020) says that Uganda is not an exception to the global threat that is now posed by cybercrime (Cybercriminals have more opportunity to take advantage of weaknesses as the digital ecosystem grows. relatedly, Atuheire, (2017) states that the increase of cybercrime in Uganda is posing serious problems for a number of businesses, which has an effect on both national security and economic progress.

III. RESEARCH OBJECTIVES

- To assess the impact of information security practices on the performance and competitiveness of public and private institutions in the Kampala CBD.
- To analyze the extent to which information security vulnerabilities and breaches affect the digital economy within the selected institutions in Kampala CBD.
- To identify and understand the specific challenges and opportunities encountered by these institutions in implementing information security measures within the local digital economy context.
- To provide recommendations and insights that can guide public and private institutions, as well as policymakers, in enhancing information security and fostering a secure and thriving digital economy in Uganda.

➤ Research Hypotheses

- *Hypothesis 1*
 - ✓ H10: There is no significant impact of information security practices on the performance and competitiveness of public and private institutions in the Kampala CBD.
 - ✓ H1A: Effective information security practices positively impact the performance and competitiveness of public and private institutions in the Kampala CBD.
- *Hypothesis 2*
 - ✓ H20: Information security vulnerabilities and breaches do not significantly impact the digital economy within the selected institutions in Kampala CBD.
 - ✓ H2A: Information security vulnerabilities and breaches have a significant negative impact on the digital economy within the selected institutions in Kampala CBD.
- *Hypothesis 3:*
 - ✓ H30: Public and private institutions in the Kampala CBD do not face specific challenges and opportunities in implementing information security measures within the local digital economy context.
 - ✓ H3A: Public and private institutions in the Kampala CBD face specific challenges and opportunities in implementing information security measures within the local digital economy context.

➤ *Research Methods*

A cross-sectional research design was adopted with mixed methods to study the impact of information security on digital economy in Uganda. Sample of 384 respondents from selected organizations as well as business entity and traders from the Kampala central business district (CBD) was studied using a survey questionnaire and interview-guide.

➤ *Data Collection*

Data collection from several sources helps build a solid research frame by triangulating information. Data from government papers, corporate directories, and trade associations ensures that the research includes many firms that contribute to the digital economy in different ways (Chigbu et al., 2021). Surveys, including well-written questionnaires for selected public and private groups, are crucial to the research method. These surveys assist to assess and understand these organizations' information security processes. Quantitative data from survey responses would help analyse information security practices in the selected firms. The research examined economic performance indicators to assess how information security had influenced the digital economy. Revenue and market share was calculated from financial records and self-reported statistics from participating institutions. Both financial data and business opinions increase the trustworthiness of economic performance statistics using this dual-source strategy. Interviews and surveys quantified information security risks and breaches. Breaches were examined using incident reports and security logs. Surveys and interviews underpin the first approach.

Organizations were surveyed to determine information security vulnerability occurrence and severity. These surveys were carefully designed to acquire quantitative data on the incidence and severity of digital infrastructure vulnerabilities in the firms being researched. In addition, key stakeholders were interviewed in-depth to provide qualitative value to the study. In addition to technology weaknesses, this strategy investigated organizational and contextual elements that might worsen information security. Interviewing influential personnel at the selected institutions was the first stage. This research employed interviews to explain the technical, organizational, and strategic issues institutions face. Interviews with key professionals disclosed their thoughts on improving information security and digital economy growth. In-depth interviews with key staff members provided qualitative data.

➤ *Data Collection Instruments*

A survey-questionnaire was used to collect quantitative data from the respondents. The process of gathering, evaluating, and interpreting data from several people is called a survey. It seeks to ascertain information about a population. This instrument had parts related to demographic information, general information and the four objectives of the study. Each objective was extensively provided with items that were intended to measure the variables/objectives of the study. An interview-guide was also used to collect qualitative data. This instrument was considered key to provide views and opinions of the participants regarding

Impact of Information Security on Digital Economy in Uganda: A Case Study of Selected Public and Private Institutions in Kampala Central Business District. The objectives of the study formed the structure of this instrument to provide the best data and information for the study. These interview-guide sought to understand digital information security challenges and opportunities. Important people like security authorities, IT managers, and others understood their organizations' complicated information security protocols. This research employed interviews to explain the technical, organizational, and strategic issues institutions face. Interviews with key professionals disclosed their thoughts on improving information security and digital economy growth.

Quantitative data and qualitative data were analyzed using the Statistical Package for Social Sciences (SPSS) and thematic methods respectively. Ethical considerations were observed and adhere to by the researcher. Based on the objectives of the study for example;

- **Assessing the Impact of Information Security Practices on Economic Performance.** This study methodically gathered, analysed, and managed data to determine how information security impacts Uganda's digital economy, focusing on the Kampala Central Business District, a few private, governmental and commercial entities. Survey data underwent many steps to ensure accuracy, homogeneity, and usable analysis. Analysing survey findings begins with data cleansing to find and eliminate errors, contradictions, and outliers. This approach improves the dataset so subsequent studies may be based on strong evidence (Carroll et al., 2020). A detailed variable analysis and procedures for unexpected or missing findings was done. Coding puts numerical codes on qualitative replies and category variables following data purification. Coding standardizes data and simplifies statistical analysis. This organized dataset underpinned quantitative analysis. Several statistical methods assessed survey responses. Descriptive statistics summarized the dataset's key characteristics, patterns, and trends. The institutions' stated information security practices are summarized below with averages, standard deviations, and frequency distributions (Chen et al., 2021). Additionally, the researcher used correlation analysis to examine variable relationships. This step tries to find connections between information security protocols and other relevant factors to better understand these variables. Regression models were utilized to study information security policies and economic performance measures.
- **Analyzing the Extent of Information Security Vulnerabilities and Breaches** Data management, processing, and analysis were rigorous in research on information security's implications on Uganda's digital economy, concentrating on the KCBD, a few private government and commercial enterprises. For complete analysis, vulnerability, breach, and incident datasets were treated separately. A summary and descriptive presentation of vulnerability and breach data is present below. This involves organizing the data in a manner that is simple to understand and summarizes the frequency and kind of vulnerabilities in the examined institutions

(Yasasin et al., 2020). Descriptive statistics described important data like vulnerability numbers and types. This study assessed information security in KCB institutions and identify issues and risks. However, incident data was examined more thoroughly. Finding security incident similarities, core causes, and results was the aim. By meticulously reviewing incident reports and security records, the research seeks security frequency trends (Reshmi, 2021). The incident origins study examined organizational elements and technology shortcomings that potentially lead to security breaches.

- Identifying Specific Challenges and Opportunities Researching information security's implications on Uganda's digital economy needed data management, processing, and analysis. Several Kampala Central Business District public and commercial entities were studied. In-depth interviews with key staff members

provided qualitative data that was analyzed. Transcription of the interviews offered written accounts of the issues addressed. Transcription is crucial to analyze spoken language. Themes were used to examine interview transcripts. Thematic analysis identifies, analyses, and reports qualitative data themes. The Researcher heard from prominent respondents at the selected organizations regarding information security opportunities and dangers. To undertake a thematic analysis, researchers carefully studied the transcripts for similarities and recurring themes. In this technique, researchers coded the data, arranged similar ideas into themes, and then interpreted the themes' underlying meanings. This interview sought for extensive responses on information security's challenges and benefits.

➤ Measurement of Variables

Table 1 Measurement of Variables

Variables	Type of Variable	Indicators	Scale of Measurement / Cut-Off Points	Sample Question Numbers
Variable	Continuous	Economic Performance	Numerical scale (e.g., revenue in USD)	NA
Independent Variables				
Information Security Practices	Categorical	Presence of security measures	Binary (0 = Absent, 1 = Present)	Q1, Q3
Information Security Vulnerabilities	Count	Number of identified vulnerabilities	Count (0, 1, 2, 3, ...)	Q2, Q4
Information Security Breaches	Count	Number of confirmed security breaches	Count (0, 1, 2, 3, ...)	Q4, Q6
Challenges in Information Security	Ordinal	Severity of challenges in implementation	Ordinal (Low, Moderate, High)	Q5, Q6, Q8
Opportunities in Information Security	Ordinal	Level of opportunities for enhancement	Ordinal (Low, Moderate, High)	Q7, Q8, Q9,

For this study, quantitative and qualitative questions were used to analyse both types of data. For example;

- Q1: "Does your institution have formal access control measures in place to protect sensitive data?" Q2: "How many security vulnerabilities have been identified within your institution in the past year?"
- Q3: "Do you conduct regular security awareness training for your employees?"
- Q4: "How many confirmed security breaches has your institution experienced in the last year?" Q5: "On a scale of 1 to 3, please rate the severity of challenges faced when implementing information security measures."
- Q6: "On a scale of 1 to 3, please rate the level of opportunities for enhancing information security within your institution."
- Q7: "Please provide the total revenue generated by your institution in the last fiscal year (in USD)." Q8: "What is your institution's current market share in the digital economy, expressed as a percentage?"
- Q9: "How would you rate your institution's operational efficiency in the digital economy on a scale of 1 to 5, with 5 being highly efficient?"

This table summarizes the key elements utilized to examine information security's impact on Uganda's digital economy, focusing on KCBG government and business groups.

- Continuous "Economic Performance," is the major dependent variable. This variable measures the economic success of participating institutions using USD numbers. Due to its continuous variable character, it was deduced from financial records that showed revenue and other economic indicators; specific question numbers are not needed.
- The category "Information Security Practices" independent variable shows whether institutions have taken security measures. With a value of 0, this variable indicates no security measures while 1 indicates they are present. Q1 and Q3 assess institutions' information security measures. The following variables focus on information security vulnerabilities and breaches.
- The count variable "Information Security Vulnerabilities" shows how many security flaws a company had. It includes the vulnerability severity data collecting questions Q2 and Q4 and the count scale (0, 1, 2, 3). Another count variable, "Information Security Breaches", counts confirmed security breaches. Security breach frequency is counted in Questions 5 and 6, like vulnerabilities. The table's last two variables discuss information security's quality.
- Ordinal "Challenges in Information Security" assesses security measures' complexity. Questions Q7 and Q8 use the ordinal scale (Low, Moderate, and High) to gather qualitative data and allow participants to evaluate in depth. As a final ordinal variable, "Opportunities in Information Security" assesses information security method improvement. In question Q9, participants pick an ordinal scale (Low, Moderate, and High) to assess

advancement potential. The table lists the primary variables, their types, indications, scales of measurement or cut-off points, and question numbers to arrange data collection and analysis in the study project.

IV. RESULTS

The impact of information security practices on performance and competitiveness had a significant effects [F (11, 279) = 4738.143, $p < .001$, $\eta^2 = .995$], significant effect for information security vulnerabilities and breaches affect the digital economy [F (16, 273) = 3266.254, $p < .001$, $\eta^2 = .995$], no statistically significant effect, for challenges and opportunities encountered by these institutions in implementing information security measures [F (20, 270) = 0.500, $p = .966$] and positive correlation with objective 4: *provide recommendations and insights that can guide public and private institutions* ($r = 0.127$, $p = 0.030$).

➤ Conclusions

The performance and competitiveness of institutions in Uganda's public and private sectors of the digital economy have been greatly influenced by information security standards, particularly in the busy Kampala Central Business District. The biggest problems in this way are known as information security vulnerabilities and breaches, which affect both public and commercial organizations in practically every area of the digital economy. In the current digital economy, putting such information security measures into practice presents opportunities as well as obstacles for the majority of companies, particularly Uganda's governmental and private institutions.

V. DISCUSSION

To examine the gender distribution it was found that the survey shows a fairly balanced gender distribution among respondents, with 47.1% identifying as female and 52.9% as male. Additionally, to focus on age group distribution it was found that respondents aged 36 to 45 and over 55 make up the biggest age groups, with 22.7% and 24.1% of the total, respectively. The other age groups, which are 21–25, 26–35, and 46–55, each have between 7.6% and 24.1% of respondents. To focus on the highest qualification distribution it was found that there is a range of educational experience among respondents, with 52.6% having a master's degree or higher. Thirtynine-point nine percent (39.9%) of those who answered have at least a bachelor's degree. Only five percent (5%) have a high school education and only two percent (2%) have a doctoral degree. In addition to focusing on Industry/Sector Distribution, it was found that the people who answered came from a wide range of industries or sectors, and no single area dominated the responses. With 15.1% to 19.6% of the total respondents came from the banking/finance, government, and information technology sectors.

To examine the frequency and percentage of the demographic characteristics it was found that a survey summary covering various demographic and professional attributes of a group of individuals. Distribution according to

gender: 52.9% male and 47.1% female. In the age structure, respondents to the survey are mostly classified within the mature age group whereby 22.1% are within the 36-45 range and 24.7% in the 46-55 range, closely followed by those above 55 years at 24.1% of the respondent population. This shows that the group is usually old. The educational level of the respondents was quite high since 52.6% had achieved a Master's degree, and 24.9% had a Bachelor's degree. Others hold a Doctorate (2.4%) or a high school diploma (5.2%). Professionally, the people are scattered in different industries, with remarkable concentrations seen in Education (14.1%) and Banking/Finance (12.2%). Other major sectors include E-commerce, Government, and Health.

Concerning the professional roles, the proportion of the respondent group is at considerable senior (29.9%) and managerial (24.3%) levels, informing about the experienced and responsible professional cadre. There is also huge representation at the executive and mid-level roles, hence covering all tiers of seniority. The survey also brings out the time length of the employment and organizational context, whereby 36.2% have been employed in their current industry for more than 10 years, and 18.2% between 1-3 years. 41.2 percent of the respondents, each carrying about 41.2% of the total work in either large organizations (more than 250 employees) or medium-sized firms (51-250 employees). Among others, over 46.0% of the organizations indicated an annual revenue exceeding \$50 million, pointing to how much the scale of the companies has been substantial in the economic-financial turnover. Overall, the study results paint a picture of an audience that is highly educated and experienced professionally, mostly in senior roles from large and financially sturdy organizations across several industries.

To examine current position distribution, it was found that based on the respondents' current jobs within their companies, there is a clear hierarchy, with 29.9% of them holding senior-level roles. Managerial jobs come in next with 24.4%, then senior jobs, mid-level jobs, and entry-level jobs, made up the remaining 7.2% to 20.3%. To focus on employment duration in current industry distribution it was found that respondents have worked in the Ugandan business for a range of lengths of time. Notably, 36.8% of them have more than 10 years of experience. Other lengths, like 1-3 years and 4-6 years, were chosen by 13.4% to 18.2% of those who responded. To focus on organization size distribution, it was found that the respondents work for a range of sizes of businesses, with about the same number of big, medium, and small businesses. 41.2% of those who answered are from large or medium-sized businesses, while 17.5% are from small businesses.

To examine an organization's annual turnover distribution, it was found that a look at the yearly turnovers of the respondents' companies shows a wide range, with 46% reporting turnovers of more than \$50 million. Other types of turnover, like less than \$1 million, \$1 million to \$10 million, and \$10 million to \$50 million, each have between 3.8% and 33.7% of responses.

Additionally, to focus on hypothesis testing objectives were examined and to examine objective 1 i.e. "Impact of Information Security Practices on Performance and Competitiveness" it was found that the corrected model, encompassing all independent variables, yielded a statistically significant effect $F(28, 262) = 1.174, p = .256$, albeit with a partial eta squared of .111, indicative of a small to moderate practical significance. However, when scrutinizing the individual effects of each independent variable, notable findings emerged. Age group, highest qualification, industry/sector, current position in the organization, employment duration, organization size, and organization's annual turnover did not exhibit statistically significant effects on the dependent variable. These results suggest that while the overall model suggests a significant impact of information security practices on performance and competitiveness, the influence of the specified independent variables appears negligible. Therefore, these variables may not serve as substantial explanatory factors for the observed outcome variable, underscoring the need for further investigation into other potential determinants.

An analysis of variance (ANOVA) was done to see how information security policies affected performance and competitiveness. The results showed that the independent variables had significant effects on this outcome, with $F(11, 279) = 4738.143, p < .001$, and $\eta^2 = .995$. When the model was fixed, it explained 99.5% of the differences in Objective 1. One of the individual variables, @question 14 (perceived improvement in information security measures), did not affect Objective 1 ($p = .849$) and a very small partial eta squared value ($\eta^2 = .000$). On the other hand, questions 15 and 18 (about how information security affects organizational performance and perceived growth in market share), 16 and 17 (about how satisfied customers are), and 18 (about how information security affects decision making) all had big impacts on Objective 1 (all $p < .001$). For example, @16, @17, and @18 all had big effects, with partial eta-squared values of .949, .951, and .932, respectively. These findings suggest that how much people think information security measures have improved might not have a big effect on how secure information is kept. Other things, like how much people think their market share is growing, how happy their customers are, and how information security measures affect how decisions are made and how well an organization does, are much better at predicting how secure information is kept and how competitive an organization is.

To examine objective 2 i.e. "Impact of Information Security Vulnerabilities and Breaches on the Digital Economy" it was found that the independent factors had a significant effect on Objective 2 ($F(16, 273) = 3266.254, p < .001, \eta^2 = .995$), as shown by the analysis of variance (ANOVA). When the model was fixed, it described 99.5% of the differences in information security holes and breaches in the digital economy. Individual factors @19 through @25 made a big difference in predicting Objective 2 (all $ps < .001$). Concerns about the possible effects of information ($\eta^2 = .949$), the frequency of company data breaches or security problems ($\eta^2 = .945$), opinions on categories of compromised information ($\eta^2 = .959$), the expected effects of

organizational security breaches ($\cdot p^2 = .949$), perceived information security vulnerabilities and breaches ($\cdot p^2 = .861$), the frequency of company vulnerability assessments and penetration tests ($\cdot p^2 = .960$), and the evaluation of employees' knowledge and understanding of information security ($\cdot p^2 = .925$) all had a big impact on Objective 2. These results show how important different factors are in predicting Objective 2 and how complete the model is in understanding the observed variation.

To examine objective 3 i.e. "Challenges and Opportunities in Implementing Information Security Measures" it was found that the total variance explained by principal component analysis (PCA), two components were found. The first component explained 28.384% of the variance, and the second component explained 25.160% of the variance. These two factors together explain 53.544% of the total variance, which means that the extracted factors explain a moderate amount of variation.

The component matrix displays the connection between the original factors and the parts that were taken out. In part 1, the variables "What is the biggest problem you face when trying to set up effective information security protocols in your organization?" and "How much do you think that cloud security solutions can help improve information security in your organization to keep up with local digital economy trends?" are linked positively, with loadings of .640 and .703, respectively. In part 2, the variables "How important do you think it is to work together with other businesses in the local digital economy to solve information security problems?" and "What do you think are the most important changes to improve information security in the local digital economy setting?" are linked positively, with loadings of .720 and -.699, respectively. The outcomes show that the variables inside each part have some kind of underlying pattern or similarity. The first part seems to be about the problems and chances that come with information security protocols and cloud security solutions. The second part is about how important it is to work together with other groups and find the best chances to improve information security in the local digital economy. Regression analysis was also used to look at the link between demographic variables and how hard people thought it would be to implement security measures.

The corrected model, incorporating all independent variables, failed to demonstrate a statistically significant effect ($F(20, 270) = 0.500$, $p = .966$), with a minimal partial eta squared of .036, indicating negligible practical significance. Delving into the individual effects of each independent variable revealed similar outcomes. Gender, age group, highest qualification, employment duration, and industry/sector did not exhibit statistically significant effects on the dependent variable. Consequently, the collective findings suggest that the selected independent variables do not serve as significant predictors of the outcome variable, "Challenges and Opportunities in Implementing Information Security Measures." This underscores the need for further exploration of alternative factors that may influence the implementation of information security measures within the specified context.

To examine objective 4 i.e. "Collaboration and Policy Recommendations for Information Security Improvement" it was found that correlation Analysis was used to assess the relationship between perceived importance of collaboration, recommended actions, and policy suggestions. The purpose of these correlations is to look at how different survey questions relate to the fourth goal. Each correlation coefficient shows how strong and in what way two variables are linked. There is a small positive correlation between Question 30 and Objective 4 ($r = 0.127$, $p = 0.030$), which means that respondents who think it's important for public and private organizations to work together and share information to reduce cyber risks and promote the best practices are also likely to agree with Objective 4. Question 31: "What do you think public and private organizations should do first to improve information security?" has a moderately positive correlation with Objective 4 ($r = 0.613$, $p < 0.001$), which means that respondents who say certain things are most important for improving information security are more likely to agree with Objective 4. Question 32, which asks what the main way is for the Ugandan government and businesses to work together to protect the digital ecosystem, has a moderately good relationship with Objective 4 ($r = 0.493$, $p < 0.001$).

This means that respondents who list detailed ways to work together are more likely to agree with Objective 4. Question 33, which asks how Ugandan politicians can get businesses to invest money on information security, has a strong positive correlation with Objective 4 ($r = 0.588$, $p < 0.001$).

This means that respondents who have ideas for policymakers are more likely to agree with Objective 4. Finally, question 34, which asks how important it is for the Ugandan government to work with other countries to protect itself from cyber threats, has a small positive relationship with Objective 4 ($r = 0.118$, $p = 0.044$), which means that respondents who think it's important to work with other countries are more likely to agree with Objective 4.

Lastly to examine the qualitative analysis it was found that responses to questions about information security and working together in Uganda's digital environment can be grouped into several main themes. First, most of the respondents who answered agree that it's important for public and private organizations to work together to reduce security risks and spread best practices. Most respondents agreed with this, with 63.2% strongly agreeing and 36.8% saying that this kind of collaboration is necessary. Also, respondents who answered stressed the most important things for making information security better, mainly the need for regular cyber security training for employees (29.2%) and strong access rules (22.3%). Public and private organizations can work together to protect the digital world in many ways, such as by creating platforms for sharing cyber threat information (23.4%) and working together on cyber security exercises (15.5%). Respondents also stressed how important it is to give companies reasons to invest in information security. For example, 37.5% supported cyber security training that builds

skills and 17.9% supported minimum cyber security criteria laws.

Respondents from all organisations strongly support working together to deal with cyber security threats, with 59.8% strongly agreeing and 40.2% saying that it is necessary for the Ugandan government. Finally, all respondents (97.6%) agree on what else should be done or laws that should be put in place to improve information security and the digital economy. Creating and enforcing cyber security laws and rules is one idea. Another is making cyber security training programs required for all workers in government agencies and private businesses. The study shows how important it is for people to work together, learn, and follow the rules to solve information security problems and make Uganda's digital economy more stable.

This chapter discusses the findings of the survey on information security practices, gaps, and opportunities in the digital economy of Uganda. The survey tends to establish how information security influences performance and competitiveness, and further, in a case where the information security is breached, what could happen and how this affects the digital economy. What problems and chances come from the setup of security measures and how organizations can work together to set up the policies to make better security? This will make the participating nature of the sample from the survey diverse concerning the background from which emanates the demographic traits of gender, age, qualification, business, and position, length of work, organization size, and annual turnover of the participants. ANCOVA, regression, factor, and correlation analysis are some of the statistical methods used while looking at the survey data to see how different variables affect the goals of the survey. The study finds that information security practices significantly affect performance and competitiveness. This impact was based on issues such as customer satisfaction, organizational performance, decisions made, and market share growth.

On the other hand, it has been found that information security breaches and holes have a great impact on the digital economy. This has the effect of linking the frequency of security incidents with the type of information being stolen, and the severity of breaches, and with the perceptions of how they impact the operation of the digital economy. The research also talked about challenges and opportunities in implementing information security controls, such as the perceptions of control difficulty, risk awareness among employees, cloud options for security, and reviews on vulnerabilities. The study also shows how important it is for public and private organizations, as well as organizations from other countries, to work together to reduce online risks and spread best practices. The study also suggests ways to make information security and the digital economy better, such as making and following cyber security laws and regulations, making cyber security training programs mandatory, and giving companies reasons to invest on information security.

It was found that Popkova (2022) asserted that in today's globally interconnected society, safeguarding

personal information is crucial. It is the foundation of the digital world that guarantees everything is reliable, trustworthy, and everlasting. Security of data, intellectual property, and vital infrastructure has grown in importance in today's internationally integrated economy as a result of the growing reliance on digital technology by individuals, organizations, and governments. This is indispensable for all of the reasons information security becomes when one is building a trustworthy digital economy, as Corallo (2020) has listed. Protection of sensitive information is quite important in ensuring stakeholders' maintenance of trust. For businesses, this translates to having stringent security measures against any form of breach or unauthorized access to the huge amount of consumer data stored, among which lies financial and personal details. Companies that treasure customers' trust and their reputation take measures to protect personal customers' information for privacy security, and accessibility. This was an argument of Litvinenko (2020) that, according to him, the problem is in dependence on data and free money flows on the Internet. "In such a way, to avoid fraud, financial, identity, and cybercrime, those who use digital transactions and communications should be extra careful.". To be valid for the security of digital interactions and the confidence of consumers or organizations in using the internet, it is important to meet a solid cyber security framework, hard authentication mechanisms, and hard encryption protocols (Vasiliev et al., 2020). The assurance of information security, as Xu (2019) has said, is an important aspect when it comes to the protection of confidential or proprietary data. The intellectual property of the company is important to safeguard to save face value and high financial stakes from falling prey to corporate espionage and other forms of unlawful access. In other words, robust cyber security procedures are simply a "sine qua non" condition to protect these invaluable assets and compete in the global digital marketplace.

The research on information security is treasured by both private and public organizations within the capital city of Uganda, Kampala. Shimali (2021) stated that information security is very essential since it protects individuals' privacy, networks, and information systems from unauthorized access, thus realizing reliability via the control measures. The direct emergent result is the acute scarcity of personnel versed in information security requirements due to the pervasiveness of technology and the increasing velocity of digital transformation. To keep sensitive information safe and government processes functioning smoothly, research into information security in public organizations is crucial. Critical infrastructure systems, financial records, personal information of citizens, and information about national security are all handled by these entities. A robust information security architecture has to be established, as pointed out by Abenawe (2022) because government networks are susceptible to cyber assaults, data breaches, and other harmful actions. Academic studies in the area of information security aid public sector organizations in preparing their employees to comply with cyber security standards, minimize risks, and meet all applicable requirements. Private companies in Kampala should also prioritize information security research. Companies from a

wide range of sectors make up these groups. According to Torky's (2020) research, businesses handle and keep a great number of confidential information, including customer records, financial documents, proprietary data, and IP. Customer trust, the company's image, and its competitive edge are all at risk if this sensitive data is not protected from cyber dangers, illegal access, and data breaches. Investing in information security education allows businesses to enhance their cyber security analysis abilities, create incident response methods, and implement strong safeguards.

Lubua (2019), stated that studying information security also encourages being proactive due to the ever-changing cyber threat and vulnerability landscape. Professionals in the field of cyber security can lessen the chances of successful breaches by keeping themselves educated and implementing strategies to avoid, identify, and counteract complex cyber-attacks. Institutions in Kampala should make information security education a top priority to combat cybercrime, which is becoming more difficult with the rise of phishing scams, malware, and ransom ware assaults. It not only needs sufficient knowledge about concepts relating to information security but also all relevant needful international regulation compliances. One such strict regulation to protect data is the General Data Protection Regulation (GDPR), which mandates among other things that the processing of personal data is to be subject to a high level of security. Guidelines followed with these sensibilities in mind can prevent one from getting into legal trouble and at the same time show respect for others' privacy. Adrian (2021) observed that the company could protect itself from superfluous expenses by organizing the implementation of the updated procedures and training, at the same time keeping an eye on hot-legal water-causing importance of information security. As a result of the city's emphasis on education in information security, visibility within Kampala has risen. Working together on the matter of education and training on cyber security, people can contribute to collecting threat intelligence, providing practical answers, and making online life more secure. Together, we can bring the bar of cyber security up for this whole city and set a barrier against cyber-attacks. Building that road from there; on means towards a more secure digital economy. In that prism, many of the adapted challenges and solutions go a long way and tend to take unique forms in varying countries of the world insofar as data security is concerned (Ali, 2020). Heeding that prism could indeed offer insights into how social forces, technological development, and legal environments have altogether shaped the varied perspectives of Ugandans and Africans. Numerous information security issues persist across Africa, even though several of the continent's states are taking steps to protect their online spaces. Data privacy in Africa is seriously threatened by the combination of weak cyber security measures and the rapid adoption of new technologies (Biswas, 2021). Despite the positive effects of digitization on the continent's economy and creativity, the frequency of cyber-attacks has grown. Many African governments face similar problems worsened by a lack of investment in trained individuals, inadequate cyber security infrastructure, and low levels of expertise. According to Tao (2022), cybercrime and data breaches can affect both public and private organizations

in numerous African countries. Ransomware, malware, and phishing attacks can cause financial losses, data breaches, and reputational harm to both public and private sector enterprises.

Because it influences their competitiveness, it has grown to be a discipline that many ICT managers and teams in organizations and corporations are very concerned about as stated by Piccoli, and Pigni (2018). However, to achieve the established aims and objectives of information security governance within the company, information security demands that organization have strong information security staff, such as an Information security manager and team members. Further, it is noted that with, as provided by Kooper, Maes and Lindgreen (2011) that high levels of performance in the area of ICT security, the aspect of governance concerns would be made possible by the abilities and competences of a security team or staff members. In addition, Laswell and Allen (2007) stated that training such employees would improve their performance in the area of information security. It should be emphasized, therefore, that this kind of training needs to be institutionalized so that every employee is exposed to it whenever training is required. The tasks assigned to the members of the information security team may impact the type of training provided by the management of the business or organization with excellent relationship-building and highquality service in terms of information security. The administrative procedures must also take into account how tasks and responsibilities are carried out in accordance with the current security plan and rules. In order to provide prompt support to the organization's information and technology department, this can assist such staff in managing the day-to-day issues of information security.

The implementation of security projects within the company or organization also depends on the security management skills held by such team members. Security analysis, project management, analytical, data analysis, computer forensic, computer-hacking knowledge, audit, decisionmaking, interpersonal, communication, and problem-solving skills would be looked for in such staff members. It would be beneficial to have competent staff in relation to information security that would enhance support building to the entire company team, adhere to internal and external IT requirements and standards. When it comes to the enforcement of policies, the detection of violation refers to the endeavour made by the management of the organization to establish a system for identifying violations, which will help identify those who are not adhering to the security-related elements of the policy (Purse, 2004). For that reason, a monitoring system can be put up to determine who, what, when, how, and why a specific security rule is not followed exactly as stated.

VI. CONCLUSIONS

➤ *Impact of Information Security Practices on Performance and Competitiveness*

Information security practices have been at the central fore of shaping institutions' performance and competitiveness

across the public and private fraternities of Uganda's digital economy, with special mention to the bustling hub of Kampala Central Business District (CBD). The present research endeavor in particular illustrates the extensive integration of information security measures into the operational effectiveness, financial sustainability, and general competitive edge of instances of organizations operating within this complex ecosystem. The heart of information security protection is the implementation of reliable security practices to preserve sensitive data and the multiple valuable assets, which are subject to the attacks of present-day cybercrime. This arrangement was able to reduce the level of risks that are entailed upon data breach, access without authorization, or attacks by malicious persons through strong cyber security policies that will ensure the security of clients' operations. Amidst the ever-changing digital economy of Kampala CBD, follow-up with adherence to the information security standards becomes indispensable to keep intact, the trust and confidence of the various stakeholders, including customers, partners, and investors.

➤ *Impact of Information Security Vulnerabilities and Breaches on the Digital Economy*

The most severe challenges within this manner are referred to as information security vulnerabilities and breaches, which have far-reaching effects on public and private institutions throughout almost every segment of the digital economy. More so from the perspective of Uganda, the above challenges become much more pronounced when these are located in the highly busy central business district of Kampala and from here portend danger towards the economic development and stability of the country. The aspect of trust emerges among the greatest impacts information security vulnerabilities and breaches in the digital economy have on the stakeholders involved, who hold consumers and other businesses in high esteem. This undermines confidence in digital transactions and online services because the sensitive data that people possess, such as financial records or trade secrets, get compromised (Riggs et al., 2023). This lack of confidence can hamper consumer engagement, resulting in a more tepid adoption rate of digital technologies, and, finally, restrain even more the development of, for example, e-commerce and other digital activities in business. Information security incidents result in most financial losses for public and private institutions. There are costs associated with the mitigation of such effects; investigation, security measures, and restoration of the systems and data.

➤ *Challenges and Opportunities in Implementing Information Security Measures*

The implementation of such measures in information security within the present digital economy era comes with challenges but also provides opportunities for most organizations, more so for public and private institutions in Uganda, to position their operations at competitive points in Kampala Central Business District. On top of the list of challenges touching on information security implementation, is the types of threats continue changing. That way, organizations would have to keep adapting their security strategies so that they remain in a good position to deal with

and cater to new and emerging risks that grow as cybercriminals also become more sophisticated with technology. These include emerging threats, investment in state-of-the-art security solutions, and promoting a security-aware culture among employees (Ahonen et al., 2005). On the other hand, other challenges include the fact that there are not enough resources, especially from larger businesses that face this kind of challenge and those public institutions with very little budgets for the same and expertise mostly recorded from many organizations.

➤ *Collaboration and Policy Recommendations for Information Security Improvement*

Stakeholder partnerships and effective, vibrant policy frameworks are very pertinent for the enhancement of the information security atmosphere in Uganda's digital space, most specifically in the Kampala Central Business District. Secondly, public-private partnerships are key in facing the myriad of challenges that cyber threats present. The partnerships entail sharing information, resources, and expertise to strengthen the detection, prevention, and response to attacks on computer systems and networks. Thirdly, there can be cooperation between academia and industry in the perspective of sharing information and resources, therefore making plans and strategies that can improve the coverage of information security for all areas. Above all, such collaboration between academia and industry may be a yardstick for moving ahead with cyber security research, education, and workforce development.

➤ *Managerial Implications/Recommendation*

By establishing guidelines for biometric records, IT trainings, management level emphasis, and the dissemination of cyber security information to all stakeholders, top management may significantly lower cyber security risk. So, in relation to management and administration, it is the responsibility of the management of both public and private organizations operating in the Kampala Central Business District to set aside sufficient funds for the installation of information security measures, such as intrusion detection systems, firewalls, encryption technologies, and a program for training employees on security awareness. By doing this, companies will be able to protect its digital assets from online attacks and lessen the potential harm that these threats could do to the digital economy and sustain its application. The best way to improve information security in Uganda is for stakeholders to pool their resources and exchange information. As a result, if people need to exchange resources, threat intelligence, and best practices for reducing cyber dangers, they should support these kinds of partnerships.

➤ *Theoretical Implication*

Based on the digital economy theory and its theoretical contributions to organizations, the profitability drive of the conventional industrial economy by bringing the market structure closer to a fully competitive market. This theory also puts it to the managers of the organization to have the best resource allocation decision to meet goals and objectives. In relation to the digital economy, it is provided that internet platforms need to be better utilized before making a

resources allocation decision. Indeed, organizations need innovation and entrepreneurial mindset that will allow staff and managers to fit in the new era of management where everything is digitally applied in organizations. Therefore, with the theory at hand, digital transformation is now a cornerstone for the sustainable innovations, development and growth for not only people (Employees, employers, suppliers and others) but also the organizations. Further, socio-economic challenges to business need to be addressed by the managers so that resilience and sustainability of business can be achieved over the time.

➤ Limitations and Suggestion for Further Research

The collaboration of academia with industry and government agencies will have the country's research in cyber security, education, and workforce development moving forward to provide them with the appropriate expertise for controlling the threats rising in the cyberspace environment. Its purview may be too narrowed by looking at only specific institutions within Kampala Central Business District, because if the case studies are given in these specific institutions, the findings in such a study may be less descriptive of a general digital economy existing in Uganda. These are some of the factors that this study, therefore, may not capture very thoroughly. For example regional variations in the practice of cyber security, infrastructure, and development of the economy (Xu, 2019). The study would, therefore, be compromised, since it has placed reliance on case studies from selected public and private institutions. The selected institutions represent selected institutions, and hence may not bring into focus the true features of the different organizations and associations in Uganda's digital economy. Add to this the availability and willingness of these institutions to participate in this study, which may influence the representation of the collected data.

Factors on which these depend and play critical roles are political stability, regulatory environment, technological infrastructure, and socio-cultural norms that shape but are not fully articulated by this research, information security practices. There remain a large number of untapped areas and opportunities for future research in the area of information security and its impact on the digital economy in Uganda. For example, one possible direction for further research may focus on assessing the effectiveness of the different strategies and technologies available in minimizing the prevailing cyber threats that exist in Uganda's digital economy. A comparative study between the various elements of security, such as firewalls, intrusion detection systems, and encryption technologies, should be best conducted to understand which type of these measures are the most effective and worthwhile to protect digital assets in Uganda and reduce cyber threats.

REFERENCES

[1]. Chakraborty, S. (2017). Information security management in the digital economy. *Information Systems Management*, 34(4), 345-346.
 [2]. Abenawe, C. (2022). Social Economic Status in Selected Secondary Schools in Ibanda District Uganda. *IAA Journal of Education*, 8(1), 73-89.

[3]. Adrian, T., & Mancini-Griffoli, T. (2021). The rise of digital money. *Annual Review of Financial Economics*, 13, 57-77.
 [4]. Torky, M., & Hassanein, A. E. (2020). Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Computers and Electronics in Agriculture*, 178, 105476.
 [5]. Shimali, F., Najjingo Mangheni, M., & Kabahenda, M. (2021). Nutrition education competencies of agricultural extension workers in Uganda. *The Journal of Agricultural Education and Extension*, 27(4), 535-552.
 [6]. Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, 5(1), 1-14.
 [7]. Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of Industry 4.0: A structured classification of critical assets and business impacts. *Computers in industry*, 114, 103165.
 [8]. Kooper, M., Maes, R., & Lindgreen, E.R. (2011). On the Governance of Information: Introducing A New Concept of Governance To Support The Management of Information. *International Journal of Information Management*, 31(3), 195-200.
 [9]. Laswell, B., & Allen, J. (2007). Building staff competence in security. *CERT's Podcast Series*. Podcast retrieved from http://www.cert.org/podcasts/podcast_episode.cfm?episodeid=82beff65-df86-176f-81247e5ff833a2ee&pageid=34765
 [10]. Litvinenko, V. S. (2020). The digital economy is a factor in the technological development of the mineral sector. *Natural Resources Research*, 29(3), 1521-1541.
 [11]. Lubua, E. W., & Pretorius, P. D. (2019, July). Cyber-security policy framework and procedural compliance in public organizations. In *Proceedings of the International Conference on Industrial Engineering and Operations Management* (pp. 1-13).
 [12]. Piccoli, GE; & Pigni, F. (2018). *Information Systems for Managers: With Cases* (Edition 4.0 ed.). Prospect Press. p. 28.
 [13]. Popkova, E. G., & Gulzat, K. (2020). Contradiction of the digital economy: public well-being vs. cyber threats. In *Digital Economy: Complexity and Variety vs. Rationality* 9 (pp. 112-124).
 [14]. Springer International Publishing.
 [15]. Tao, R., Su, C. W., Naqvi, B., & Rizvi, S. K. A. (2022). Can Fintech development pave the way for a transition towards a low-carbon economy: A global perspective? *Technological Forecasting and Social Change*, 174, 121278.
 [16]. Vasiliev, V. L., Gapsalamov, A. R., Akhmetshin, E. M., Bochkareva, T. N., Yumashev, A. V., & Anisimova, T. I. (2020). Digitalization peculiarities of organizations: A case study. *Entrepreneurship and Sustainability Issues*, 7(4), 3173.