INFORMATION SECURITY MANAGEMENT: A REQUISITE FOR SUSTAINABILITY OF MANUFACTURING FIRMS IN RIVERS STATE, NIGERIA

ALLISON IGBIKIS ANDERSON[1] **and** OBARA CHIZI ERUCHI (PhD)[1]

allisonanderson214@gmail.com;chizi.obara@ust.edu.ng,
[1]Department of Office and Information Management Faculty of Management Sciences
Rivers State University, Port-Harcourt, Nigeria

ABSTRACT

The study investigated the relationship between information security management and sustainability of manufacturing firms in Rivers State. The study dimensions were authentication and encryption algorithm; while growth and customer loyalty measured the dependent variable. The research provided answers to two questions and tested four hypotheses in order to establish the hypotheses formulation that there is no significant relationship between information security management and sustainability. The study population comprised of the twenty-six Manufacturing firms in Rivers State. The research selected three managerial staff members from each of the firms under study making it total seventy-eight study elements. Data were generated from the respondents by the use of a well-structured questionnaire. Pearson's product moment correlation was used to test hypotheses with the aid of statistical packages for social science (SPSS) version 23.0. The p-values were calculated to determine the significance of the hypothesized relationship. Analytical outcomes revealed statistically positive and significant relationships between the dimensions of our predictor variable-information security management and the measures of the criterion variable-sustainability. Based on the findings, the study concluded that information security management has a positive, significant relationship with sustainability of manufacturing firms in Rivers State. The study further recommended amongst others, that Management of manufacturing firms should seek to build strong encryption algorithms in line with their company policies and practices aimed at achieving Organizational sustainability.

Keywords: Information security Management, Sustainability, Encryption, Authentication, Manufacturing firms

INTRODUCTION

Organizational establishments have invested significant effort in establishing and improving information security systems to ensure that information is properly guarded, retained and easily retrieved (Sarita & Paul, 2020). International Federation of Data Organizations for Social Science (2012) alludes to information security as the act of protecting and maintaining both the security and integrity of information. This is achieved through a set of formal activities governed by policies, regulations and strategies aimed at maintaining and expanding the existence and reliability of information and its meta-information. The goals and objectives of information security are to protect information from loss or destruction and to contribute to its reuse and further development. Information security goes beyond the concept of information ownership and information backup. Information security ensures reliable access to information by incorporating backup and recovery mechanisms before disasters or technological changes occur (Kennedy, 2020). Consecutively within different years, collected historical information has been destroyed by war and natural disasters, and there is a "severe lack of the materials and related practices needed to preserve and protect the information" (Kitchin, 2012). There are some facts. Typically, only the most relevant sets of information were stored, such as government information and statistics. Information in scientific research papers and doctoral dissertations is largely destroyed due to improper storage and lack of awareness of information security and implementation.

Repeatedly, information security has experienced growth and significant change, gaining increased importance and prominence. Currently, there are different types of information storage and different major organizations are involved (Kitchin, 2012). Information can be described as the elements or entities from which knowledge is created. Information provides evidence of an organization's official activities and is important for decision-making, accountability, and reconstruction of an organization's past activities (Sandy, 2016). Fermi National Accelerator Laboratory (2011) emphasizes the importance of information in improving access to information, increasing productivity, increasing the security of critical information, and increasing regulatory compliance and decision support. Information security management is the process of establishing efficient practices to maintain access to usable information, ensure that results are verified, and that information can be reused in the future. Information security involves the collection of relevant information, analyzing, integrating, storing and safeguarding relevant information collected to be discovered for future and reference purposes (Blessing, 2015). Information security is geared towards the identification of relevant strategies and practices that improve efficiency, agility, plan to reduce cost, make incremental changes and easily share overview with stakeholders and investors (Khan & Ejike, 2017). Information security is aimed at countering threats such as Loss of ability to identify the location of information, Lack of sustainable hardware, software, or support of computer environment that may make the information inaccessible, access and use restrictions may not be respected in the future, evidence may be lost because the origin and authenticity of the information may be uncertain by maintaining information and information accessible, independently understandable and usable by a designated community, and with evidence supporting its authenticity, over the long term (Giaretti, 2011).

Most manufacturing companies today are at risk because fraudsters with IT skills are trying to break into the organization's data warehouse to steal and defraud manufacturers and their customers. Therefore, information security needs to be improved to ensure that people's assets are safe. Preserve, protect and protect the way the business can do well. Information security needs to be able to monitor resources or potential areas where unauthorized individuals can plan an attack. In this context, data security has been implemented. Loss of relevant information cannot be prevented, but loss must be prevented (Tantua Jnr. & James, 2019). Singh (2009) believes that important features and key features are needed to protect important information, which he calls the three elements of information security. One of these is data encryption. Encryption means that encryption prevents messages from being sent to unauthorized people or systems. For example, make a credit card payment online. The system encrypts the card number during the sending process, restricts where the card number appears (such as databases, records, backups, and receipts), and does not enter it where the bus number appears. Try to bypass security by breaching the security code. Encryption is necessary (but not sufficient) to protect individuals' privacy when personal information is stored in databases (Xuemei, Yan, & Lixing, 2009).

The topic of sustainability in business development has received a lot of attention. The manufacturing industry in Rivers State, Nigeria, has been facing serious demise in the last decade. This difficulty arises from the inability to manage information security. It can be said that these companies ignore the negative aspects of starting from internal knowledge management. Overtime, these challenges affect the growth and sustainability of the organization and often lead to its failure. Therefore, this study tries to solve this problem by managing information security. Issues related to information security management have been discussed by many researchers. These researchers believe that most organizations will, from time to time, face competitive threats, that is, external threats from hackers and criminals. This can be very disruptive, impacting organizational processes and reducing productivity. Therefore, it becomes important for organizations. In this context, manufacturing companies in Rivers State, Nigeria, need to understand the need to carefully manage various key aspects of the enterprise. This is because it helps you create a solid organization that will stand the test of time. Upon this backdrop, this study sought to investigate the relationship between Information security management and organizational sustainability of manufacturing firms in Rivers State, Nigeria.

REVIEW OF RELATED LITERATURE

Data security management is the process of ensuring that currently stored data is secure and still readable and interpretable even years or centuries after being stored (Nova, 2018). According to Brown et al. (2009), the term “security management” is best used to describe the measures necessary to ensure the security of information created and stored by organizations that use computers. Data security management is good practice for managing data availability, ensuring results can be verified and data can be reused in the future. Data security management is the protection and management of data protection and ethics. Management of information security is carried out through main activities aimed at protecting and expanding information, regulated by current and former laws, regulations and procedures. The main purpose of information security management is to protect information from loss or damage and to monitor the use and development of information (Jackson 2015). According to Sydney (1997), over the years, different authors and researchers have given different definitions of information security management; While many try to limit information management security for data storage, others believe that security management is not just about storage. Instead, it has many activities that ensure the correct management of information and ensure that it is honest. Information security management involves technical and intellectual interventions that ensure that information remains safe and secure for as long as possible. The purpose of information security management is to ensure that information can be reused when needed after its life cycle. Data security management is about keeping our data consistently and reliably accessible over time; although adequate efforts must be made to manage both types of information, protecting digital information requires greater care than protecting non-digital information to ensure timely access. Information security management is a fundamental need for every organization because it provides the necessary support for employees and the entire organization to gain a competitive advantage. In all areas and industries of business, security management is essential for growth. From the information collected, even new employees will be able to learn and explore many aspects of the organization; they will understand the organization and culture. Information security management aims to address threats such as loss of the ability to identify the source of information, lack of stable hardware, software or computer environment support that may make data inaccessible or fail to meet access and use restrictions. Because in the long run, the source and authenticity of information can be uncertain, with the collection of data and information that is accessible, self-understanding and used by selected communities with evidence supporting its accuracy (Giarretti, 2011).

Banach and Li (2011) believe that information security management processes have become a very difficult task as technology is constantly changing and digital information faces many threats. Conway (1996) defined the main problem of the digital age as follows: "While our ability to collect information has increased over time, the lifespan of the media used to store it has also shortened." However, Lavoie and Dampsey (2004) views this as controversial at the same time, they opine that the goal of data security management has changed from the need to quickly "recover" data to ensure data security. Long-term digital data requires the use of digital asset management tools throughout the life of the data. Additionally, Lavoie and Dampsey (2004) suggest that information security management works best when first implemented because items that are damaged or unusable are returned, meaning wasting money is not allowed or restricted. Awareness of the urgency of data security management has led to the development of various methods to solve the problem of long-term data storage. Systems can now be divided into digital backup, storage, encryption and storage (Becker et al., 2009). Becker et al. (2009), however, note that this approach faces problems with many different and mixed products and large data sets. Recently, there has been an emphasis on open source to facilitate long-term access to digital information. Today, as technology changes, business faces a level of complexity that makes it nearly impossible for many organizations to manage their storage facilities without using technology output. Generally speaking, it is very difficult to manage data security without using technology, but this technology exposes company databases to some risks. Managing information security is important for the business to be efficient and effective. Security management is important for every organization (Lanre & Toke, 2000). Therefore, information security management has proven to be an important management tool for successful operations and performance. From a security management perspective, information security knowledge is as old as humanity. It dates back to the early days when humans were able to store information in their brains and send it to people. It came back from the mouth. However, more specific information was written on stales, scrolls, and walls that could be used for future reference if properly preserved. However, the reliability of data collection is limited. This might be why everyone is paying so much for security checks lately.

Authentication

Verification applies to both hard copy and electronic documents. There are special problems in protecting the integrity of electronic data, such as data stored in emails or data contained in files; both are easy to replace. Measures should include: controlling access to data or information, understanding who is responsible for and accessing the data or information, preventing unauthorized changes to the extent possible that are inaccurate or offensive, and reviewing the accuracy of recorded data or information from time to time. Organizations must decide what format or medium the message will be stored in and choose the most secure format or medium. To prevent loss, they need to recover data, especially if it is important or business-critical in some way. Data must be stored properly and securely, electronically and physically. Sensitive information should not be placed on a desk, computer or laptop. Organizations must consider the best way to deal with data at the end of its lifecycle. Two certificate management technologies, shredding and offsite storage, are designed to protect your sensitive data. Usually the criminal only asks for more money when he finds some financial documents in the office; this information includes credit card numbers, tax IDs, banking information and more. Keeping documents in plain sight, whether scattered around or neatly tucked away in a filing cabinet, is a poor form of information security. To solve this problem, consider storing your financial and other sensitive information in a safe and secure place. New information in digital form; Security management is the practice of protecting information in an organization from its creation to its final destruction. Information security management is often associated with evidence of the organization's activities and is often used based on the value of information rather than its physical nature. Data must be protected from unauthorized users. Media in Information management allows electronic management and control of Information from receipt or creation through processing, storage and retrieval, to disposal. The advantage of such a system is that it allows all Information security management tasks to be performed with limited personnel (Olivero, Pasewark & White, 2015).

Encryption Algorithm

Encryption is the process of using an algorithm (Bassel) to convert information or words, called plaintext, into an unreadable form called ciphertext. It is derived from the Greek word "cryptos" meaning secret. There are two types of encryption: symmetric encryption and asymmetric encryption. Symmetric encryption uses a key to encrypt plaintext into ciphertext and convert ciphertext into plaintext. Asymmetric encryption involves having two keys (one public, one private) one used to encrypt plaintext and the other used to decrypt ciphertext. The use of encryption dates back to times when people felt the need to hide messages that were unsuitable for certain parties. Legacy encryption methods fall into two main categories: transfer ciphers and exchange ciphers. The transposed cipher will reorder the order of the alphabet so that the first character of the alphabet becomes the last character. Substitution ciphers involve replacing one letter or group of letters in the alphabet with another letter or group of letters in the alphabet (Pandya et al., 2015). Medieval literature on cryptography emerged after it was discovered multiple times in the 9th century by an Arab mathematician and scholar named Al-Kindi, which made it easier to decipher written records using ancient forms of cryptography. Although the method is said to have been developed earlier, the Alberti cipher was one of the first to use the polyalphabet cipher, using a disk cipher consisting of two matching disks, both written in letters and Mathematics. It was created in 1467 by cryptographer Leon Battista Alberti. He has been called the "father of Western cryptography" by cryptography historian David Khan (Khan, 1973). The first published book on cryptography was written by Johannes Trithemius, who introduced the basic principles of cryptography in the form of several alphabets modified into tabular form called Strath. This formed the basis of the Vigenere Cipher (also known as the Automatic Key Cipher), which, according to David Khan, is mistaken for Blaise de Vigenere rather than Giovan Battista Bellaso. The Vigenère cipher was said to be unbreakable by its author, but was cracked by Charles Babbage between 1853 and 1856; developed techniques to crack many table passwords. This period witnessed the rise of knowledge, which is now the world's most valuable commodity. This means that companies, organizations, groups and individuals will spend a lot of money to ensure that information on a particular subject is protected. In ancient times and the middle Ages, communication was mainly used for communication between two parties, requiring a third party to be unable to understand the words of either party. Today, encryption goes beyond communication to protect data from hackers and cybercriminals. With the rise and advancement of technology in different sectors, businesses using these digital technologies are aware of the threats posed by cyber criminals to their businesses, so they need to protect their information and this security can only be achieved through encryption. Traditional encryption is a classic technology used before the development of public key encryption. Cryptography is divided into three different areas: the type of operation used to convert plaintext into ciphertext (via substitution and modification), the number of keys used, and the method of executing the text (block or stream). Manipulation of key points includes permutation, Caesar ciphers, game fair, Hill ciphers, etc. However, with the introduction of today's encryption methods (such as block ciphers based on the Feistel encryption model), encryption support provides more comparison opportunities in every aspect.

Sustainability

Organizations are increasingly challenged to incorporate social expectations into their business strategies to adapt to the needs of customers, employees and others (Bielak, Bonini, & Oppenheim, 2007; Bonini, Mendonça, & Oppenheim, 2006). To understand sustainability, it is necessary to define the concept and take into account the values and concepts behind the concept. There is no consistent definition of sustainability. It means different things to different people. Generally, sustainable organizations are believed to be businesslike, responsible, and environmentally friendly (Beal et al., 2017; KPMG, 2011; Daood & Menghwar, 2017; Bocken et al., 2014; Clarke & Roome, 1999). A company can be viewed from two different perspectives: the business perspective (the organization) and the non-organizational perspective that affects the company. From an organizational perspective, marketing is important in the company/business. The inside of the company is visible to the owners/businesses and the organization (management) (Harianto & Sari, 2021). Goodwill and good management are necessary to sustain business growth. Events outside the company are not related to the company's operations but may affect business continuity. For example, the customer is an external part of the company. However, the level of customer loyalty using the products produced by the company affects the company's income (Muhamad & Rilvani, 2021). Sustainability is a term used for sustainable development; this means development that meets the needs of the present without compromising the ability of future generations to meet their needs (Brundtland Report, 1987). This approach includes three dimensions of sustainability: environmental, social and economic, and directly addresses the environmental damage that often accompanies economic growth, rather than encouraging growth to reduce poverty. To avoid this conflict, organizations must be responsible for creating natural resources so that they can be used in a way that can be beneficial forever, rather than permanently destroying or destroying them (Garcia, 2022). De Carvalho, Chim-Miki, Da Silva, and De Araujo (2019) say that sustainable business is defined as integrating sustainability goals into its activities. Wong and Ngai (2021) pointed out that the company's ability to achieve sustainable development is based on three elements: cooperation and social management. Environmental potential refers to the application of the 5 Rs (repair, rehabilitate, reuse, recycle, reduce) and job potential through business competition and new construction. Security management must meet the needs of stakeholders at all business, environmental and organizational levels. Stakeholder theory is a simple method that demonstrates the connection between people and business and reveals the value of interacting stakeholders. Companies can achieve joint venture visibility by building strong relationships with internal and external stakeholders and collaborating to achieve business goals (Garcia, 2022).

Growth

The key to these companies' survival in the global business environment is their ability to grow their business. Business growth is an indicator of business success. A company's growth can mean the company's overall performance as well as other factors such as size, productivity, performance, debt, inflation, exchange rates, economic growth, and interest rates (Musah, Kong, Atwi, Donkor, Quansah & Obeng, 2019). Gupta et al. (2013) defines business growth as generating income, creating value and expanding business volume. Business growth is often defined and measured in terms of changes in sales, assets, operations, productivity, profits and margins. Business development is the process in which business success is increased to a certain extent through growth and profit maximization. This can be interpreted in terms of revenue generation, value creation and business expansion (Owolabi & Ogan, 2022). Gupta, et al. (2013) identified economic history, characteristics of entrepreneurs, various policies (i.e., market and government), and geography as some of the factors that influence business growth. Aregbeen (2012) identified the company's past growth, size, retirement expenses, financial constraints, operational efficiency, and degree of integration as important factors of company development. Zhuo and Wit (2009) divided the determinants of economic growth into three factors: individual determinants, organizational determinants and environmental determinants. They believe that these three measures generally lead to economic growth. Self-determination of business growth refers to business decisions made by an individual entrepreneur. These include personal characteristics (need for achievement, willingness to take risks, locus of control, self-efficacy and adaptability), increased motivation, self-efficacy and personal history (Zhuo & Wit, 2009). The decision-making bodies of companies are the ones most affected by economic growth. These effectively include firm characteristics (firm age and size), firm strategy, specific resources (financial and human capital), design and capacity (Zhuo & Wit, 2009). Environmental determinants are factors external to the company. These include dynamism (business or technology), heterogeneity (complexity of the environment), hostility (more competition may threaten the company), and tolerance (environmental support such as economic capacity) (Zhuo & Wit, 2009). Researchers define economic growth as a situation in which a company's sales increase but its operating costs in terms of profit decrease. The trust company is entrusted to the agent, the trustees manage the assets of the company and the human capital layer of the company's assets, production, marketing, etc. must distribute and manage its assets. All work is done by the beneficiaries. This means that the trustee does not work for his own benefit, but for the benefit of the stakeholders, who are the true owners or investors of the departmental company. This means working for money. Therefore, in order to ensure trust and confidence, trust must exist between the beneficiary and the trusted (Moud-Yusuf, 2012).

Customer Loyalty

To understand the importance of customer loyalty, consider the following facts: Problematic customers often do not respond, with only 4% of customers complaining; often one person finds it difficult to teach nine others; one interested person mentioned it to five people - their experiences. The cost of retaining existing customers is approximately 1/7 of the cost of acquiring new customers; the cost of retaining existing employees is 1/10 of the cost of hiring and training new employees. This explains the saying "the customer is always right". These facts; highlight the important role of meeting customer needs in driving employee engagement; thus maximizing profits for the company/organization. Therefore, organizations need to understand the customer at a high level. Customer loyalty has a special meaning in the business world. Anders, Johnson and Inger (2005) define customer loyalty as the overall evaluation of a product to date. This trust is effective in retaining customers for different services and products. In the service sector, service quality directly affects customer loyalty. Ingrid (2004) defines loyalty as a feeling that arises from the process of evaluating what is purchased according to expectations, the purchasing decision itself and/or need/need satisfaction. Loyalty means getting what we want. If loyalty is defined as infallibility, companies need to reduce complaints, which alone is not enough. To satisfy customers, the company or organization needs to improve its services and products. In a competitive business, understanding your customers' needs is crucial. As a result, companies moved from a product-focused approach to a customer-focused approach. Customer retention is directly affected by customer loyalty. Insurance is a major challenge especially when it comes to ethical issues in organizations because customers can easily switch from one service provider to another for others at low cost based on ethical issues (Khalifa & Liv, 2003). Consumers want their values (wants and needs) to be consistent with the values they evaluate (Paker & Matthew, 2001).

Recently, new interest has focused on the nature of justice, emotions, success, and status. Accordingly, recent literature has added this perspective in two ways: First, while traditional models implicitly assume that customer loyalty is an important part of the cognitive process, new ideas suggest that the emotional process may also play an important role in customer loyalty (Fornell & Wernerfelt, 1987; Westbrook & Olive, 1991). Second, loyalty should be viewed as a decision based on experiences with particular services rather than a specific change (Wilton & Nicosia, 1986). It is generally accepted that loyalty is the happiness or disappointment that arises in relation to an individual's hope for the performance (or profit) of the company's products (Kotler, 2003). This overall loyalty has a positive and strong impact on customer loyalty intentions across a variety of products and services (Gustafsson, 2005). Ethical decisions relate to all the know-how the company has with its specific products, sales processes and after-sales services. Post-purchase satisfaction also depends on how the offer connects to the customer's needs. Customers receive expectations from past purchases, recommendations from friends and colleagues, promises and promises from business and people, and competition (Kotler, 2000). Factors that determine the expectation level are customer demand, total customer value and total customer value.

Theoretical Framework

This study hinges on Open Archival Information System Reference model, as its theoretical foundation for Information security management.

Open Archival Information System Reference Model (OAIS)

Information security management is a field with different structures such as digital libraries, digital archives, digital warehouses and data storage. However, the most widely used model in the development of digital names is the OAIS model (Quist, 2008). Since its introduction, the OAIS standard has had a significant impact and impact on the development of digital preservation systems. The OAIS model was prepared by the Consultative Committee on Space Science Data Systems (CCSDS) and is associated with the National Aeronautics and Space Administration (NASA) (CCSDS, 2002). This standard has been adopted as the ISO standard for long-term storage of digital data (ISO14721:2003). Although the OAIS reference model has its roots in spatial research, it is a general model that describes archive organization. The main idea behind the standard used is OAIS. The word "open" means that the standard has been developed and published in a public forum where participation by interested parties is encouraged. Archival information systems, on the other hand, are "organizations created by people and systems responsible for preserving information and presenting it to a specific community" (Lavoie & Dempsey, 2004). The first section describes the external environment in which the OAIS operates, while the second section describes the operational activities that constitute the OAIS's protection mission. The third section describes the material OAIS receives, manages and publishes (Lavoie & Dempsey, 2004). The implementation of the OAIS environment is most suitable for the current study because banks are representatives of developers in the OAIS environment; they create the information and send it to the OAIS archive. This information is available free of charge online to users (individuals, organizations, systems and the public) who use the information. In addition to the functional components of the OAIS model, there is also a data model built around the data package. This package is primarily designed to store metadata that must support long-term storage and access. These are Information Distribution (SIP), Information Protocol (AIP) and Information Distribution (DIP). SIP is the data packet sent by the Producer to the OAIS and AIP is the data packet stored and maintained by the OAIS. DIP is the version of the data packet sent to the Customer in response to the access request. Despite its influence in the archival community, the model has been criticized for its high cost of time and money and the danger of items being lost during migration (Ball, 2006). Egger (2006) shows how models combine management and operations functions and continue to use different levels of abstraction to describe their operations. Given that many digital preservation projects are based on the OAIS model (Corrado and Moulaison, 2014), the current study found it appropriate to use the OAIS model as it addresses the various roles and work of community partners. Repositories, such as the OAIS model, help increase the sustainability of firms by reliably storing information and providing access to digital information. The main purpose of this reference is to promote a general understanding of the need to store and access information in the long term, based on this work. So far, basic studies on the theory and model needed to create a framework for the management of sustainability in manufacturing firms have been discussed. One of the main objectives is to learn how the manufacturing sector creates and manages information. Currently, it is suggested that the OAIS model is suitable for teaching research because they raise questions and changes that are important and relevant for research.

This study conceptualized the following framework as a guide through the study.

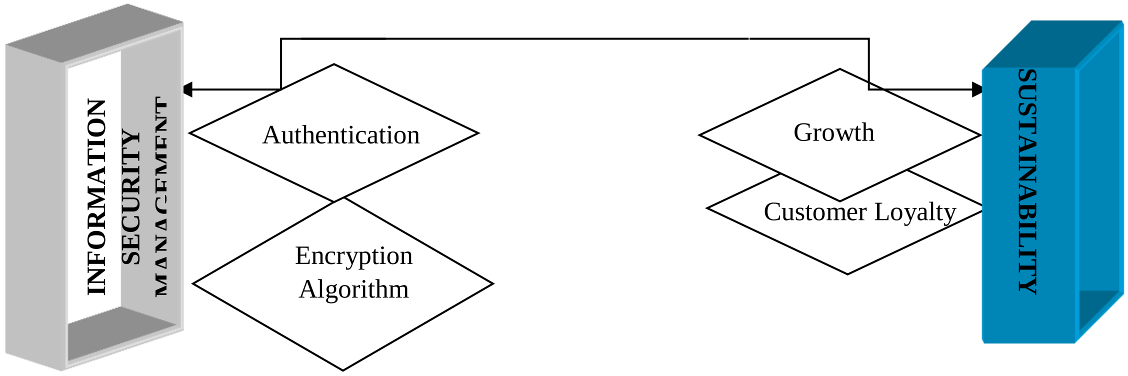

Fig. 1.1: Showing Framework of Information security management and Sustainability of Manufacturing firms in Rivers State, Nigeria.

Source: Researchers' Mindset, 2023

METHODOLOGY

This study is a descriptive study assuch adopted a cross-sectional survey design suitable for this study. The study population comprised of twenty-six manufacturing firms operating in Rivers State. The researcher considered three (3) managers of each of the Manufacturing firms in Rivers State as the target population. The respondents/elements of this study were limited to the top, senior, and junior managers of each of the manufacturing firms in Rivers State. Thus, 78 copies of the structured close ended 4point lykert scale questionnaire were administered on the categories of employees that formed the respondents mainly Top and Senior Managerial Cadres. The reliability test of the structured questionnaires was ascertained through Test-re-test in which a pilot administration of the questionnaire was made on a portion of the chosen sample and administered after two months and relationship between the two results determined by correlation coefficient, through SPSS version 20. Our reliability test was also anchored on the Cronbach Alpha at 0.7. At the primary level of our analysis, this study adopted the use univariate descriptive statistical tool such as mean, standard deviation, frequency tables, simple percentages, bar charts and histograms to present the data that was generated while for bivariate inferential statistics, the Pearson's Product Moment Correlation was employed at the secondary level of analysis, to test the hypothesized statements. All the statistical analyses were performed using the Statistical Package for Social Sciences (SPSS) version 23.0.; because this version has the ability to transform scaled data into discrete or continued data and vice versa.

Decision rule

Reject Ho if PV< 0.05

Accept Ho if PV > 0.05

Table 1 Showing Strength and Direction of Relationship between Variables

Range of values	Degree of relationship
$\pm 0.00 - \pm 0.19$	Very weak
$\pm 0.20 - \pm 0.39$	Weak
$\pm 0.40 - \pm 0.59$	Moderate
$\pm 0.60 - \pm 0.79$	Strong
$\pm 0.80 - \pm 1.00$	Very strong

Test of Hypotheses

H_{01}: There is no significant relationship between Authentication and Growth in manufacturing firms in Rivers State

Table 2 Relationship between Authentication and Growth

		Authentication	Growth
Authentication	Pearson Correlation	1	.729**
	Sig. (2-tailed)		.000
	N	73	73
Growth	Pearson Correlation	.729**	1
	Sig. (2-tailed)	.000	
	N	73	73

**. Correlation is significant at the 0.01 level (2-tailed).

From the SPSS output on Table 2, it can be observed that there is a correlation coefficient of 0.729** between Authentication and Growth, indicating a strong and positive relationship between Authentication and Growth. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a strong significant relationship between Authentication and Growth. This further implies that most of the changes in Growth among manufacturing firms in Rivers State are caused by their Authentication while others are caused by externalities. Based on this, we reject the null hypothesis that there is no significant relationship between Authentication and Growth of manufacturing firms and incline to the alternate hypothesis that there is a strong, significant relationship between Authentication and Growth of manufacturing firms.

H$_{02}$: There is no significant relationship between Authentication and customer loyalty in manufacturing firms in Rivers State

Table 3 Relationship between Authentication and Customer loyalty

		Authentication	Customer loyalty
Authentication	Pearson Correlation	1	.875**
	Sig. (2-tailed)		.000
	N	73	73
Customer loyalty	Pearson Correlation	.875**	1
	Sig. (2-tailed)	.000	
	N	73	73

**. Correlation is significant at the 0.01 level (2-tailed).

From the SPSS output on Table 3, it can be observed that there is a correlation coefficient of 0.875** between Authentication and customer loyalty, indicating a very strong and positive relationship between Authentication and customer loyalty. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a very strong significant relationship between Authentication and customer loyalty. This further implies that most of the customer loyalty experienced among manufacturing firms in Rivers State is caused by their Authentication while others are caused by externalities. Based on this, we reject the null hypothesis that there is no significant relationship between Authentication and customer loyalty of manufacturing firms and incline to the alternate hypothesis that there is a very strong, significant relationship between Authentication and customer loyalty of manufacturing firms.

H$_{03}$: There is no significant influence of encryption algorithm on Growth in manufacturing firms in Rivers State

Table 4 Relationship between Encryption algorithm and Growth

		Encryption algorithm	Growth
Encryption algorithm	Pearson Correlation	1	.794**
	Sig. (2-tailed)		.000
	N	73	73
Growth	Pearson Correlation	.794**	1
	Sig. (2-tailed)	.000	
	N	73	73

**. Correlation is significant at the 0.01 level (2-tailed).

From the SPSS output on Table 4, it can be observed that there is a correlation coefficient of 0.794** between encryption algorithm and Growth, indicating a strong and positive relationship between encryption algorithm and Growth. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a strong significant relationship between encryption algorithm and Growth. This further implies that most of the changes in Growth among manufacturing firms in Rivers State are caused by their encryption algorithm while others are caused by externalities. Based on this, we reject the null hypothesis that there is no significant relationship between encryption algorithm and Growth of manufacturing firms and incline to the alternate hypothesis that there is strong, significant relationship between encryption algorithm and Growth of manufacturing firms.

H_{04}: There is no significant influence of encryption algorithm on customer loyalty in manufacturing firms in Rivers State

Table 5 Relationship between Encryption algorithm and Customer loyalty

		Encryption algorithm	Customer loyalty
Encryption algorithm	Pearson Correlation	1	.776**
	Sig. (2-tailed)		.000
	N	73	73
Customer loyalty	Pearson Correlation	.776**	1
	Sig. (2-tailed)	.000	
	N	73	73

**. Correlation is significant at the 0.01 level (2-tailed).

From the SPSS output on Table 5, it can be observed that there is a correlation coefficient of 0.776** between encryption algorithm and customer loyalty, indicating a strong and positive relationship between encryption algorithm and customer loyalty. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a strong significant relationship between encryption algorithm and customer loyalty. This further implies that most of the customer loyalty experienced among manufacturing firms in Rivers State is caused by their encryption algorithm while others are caused by externalities. Based on this, we reject the null hypothesis that there is no significant relationship between encryption algorithm and customer loyalty of manufacturing firms and incline to the alternate hypothesis that there is a strong, significant relationship between encryption algorithm and customer loyalty of manufacturing firms.

DISCUSSION OF FINDINGS

The analysis of the study revealed a correlation coefficient of 0.729** between Authentication and Growth, indicating a strong and positive relationship between Authentication and Growth. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a strong significant relationship between Authentication and Growth. The analysis results also revealed a correlation coefficient of 0.875** between Authentication and customer loyalty, indicating a very strong and positive relationship between Authentication and customer loyalty. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a very strong significant relationship between Authentication and customer loyalty.

The analysis of the study revealed a correlation coefficient of 0.794** between encryption algorithm and Growth, indicating a strong and positive relationship between encryption algorithm and Growth. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a strong significant relationship between encryption algorithm and Growth. The analysis results also revealed a correlation coefficient of 0.776** between encryption algorithm and customer loyalty, indicating a strong and positive relationship between encryption algorithm and customer loyalty. More so, the probability value (0.000) is less than the critical value (0.05), this shows that there is a strong significant relationship between encryption algorithm and customer loyalty.

CONCLUSION

In consonance with the findings of this study and to the extent of its consistency with results of extant studies, we conclude that information security management has a positive, significant relationship with the sustainability of manufacturing firms in Rivers State.

RECOMMENDATIONS

Based on the findings of the study and to the extent of its consistency with the result of similar studies we make the following recommendations.

1. Management of manufacturing firms should capitalize on the pivot role of Authentication in their operations to ensure their Organizational sustainability.
2. Management of manufacturing firms should seek to build strong encryption algorithms in line with their company policies and practices aimed at achieving Organizational sustainability.

REFERENCES

Aregbeyen, O. (2012). The determinants of firm growth in Nigeria. *Pakistan Journal of Applied Economics, 22*(1 & 2), 19-38

Boiko, B. (2002). *Content management bible*. New York: Hungry Minds.

Chachage, B. Ngulube, P. & Stilwell, C. (2006). Developing a model corporate records management system for sustainability reporting: A case of the Iringa region in Tanzania. *SA Journal of Information Management 8*(1)

Clarke, S., & Roome, N. (1999) Sustainable business: Learning-action networks as organizational assets. *Business Strategy and the Environment, 8*(5), 296-310.

De Carvalho, J. R. M., Chim-Miki, A. F., Da Silva, C. C., & De Araujo Carvalho, E. K. M. (2019). Análise multicriterial da competitividade empresarial sob tríplice perspectiva: *Financeira, Governança Corporativa e Sustentabilidade*. *Revista de Globalización, Competitividad & Gobernabilidad, 13*(2), 116-131.

Garcia, M. L. S. (2022). Business sustainability and financial performance. *Journal of Management* 38(72)

Giaretta, D. L. (2011) *Advanced Digital Preservation*. Springer Verlag.

Gupta, P. D., Guha, S. & Krishnaswami, S. S. (2013). Firm growth and its determinants. *Journal of Innovation and Entrepreneurship, 2*(15), 1-14

Harianto, R. A., & Sari, P. N. (2021). Strategic digitalization of UMKM business as an alternative to survive the COVID-19 pandemic. *Linguistics and Culture Review*, *5*(S1), 617–663.

Indianapolis (1996). *Database Unleashed.* SAMS Publishing

International Federation of Data Organizations for Social Science (2012). *Data preservation.*

Khan, H.U. & Ejike, A.C. (2017). An assessment of the impact of mobile banking on traditional banking in Nigeria, *Int. J. Business Excellence*, 11(4), 446–463

KPMG. (2011). *Business briefing series: 20 issues on building a sustainable business*.

Mohd Yusuf, B. N. (2012). Communications and trust is a key factor to success in virtual teams collaborations. *International Journal of Business and Technopreneurship*, *2*(May), 389–397.

Muhamad, L. F., & Rilvani, E. (2021). Systematic review: Perlindungan Konsumen Transaksi Online. *SMART Management Journal,* 40–46

Musah, M., Kong, Y., Atwi, S. K., Donkor, M., Quansah, P. E. & Obeng, A. F. (2019). A study into growth and firms' financial performance: Evidence from the Ghana Stock Exchange (GSE). *International Journal of Multidisciplinary Research and Development, 6*(5), 45-53

Oliverio, M. E., Pasewark, W. R. & White, B. R. (2015). *The Office, Procedures and Technology,* (South-Western Educational Publishing; New York), 545- 547.

Penn, I. A., Pennix, G. & Coulson, J. (1994). *Records management handbook*, 2nd rev. Ed.

Sarita, S. & Paul, C. (2020). Data and power: Archival appraisal theory as a framework for data preservation. *Proceedings of the ACM on Human-computer interaction 4*(CSCW2), 1-18.

Shepherd, E. & Yeo, G. (2003). *Managing Records*: A Handbook of Principles and Practice. Facet Publishing, London.

Singh, S. (2009). *Database systems*: Concepts, Design and applications New Delhi: Pearson Education India

Tantua Jr. E. & James, P. G. (2019). Information Security and Organizational Efficiency of Deposit Money Banks in Port Harcourt, Rivers State, Nigeria. *International Journal of Business & Entrepreneurship Research, 13*(1), 1-11

Webster, B. Hare, C. & McLeod, J. (1999). Records management practices in small and medium-sized enterprises: a study in North-East England. *Journal of Information Science 25*(4), 283-294

Wong, D. & Ngai, E. (2021). Economic, organizational, and environmental capabilities for business sustainability competence: Findings from case studies in the fashion business. *Journal of Business Research*, *126*, 440-471.

Xuemei, L., Yan, L., & Lixing, D. (2009). Study on information security of industry management. In Information Processing, APCIP, *Asia-Pacific Conference,* 1, 522 –524.