DATA ENCRYPTION AND INFORMATION SECURITY OF PUBLIC SECTOR ORGANIZATIONS IN SOUTH-SOUTH, NIGERIA

OKERE, Albert Eziuche [1], Prof. Ebikaebina Tantua Jnr[1] and Prof. Patrick Nyinyokpugi [1]

Department of Office and Information Management
Faculty of Management Sciences
Rivers State University, Port Harcourt

Email: okerealbert@gmail.com. Tel: +234-8036734933

ABSTRACT

The prevalence of cyber-attacks, data breaches, insider threats, thirty-party risks and advanced persistent threats has forced organizations to adopt new technologies to secure its information assets. This study examined the application of data encryption in relation to information security in the public sector organizations in South-South Nigeria. The cross-sectional survey plan and a quasi-experimental research design were adopted for the study. The study population were 6 public sector organizations in South-South Nigeria. The study elements were 5 Directors from each of the organizations, bringing the total of respondents to 30. Data for the study was generated through structured open-ended questionnaire. The study used simple descriptive and inferential statistics to analyze data generated. The hypothesis of the study was tested using the Pearson Product Moment Correlation Statistics and presented with the aid of Statistical Package for Social Sciences. The study established a significant and positive relationship between data encryption and confidentiality in information security; significant and positive relationship between data encryption and integrity in information security; and a significant and positive relationship between data encryption and availability in information security. It concludes that there is a positive and significant relationship between data encryption and information security and therefore recommended that organizations adopt the data encryption mechanism that protects its information from unauthorized access, mutilation and alteration.

Keywords: Data Encryption, Information Security, Confidentiality, Integrity, Availability

INTRODUCTION

The prevalence of cyber-attacks, data breaches, insider threats, thirty-party risks and advanced persistent threats has forced organizations to new technologies to secure its information assets. Encryption ensures the protection of information and communications in different spheres – personal, commercial, and in the public sector. It secures data against unwanted access, helps ensure the confidentiality of data and delivers trust in the digital economy. It is essential for all key actors: governments, individuals, and businesses. For citizens, encryption provides privacy and anonymity, while businesses use encryption to secure trade secrets, communicate securely, and build trust. Governments use encryption to protect critical information, secrets, and systems. (David & David, 2015). Encryption has also become a ubiquitous part of the digital economy and is the necessary protection that underpins the digital marketplace. Across sectors, encryption has emerged as the tool that has allowed for the financial transformation of the modern Nigerian economy. It has enabled innovation, growth, research and development, and ultimately redefined digital trust.

At the same time, there is growing risk to public information safety as organized crime, terrorists, and child pornographers are drawn to the use of encrypted platforms that are technically impossible to access by law enforcement or by the companies that provide the devices and applications (Okerenke, 2015). Since the beginning of the new century, with the

rapid development of modern computer information technology, computers have gradually entered thousands of households, becoming a necessity for modern people to engage in communicative work such as cooperation and business negotiation, entertainment, education and learning, and daily life, although computer network wireless communication has various advantages, such as instant, convenient, fast, no working time, and network space restrictions (Zheng & Cai, 2020). But there are often pros and cons in all things. While achieving good convenience for people's lives and work, security technical problems such as network security vulnerabilities, virus software intrusions, hacker vulnerability intrusions, and network server security information system leaks also frequently break out (Treacy & Mccaffery, 2017). The security of the wireless communication system of the multicomputer network has been greatly reduced, which has caused serious threats to the legitimate rights and interests of network users and the security of citizens' personal information.

Data plaintext encryption, in brief, is to convert those plain digital plaintext information into digital ciphertext that ordinary people cannot easily understand by using certain encryption technology. In turn, it cannot be decrypted without the decryption key. In this concept, the technical staff ensures that the basic meaning and functional difference between the plaintext of the password and the ciphertext are correctly distinguished (Al-Darwish & Choe, 2019). The opposite is the ciphertext, which is something that ordinary people cannot easily understand, and it has been used by transformation processing. When technicians are preparing for network data security encryption, they may also need to figure out the data sender and data receiver separately (Treacy & Mccaffery, 2017).

Information has experienced exponential growth and consideration in recent years. It has become a major financial staple for organizations as it is a driving force for companies to increase revenues or significantly reduce expenses. Santos et al. (2011) describe organizational information or corporate data as the "new currency of business". In spite of the current worldwide economic state, security spending is one area that does not appear to be losing momentum (David & David, 2015). This has given organizations every reason to protect their information, and yet security threats and breaches will and do occur. Most security defenses are geared towards the prevention and/or mitigation of security breaches and often have to be policy driven (Treacy & Mccaffery, 2017). The typical countermeasures for hardening security include layering defense systems, diversifying defense methods, ongoing management of hardware and software updates or patches, access controls with auditing, and authentication mechanisms (Okerenke, 2015). The issue with traditional information security counter measures is that organizations often adopt a "passive" approach. This passive approach is operationally defined as putting security measures and countermeasures in place, and hope they work. If a breach occurs, these measures are not updated to stop future breaches (Al-Darwish & Choe, 2019).

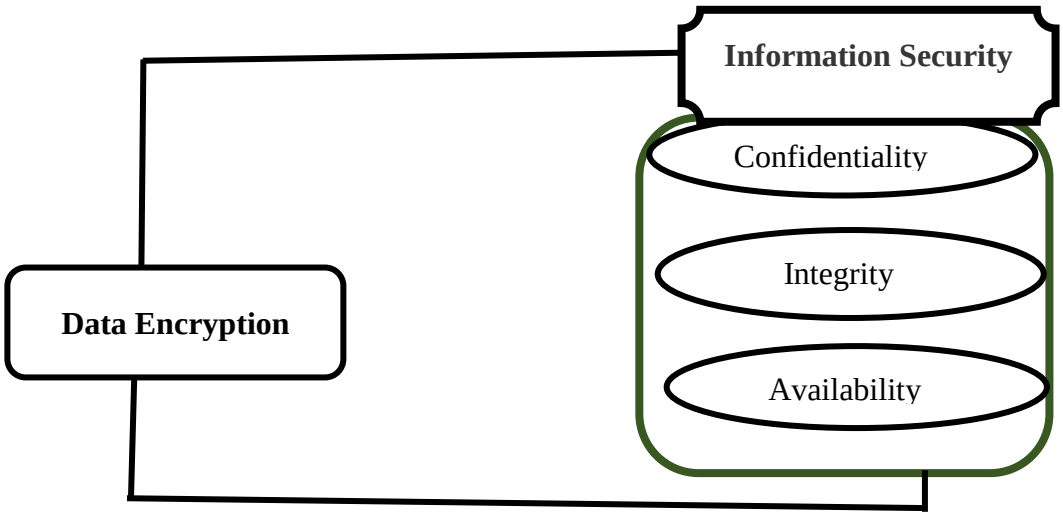

Figure 1: Conceptual Framework of the relationship between Data Encryption and Information Security

LITERATURE REVIEW

Theoretical Framework -PMT (Protection Motivation Theory)

The protection motivation theory explains how individuals change their attitudes and actions when facing danger. This theory was developed by Rogers (1975). The theory, mainly developed in the field of psychology, tries to find the factors that affect the intentions of activity based upon "fear appeal." According to the theory, when an individual is exposed to a message of danger, protection motivations that stimulate the actions are made. This theory assumes that there are three factors in fear appeal: **the severity**, which measures the extent of the threat; **the exposure**, which measures the possibility of being exposed to the threats; and **the response efficacy**, which measures how to treat the threats efficiently. Later, Rogers (1983) added self-efficacy to the list.

Johnston and Warkentin (2010) studied the relationship between security activity and the fear appeal and derived the research model based upon the protection motivation theory. They also added "the social effects" and "the intentions of action" which were used in technology adoption. Furthermore, they assumed that severity and danger sensitivity affected efficacy and efficacy directly affected intentions of behavior. The Theory of Protection Motivation predicts how the use of encryption could be applied with the intentions to protect information and maintain its confidentiality, integrity and availability.

In this paper, information security is seen as a process where people and organizations attempt to create sustainably viable resources, from information. In this study the application of suitable controls to protect information from threats, according to the goals of the organization, which results in sustainable resources, is recommended. Also, controls should be applied to ensure that the confidentiality, integrity, and availability of information is maintained.

Concept of Data Encryption: Encryption involves the transformation of 'plaintext' or readable information into unintelligible data. This process of transforming data into encrypted information

uses cryptography, a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use (Zheng & Cai, 2020). At the most fundamental level, algorithms are used to encrypt information and generate keys. The key is used to scramble the data into unreadable text. Depending on the type of encryption, the same key can be used to decrypt the data, or a separate set of keys will be used. For a given algorithm, the strength of the encryption increases with the length of the key, which is measured in bits. Chang (2016) submits that encryption technology is the protection of our critical security technology transfer and exchange of information across the network. With the continuous progress of science and technology, encryption technology will gradually lead to accurate and complete technology, which is helpful for the establishment of computer network security systems and perfection.

Symmetric encryption is an ancient and well-known method. In this method, the mystery key is used which may be a number, a phrase, or a string of arbitrary letters. It is mixed with the obvious textual data or a message to enclose the content material in a specific manner. The sender and recipient must know the name of the key which is used to encrypt and decrypt all of the messages. A process can be applied to encrypt data in transit, i.e., when it is sent from one place to another through a network; or at rest, i.e., where it is stored, such as on a server, end-device, or hard-drive.

An algorithm can be applied to encrypt data in transit, i.e., when it is sent from one place to another through a network; or at rest, i.e., where it is stored, such as on a server, end-device, or hard-drive. Encryption can either be symmetric or asymmetric, or a combination of both. In symmetric encryption, the same key is used for encrypting and decrypting. In addition to its security benefits, it also does not take a lot of time to encrypt and decrypt data. On the other hand, in asymmetric encryption, the key used for encrypting is different from the key used for decrypting. This is also called 'public key cryptography', because one of the keys used for encryption is public. For example, a user can list one of their keys in a public directory, which would allow anyone to send them a message. However, the message can only be decrypted by the user through their private key, which remains secret (Chang, 2016). On another level, encryption can be either server side or user-side. In the former, the server of the service provider manages the encryption and the decryption of the data, by managing the keys. For example, e-mail encryption is typically server side, as users expect to be able to access stored e-mails, recover account passwords if they forget them, access their e-mail from any device, and send e-mails to their friends using different e-mail platforms. Notably, because the service provider has access to the encryption keys, they can share them with law enforcement or other third parties pursuant to a legal request (Zheng & Cai, 2020).

On the other hand, user-side encryption refers to cryptography applied by the user, or at the device of the user. This can include both user-deployed encryption such as VPNs, and technologies such as end-to-end encryption that are deployed by the service provider at the application level. The service provider does not hold access to the keys and will be unable to share them with law enforcement agencies, regardless of a legal request or court order. Also known as unrecoverable encryption, it is used to secure both data in transit and data at rest. Over time, encryption has become stronger, more widespread, and easier to use (Chang, 2016). Major

technology companies are increasingly enabling user-side or unrecoverable encryption, such as end-to-end encryption, encryption of smartphone operation systems, as well as default encryption of mobile devices (Zheng & Cai, 2020). This has complicated law enforcement investigations, leading to calls to access encrypted information. Intelligence communities have found it increasingly difficult to carry out investigations in an age where the internet is going dark. Law Enforcement Agencies find that encrypted system poses a unique legal challenge when it comes to issuing warrants and granting access (Zheng & Cai, 2020). Intelligence Agencies have consistently asked for a backdoor to encrypted systems in order to solve and prevent a battery of crimes, including child pornography, curbing hate speech and the illegal sales of armaments, to name a few.

A slew of incidents caused by the dissemination of misinformation over the Internet propelled the government to impose a traceability obligation onto messaging platforms (Okerenke, 2015). The traceability requirement is similar to regulatory developments in different countries that obligate companies to develop capabilities to provide law enforcement with on-demand access to information – even when deploying user-side encryption. On the other hand, weakening encryption through such mandates may hurt the privacy of users, weaken security, damage the economic viability of technology companies, and also result in significant economic harm for the nations (David & David, 2015). In this context, the key consideration for policymakers in Nigeria and across the world is to balance these competing facets of encryption, i.e., privacy, cybersecurity, and national security.

Information Security

The security of information especially in the software is very important on all of the fields (Wang, Yao & Yu, 2018). The core concepts of information is CIA (confidentiality, integrity and availability) presented in articles by (Kumar & Bhatia, 2020), were adopted in the information security requirements and are commonly used in various fields of study. For example, information security in digital information may be appropriately exposed if its confidentiality is violated, improperly changed if its integrity is jeopardized, and weakened or destroyed if its availability is threatened (Khidzir et al., 2018). A best Information Security Management System, provides the ISO 27000x Series as a guide to practice (Aminzade, 2018).

Dhillon (2007) has defined information and communication technology security as the protection of information resources allocated in information technology systems. It has been discovered that technology and communication can be viewed as a risk factor that can be manipulated by threats in order to protect information (Alkhudhayr et al., 2019). An article written by Al-Darwish & Choe (2019) indicates that both organizations and personal factors affect compliant actions in Information Security. The overall findings are encouraging self-efficacy, ensuring a favourable understanding of the Information Security environment, and ensuring that all levels of the company, for example supervisors, co-workers and upper management, apply security guidelines to their daily actions to improve compliance.

There are many information security issues concerned in all the fields of endeavour. A security issue shows in the article by Alhosani et al. (2019). In order to decrease the security incidents in the bank sector, the experts agreed to provide employees with security policies awareness to understand the policy requirements. In addition, experts also provide strategies to help banks

improve the security such as social engineering evaluation, privileged access (logical access or physical access), security quiz, and phishing campaign. Due to continuous learning and education culture, employees who have the latest safety trends and environment would have minimal accidents. In order to support the advanced technology unit, training enables staff to resist information security risks. Threats and risks will be faced in an organization in any field.

Confidentiality

Confidentiality is defined as the restrictions on the use and storage of various types of data (Khidzir et al., 2018). The principle of information confidentiality involves restricting data access strictly to authorized personnel. Users have a responsibility to ensure they maintain secure access control systems, including both logical (e.g. PC passwords) and physical restrictions (e.g. ID cards). For this reason, it is important that all employees receive thorough training in information security awareness and best practices. It is important to limit data sharing and state availability restrictions, so confidentiality is not inadvertently breached (Thangaraju & Rani, 2016). The importance of physical restrictions should not be underestimated. Remember, unwarranted access to your building can facilitate unauthorized access to valuable assets, including information asset. Door codes help to ensure your building remains secure. They should not be written down and staff should be vigilant in ensuring no one is watching or recording them input codes. Similarly, many organizations insist that their employees wear ID badges, this makes it easier to identify non-employees within your workplace. ID badges should be worn at all times within the workplace but never outside of work. Wearing them outside of work enables criminals to quote your details (e.g. name, position and organization) in an attempt to gain access to your building. Areas containing particularly sensitive information can be protected by extra access restrictions e.g. an additional door code.

Passwords are another basic, yet vital, means of protecting your information. A strong password is at least 8 characters long, contains upper and lower case letters, numbers and special symbols. Passwords should never be shared (even with your colleagues or IT providers) and should be changed immediately if discovered. Changing your password regularly allows hackers less time to guess it and stops them from using your account if they have already obtained your password. You should change your password at least once every 90 days.

Confidentiality measures protection of information from unauthorized access and misuse. Most information systems house information that has some degree of sensitivity. It might be proprietary business information that competitors could use to their advantage, or personal information regarding an organization's employees, customers or clients (Aminzade 2018). Confidential information often has value and systems are therefore under frequent attack as criminals hunt for vulnerabilities to exploit. Threat vectors include direct attacks such as stealing passwords and capturing network traffic, and more layered attacks such as social engineering and phishing. Not all confidentiality breaches are intentional. A few types of common accidental breaches include emailing sensitive information to the wrong recipient, publishing private data to public web servers, and leaving confidential information displayed on an unattended computer monitor (Chang, 2016).

There are many countermeasures that organizations put in place to ensure confidentiality. Passwords, access control lists and authentication procedures use software to control access to resources. These access control methods are complemented by the use of encryption to protect information that can be accessed despite the controls, such as emails that are in transit. Additional confidentiality countermeasures include administrative solutions such as policies and training, as well as physical controls that prevent people from accessing facilities and equipment (Kumar & Bhatia, 2020). In information security, confidentiality is the "property" that information is not made available or disclosed to unauthorized individuals, entities, or processes. While similar to "privacy" the two words are not interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers (Thangaraju & Rani, 2016). Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals (Aminzade, 2018).

To maintain confidentiality in automotive systems, data needs to be protected inside and outside the vehicle, while it is stored (data at rest), while it is transmitted (data in motion), and while it is being processed (data in use). Memory protection can be applied to data in use. Cryptography is excellent for protecting the confidentiality of data at rest and data in motion, but keep in mind that it imposes computational complexity and increases latency, so it should be used with caution in time-sensitive systems (Tchernykh et al., 2019).

Integrity

Integrity is the guarantee that data has not been tampered with Khidzir et al. (2018). It presents a broadcast encryption method using dynamic ciphertext, which provides security guarantee for text decryption and attacks. Data replication is one of the data de-duplication processes that is used to reduce storage space and bandwidth use. The other way is creating the privacy preserving keyword search. It allows to solve the decryption and only return files that contain the specified keywords. Integrity measures protect information from unauthorized alteration. These measures provide assurance in the accuracy and completeness of data. The need to protect information includes both data that is stored on systems and data that is transmitted between systems such as email. In maintaining integrity, it is not only necessary to control access at the system level, but to further ensure that system users are only able to alter information that they are legitimately authorized to alter (Khidzir et al., 2018)

The protection of data integrity extends beyond intentional breaches. Effective integrity countermeasures must also protect against unintentional alteration, such as user errors or data loss that is a result of a system malfunction. While all system owners require confidence in the integrity of their data, the finance industry has a particularly pointed need to ensure that transactions across its systems are secure from tampering. There are many countermeasures that can be put in place to protect integrity. Access control and rigorous authentication can help prevent authorized users from making unauthorized changes. Hash verifications and digital signatures can help ensure that transactions are authentic and that files have not been modified or corrupted. Equally important to protecting data integrity are administrative controls such as separation of duties and training. Upholding integrity means that measures are taken to ensure that data is kept accurate and up to date. The integrity of your data impacts how trustworthy and conscientious your organization is. Users must make sure that they comply with their legal duties

and fulfil this requirement. It can be useful to assign individuals specific roles and responsibilities regarding data integrity. This way employees cannot shelve the responsibility and expect someone else to pick up the slack.

Integrity is the ability to ensure that a system and its data has not suffered unauthorized modification (Shoufan & Damiani, 2017). Integrity protection protects not only data, but also operating systems, applications and hardware from being altered by unauthorized individuals. In automotive systems, CRC (cyclic redundancy check) is known to provide integrity protection against accidental or non-malicious errors; however, it is not suitable for protecting against intentional alteration of data. Hence, the sensitive data should include cryptographic checksums for verification of integrity. Moreover, mechanisms should be in place to detect when integrity has been violated and to restore any affected system or data back to their correct state.

Availability

In order for an information system to be useful it must be available to authorized users (Treacy & Mccaffery, 2017). Availability measures protect timely and uninterrupted access to the system. Some of the most fundamental threats to availability are non-malicious in nature and include hardware failures, unscheduled software downtime and network bandwidth issues. Malicious attacks include various forms of sabotage intended to cause harm to an organization by denying users access to the information system. The availability and responsiveness of a website is a high priority for many businesses (Aminzade, 2018). Disruption of website availability for even a short time can lead to loss of revenue, customer dissatisfaction and reputation damage. The Denial of Service (DoS) attack is a method frequently used by hackers to disrupt web service. In a DoS attack, hackers flood a server with superfluous requests, overwhelming the server and degrading service for legitimate users. Over the years, service providers have developed sophisticated countermeasures for detecting and protecting against DoS attacks, but hackers also continue to gain in sophistication and such attacks remain an ongoing concern.

Availability countermeasures to protect system availability are as far ranging as the threats to availability. Systems that have a high requirement for continuous uptime should have significant hardware redundancy with backup servers and data storage immediately available. For large, enterprise systems it is common to have redundant systems in separate physical locations. Software tools should be in place to monitor system performance and network traffic. Countermeasures to protect against DoS attacks include firewalls and routers. Availability means guaranteeing reliable access to information by authorized personnel (Wang, et al 2018). In order to be readily accessible, data must be stored in a logical yet secure system. High availability aids rapid business processing and ultimately benefits an organization. It is every user's responsibility to file desktop documents in a way that makes them easy to locate in the future. Similarly, paper copies should be filed securely and not left lying around. Copies should be made to ensure important information is not irreversibly lost. Certain storage methods are more vulnerable to loss and theft than others. Information on portable storage devices, such a USBs, is particularly vulnerable. That is why the information should be encrypted and backed up. Temporary displays (e.g. whiteboards and charts) are similarly vulnerable to prying eyes, and information recorded in this way should be transferred to a more permanent, confidential place at the earliest opportunity (Kumar & Bhatia, 2020). It is business owners' responsibility to implement a thorough business contingency plan, allowing rapid disaster recovery. This ensures

minimal disruption to service. Getting information systems up and running as soon as possible ensures that there is not an excessive interruption to information availability.

Data is often shared, not only within an organization, but also to individuals outside of the organization, such as customers, business partners and the public. Emails are a quick and easy way of sharing data around the world, especially convenient when transferring big data sets. However, information sent over the internet can sometimes be intercepted and accessed by hackers, compromising confidentiality. Encrypting information can make it harder for hackers to access, as without the decryption key the data will appear to be nonsense (Tsaregorodtsev, 2018). Availability guarantees that systems, applications and data are available to users when they need them. The most common attack that impacts availability is denial-of-service in which the attacker interrupts access to information, system, devices or other network resources. A denial-of-service in an internal vehicular network could result in an ECU (electronic control unit) not being able to access the information needed to operate and the ECU could become non-operational or even worst, it could bring the system to an unsafe state. To avoid availability problems, it is necessary to include redundancy paths and failover strategies in the design stage, as well as to include intrusion prevention systems that can monitor network traffic pattern, determine if there is an anomaly and block network traffic when needed (Treacy & Mccaffery, 2017).

Data Encryption and Information Security

The security of data resources is vital for any organization. Good data management involves secure storage of data and its secure transmission. Security deals with a triplet of confidentiality, integrity, and availability. Data encryption is the procedure of transforming information from a readable format to a scrambled element of information. This is completed to avoid prying eyes from reading confidential information in transit. Encryption can be used on documents, files, messages, or some different forms of communication over a network (Tchernykh et al., 2019). David and David (2015) submit that encryption is a security approach where data is encoded and can only be accessed or decrypted by a user with the proper encryption key. Encrypted data is also called a ciphertext. It can appear scrambled or illegible to a person or entity accessing information without permission.

Data Encryption is used to check malicious or negligent parties from accessing sensitive information. As an important line of defense in a cybersecurity structure, encryption makes using intercepted information as complex as possible. It can be used to all types of data security needs ranging from classified government information to personal credit card transactions. In encryption, based on the type of encryption, information can be shown as several numbers, letters, or symbols. Data encryption software is called encryption algorithm or cipher. It is used to make an encryption scheme which theoretically can only be divided with high amounts of calculating power (Chang, 2016). Encryption is an important method for individuals and organizations to secure sensitive data from hacking. For instance, websites that transmit credit card and bank account numbers should continually encrypt this data to avoid identity theft and fraud. The numerical study and application of encryption is called a cryptography.

Data encryption technology secures both transmitted information and stored digital information on computer systems and the cloud. As the web has changed computing and systems have gone online, modern encryption algorithms have restored the outdated Data Encryption Standard

(DES) to secure IT communications and systems (Chang, 2016). These algorithms guard confidentiality and fuel basic security initiatives such as integrity, authentication, and non-repudiation. The algorithms first authenticate any message to check its origin, and thus check its integrity to test that its contents remained unaltered during transmission. Finally, the non-repudiation initiative avoids senders from weak legitimate activity (Chang, 2016).

METHODOLOGY

This study aimed to establish a relationship between data encryption and information security in the public sector organizations in South-South Nigeria. The cross-sectional survey plan and a quasi-experimental research design were adopted for the study. The study methodology adhered to the positivist philosophy, which involves identifying essential relationships relating to the phenomenon (in this instance, the adoption of data encryption). Structured close-ended 4-point Likert Scale questionnaire were administered on 5 Directors in each of the 6 public sector organizations studied in South-South Nigeria. The study used simple descriptive and inferential statistics to analyze data generated. The hypothesis of the study was tested using the Pearson Product Moment Correlation Statistics and presented with the aid of Statistical Package for Social Sciences (version 25.0).

DATA ANALYSIS

This section of this study presents the analysis of data collected in line with the purpose of the study. The results obtained are presented in tables, and descriptive statistics such as mean and standard deviation were used to present the responses.

Table 1: Descriptive Statistics for Data encryption

	Question Items on Data encryption	Mean	STD
1	Encryption prevents unauthorized access, eavesdropping, or data breaches, thereby safeguarding information confidentiality	3.672	0.510
2	Implementing encryption measures can enhance an organization's information integrity	3.133	0.642
3	By encrypting digital signatures or certificates, it becomes difficult for malicious actors to forge or tamper with them, thereby enhancing data availability	3.200	0.997
4	Encryption processes in the organization is dependent on functional information and communication technology	3.110	0.929
	Valid N listwise	28	

Source: Survey Data, 2023, and SPSS Window Output, Version 25.0

Table 1, showed a mean and standard deviation scores of 3.672±0.510 which indicated that respondents are in agreement that data encryption prevents unauthorized access, eavesdropping, or data breaches, thereby safeguarding information confidentiality. With mean and standard deviation scores of 3.133±0.642, the respondents agree that implementing data encryption measures can enhance an organization's information integrity. The respondents agree that by encrypting digital signatures or certificates, it becomes difficult for malicious actors to forge or tamper with them, thereby enhancing data availability, as indicated by the mean and standard deviation scores of 3.200±0.997. The respondents' response returned positive with the mean and

standard deviation scores of 3.110±0.929, indicating that they agreed that encryption processes in the organization is dependent on functional information and communication technology.

Table 2: Descriptive Statistics for Confidentiality

	Question Items on Confidentiality	Mean	STD
1	A security-conscious organizational culture enhances the confidentiality of the organization's information asset.	3.848	0.373
2	It is important to prevent unauthorized individuals or entities from accessing confidential information and compromising it through hacking, data breaches, physical theft of devices, or social engineering techniques.	3.190	0.588
3	Confidentiality can be compromised by insiders like employees, contractors, or partners who have legitimate access to sensitive information	3.352	0.770
4	Information and communication technology plays keep role in keeping information secure and confidential.	3.281	0.808
	Valid N listwise	28	

Source: Survey Data, 2023, and SPSS Window Output, Version 25.0

From table 2, the mean and standard deviation scores of 3.848±0.373 indicates that the respondents agreed that a security-conscious organizational culture enhances the confidentiality of the organization's information asset. The mean and standard deviation scores of 3.190±0.588 shows that it is important to prevent unauthorized individuals or entities from accessing confidential information and compromising it through hacking, data breaches, physical theft of devices, or social engineering techniques .indicate positive agreement from the respondents. The mean and standard deviation scores of 3.352±0.770 revealed that the respondents agreed that confidentiality can be compromised by insiders like employees, contractors, or partners who have legitimate access to sensitive information. It was agreed by respondents that information and communication technology plays key role in keeping information secure and confidential, going by the mean and standard deviation scores of 3.281±0.808.

Table 3: Descriptive Statistics of Integrity

	Question Items on Integrity	Mean	STD
1	Ensuring information integrity is a critical challenge in the digital age, where vast amounts of information are created, stored, and shared	3.338	0.709
2	Digital information can be easily tampered with or manipulated, making it difficult to trust the authenticity and accuracy of the data	3.933	0.872
3	Sophisticated cyberattacks can compromise the integrity of information systems, allowing unauthorized access, modification, or destruction of data	3.295	0.823
4	The integrity of information can be compromised if data is not properly protected by adequate information and communication technology infrastructures	3.262	0.832
	Valid N listwise	28	

Source: Survey Data, 2023, and SPSS Window Output, Version 25.0

In Table 3, by the mean and standard deviation scores of 3.338±0.709 respondents agreed that ensuring information integrity is a critical challenge in the digital age, where vast amounts of information are created, stored, and shared; the mean and standard deviation scores of 3.933±0.872, they that digital information can be easily tampered with or manipulated, making it difficult to trust the authenticity and accuracy of the data; by the mean and standard deviation scores of 3.295±0.823, they also agreed that sophisticated cyberattacks can compromise the integrity of information systems, allowing unauthorized access, modification, or destruction of data, and mean and standard deviation scores of 3.262±0.832 indicate that the integrity of information can be compromised if data is not properly protected by adequate information and communication technology infrastructures.

Table 4: Descriptive Statistics of Availability

	Question Items on Availability	Mean	STD
1	There is an overwhelming amount of information available across various sources in the organization	3.605	0.765
2	Misinformation, biased content, and fake news can easily spread, making it challenging to discern reliable information from false or misleading data	3.605	0.699
3	Limited internet connectivity, lack of resources and inadequate orientation can create barriers to accessing and benefiting from available information	3.457	0.771
4	Information and communication technology-driven data is easily accessible but are prone to internal and external attacks and hacks.	3.576	0.495
	Valid N listwise	28	

Source: Survey Data, 2023, and SPSS Window Output, Version 25.0

Through the mean and standard deviation scores of 3.605±0.765 the respondents agreed that there is an overwhelming amount of information available across various sources in the organization; misinformation, biased content, and fake news can easily spread, making it challenging to discern reliable information from false or misleading data (3.605±0.699); limited internet connectivity, lack of resources and inadequate orientation can create barriers to accessing and benefiting from available information (3.457±0.771); and the mean and standard deviation scores of 3.576±0.495 indicate that information and communication technology-driven data is easily accessible but are prone to internal and external attacks and hacks.

To determine the relationships that exist between these variables, the study formulated the following hypotheses:

$Ho_{1:}$ There is no significant relationship between data encryption and confidentiality.

Ho_2: There is no significant relationship between data encryption and integrity.

Ho_3: There is no significant relationship between data encryption and availability.

Table 5: Test Result of data encryption and information security

Statistics	**HO_4**	**HO_5**	**HO_6**
	DE (C)	**DE (I)**	**DE (A)**
Pearson correlation	0.807**	0.815**	0.711*
Sig(2-tailed)	.000	.000	.000
N	28	28	28

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

Source: Survey Data, 2023, and SPSS Window Output, Version 25.0

Table 5 above indicates a significant and positive relationship between data encryption and confidentiality; a significant and positive relationship between data encryption and integrity; data encryption and availability. The result has discarded the null hypothesis formulated and accepted the alternate hypothesis and thus established unequivocally that there is a positive and significant relationship between data encryption and information security.

DISCUSSION OF FINDINGS

Data Encryption and Information Security

The result of this study has established a strong, positive, and significant relationship exist between data encryption and confidentiality as a measure of information security. This finding aligns with the study of Khidzir et al. (2018) that showed that different data encryption provides different values for companies and these values can complement each other which improves

companies' information security. The findings of this study is supported by Bivbere (2019), who posits that data encryption is characterized by its mixed public-private orientation with security information that cannot be easily tampered with or manipulated, thereby making it easy to achieve authenticity and accuracy of the data. Also, Okerenke (2015) found that encryption is an important method for individuals and organization to secure sensitive data from hacking.

CONCLUSION

The study revealed that there is significant and positive relationship between data encryption and the measures of information security – confidentiality, integrity and availability. The study therefore concluded that there is significant and positive relationship between data encryption and information security.

RECOMMENDATION

The study therefore recommended that organizations should adopt the data encryption mechanism that protects its information from unauthorized access, mutilation and alteration.

REFERENCES

Al-Darwish, A. I., & Choe, P. (2019). A framework of information security integrated with human factors. In *International Conference on Human-Computer Interaction*. Springer, Cham, 217-229.

Alhosani, K. E., Khalid, S. K., Samsudin, N. A., Jamel, S., & Mohamad, K. M. (2019). A policy driven, human oriented information security model: A case study in UAE banking sector. IEEE Conference on Application, Information and Network Security (AINS).

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information security: A review of information security issues and techniques. *2nd International Conference on Computer Applications & Information Security (ICCAIS),* 1-6.

Aminzade, M. (2018). Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security*, *2018*(5), 9-11.

Bivbere, G. (2019). Sea Time Training: No Hope in Sight for Graduate Cadets (p. 5). Vanguard, (Lagos, 28 August).

Chang, H. S. (2016). International data encryption algorithm," *Hepatology*, 60 (6), 2125-2126.

Chernykh, L., Davydov, D. & Sihvonen, J. (2019). Financial stability and public confidence in banks BOFIT- Institute for Economies in Transition Bank of Finland BOFIT Discussion Papers 2/ 2019.

David, M. K & David, J. A. (2015). Database processing, information system relationships in 18th International Conference on Enterprise Information Systems. *International Journal of Computer Science and Mathematical Theory*, 5(1) 79-103.

Dhillion, G. S. (1995). Interpreting the management of information systems security. PhD Thesis, The London School of Economics and Political Science.

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An Empirical Study," *MIS Quarterly: Management Information Systems*, 34 (3), 549–566

Khidzir, N. Z., Daud, K. A. M., Ismail, A. R., Ghani, M. S. A. A., & Ibrahim, M. A. H. (2018). Information security requirement: The relationship between cybersecurity Risk confidentiality, integrity and availability in Digital Social Media. In Regional Conference on Science, Technology and Social Sciences, 229-237.

Kumar, R., & Bhatia, M. P. S. (2020). A systematic review of the security in cloud Computing: data integrity, confidentiality and Availability, *IEEE International Conference on Computing, Power and Communication Technologies (GUCON)*, Greater Noida, Nigeria. 334-337.

Okerenke H. (2015). The information flow in data warehouse ETL techniques for extracting, cleaning, conforming, and delivering data. *Wiley Publication*, 5(1), 37-48.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change, *Journal of Psychology*, 91, 93–114.

Rogers, R. W. (1983). Cognitive and psychological process in fear appeals and attitude change: a revised theory of protection motivation, in *Social Psychology*, J. Cacioppo and R. Petty, Eds., Guilford, New York, NY, USA.

Santos, R., Bernardino, J., & Vieira, M. (2011). A survey on data security in encryption: challenges and opportunities. EUROCON - International Conference on Computer as a Tool. *EUROCON, 5(1)14-30*.

Shoufan, A., & Damiani, E. (2017). On inter-rater reliability of information security experts. *Journal of Information Security and Applications, 37*, 101–111.

Thangaraju, G., & Rani, X. A. K. (2016). A Survey on Current Security Perspectives in Data warehouses. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 19(2).

Treacy, C., & Mccaffery, F. (2017). Data security overview for medical mobile apps assuring the confidentiality, integrity and availability of Data in Transmission. *International Journal on Advances in Security. 9*(3&4), 146-157.

Tsaregorodtsev, A. V., Kravets, O. J., Choporov, O. N., & Zelenina, A. N. (2018). Information security risk estimation for cloud infrastructure. *International Journal on Information Technologies & Security*, *10*(4).

Wang, Y., Yao, J., & Yu, X. (2018). Information security protection in software testing, *14th International Conference on Computational Intelligence and Security (CIS)*, Hangzhou, China, 449-452.

Zheng, X. & Cai, Z. (2020). Privacy-preserved data sharing towards multiple parties in industrial IoTs, IEEE *Journal on Selected Areas in Communications (JSAC), 38* (5), 968–979.