ANTHONY BABAJIDE BALOGUN
ID No: **UB73361SIN82521**

COURSE TOPIC:

Managing Organizational Information

ATLANTIC INTERNATIONAL UNIVERSITY

APRIL 2022

TABLE OF CONTENTS

1.0 INTRODUCTION

Information is defined as, a knowledge communicated or received concerning a particular thing or situation such as; news concerning a crime, an invention, knowledge gained through study, communication and even research.

Information Management is defined as a process that support the organization's learning activities. The process is classified into six related cycle such as; Identification, Acquisition, Analysis, Storage, Dissemination, and lastly; Information use.

Information Security is an act and the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information which can either be physical or in electronic format Information can also be anything on social media, data in mobile phone, biometrics etc. So, information security extends to many research areas such as; Cryptography, Mobile Computing, Cyber Forensics and even social media.

Knowledge management is the process of collecting, sharing, managing and deploying organizational knowledge. It is therefore a part of the organizational learning process focused on connecting people who are looking for knowledge within an organization to those who have it with the aim of improving and increasing the general level of team knowledge.

In this essay, I have carefully segmented my writing into the following headings in order to shed more light on how to manage organizational information:

- Information Management
- Information Management (IM) Vs Knowledge Management (KM)
- Information Management Process Cycle
- Information Management Policies
- Information Management Best Practices
- Principles of Information Management
- Information Security
- Authentication, Authorization and Access Control
- Types of Access Control
- Information Security Threats & Vulnerabilities
- Information Security Training & Awareness

2.0 INFORMATION MANAGEMENT

2.1 Definition

Information Management is defined as a process that support the organization's learning activities. The process is classified into six related cycle such as; Identification, Acquisition, Analysis, Storage, Dissemination, and lastly; Information use.

2.2 Importance

(i) Complex Decision Making

It helps to manage data which can be accessed by the administration in order to make a decision.

(ii) Analyses Trends

It uses tools to study the present market trend and to predict future trends.

(iii) Strategic Planning

It helps to determine the future needs of the organization and also helps in formulating goals and strategy. It helps to identify what is needed in order to meet the organization’s objective.

(iv) Goal Setting

Since the information given is based on the present data analysis, it is therefore considered suitable to determine the goals and objectives of an organization, hence, it is quite difficult for any organization to neglect this crucial importance.

(v) Problems Identification

It is easier to identify any problem as it relates to every aspect of activity that is taking place in the organization and likewise it's solution.

(vi) Increases Efficiency

Information provided is used to formulate the goals and strategy of the organization, hence the performance of the business can be determined which plays a very important role in increasing the efficiency of the organization.

(vii) Comparison Of Business Performance

The essential business data and information of the organization is stored and maintained in the information system database and since it can be accessed at any time; the present performance of the organization could be compared with its previous year’s achievement in order to ascertain the growth of the organization.

3.0 Information Management (IM) vs Knowledge Management (KM)

3.1 Information Management (IM)

Information Management is defined as a process that support the organization's learning activities. The process is classified into six categories such as; Identification, Acquisition, Analysis, Storage, Dissemination, and lastly; Information use.

3.2 Knowledge Management (KM)

Knowledge management is the process of collecting, sharing, managing and deploying organizational knowledge. It is therefore a part of the organizational learning process focused on connecting people who are looking for knowledge within an organization to those who have it with the aim of improving and increasing the general level of team knowledge.

3.3 Knowledge Management Basic Steps

(i) Collecting

This most important step or aspect of the knowledge management process is data collecting. If data is collected incorrectly, the resulting knowledge and the decision made based on such knowledge may not be accurate.

The process explains certain data collection points which may include the summary of routine reports such as monthly sales report or daily attendance reports.

(ii) Organizing

The next step after data collection is how to organize the data collected according to the set of rules as defined by the organization. For example, all sales related data could be grouped together and stored in the same table in a database which helps in data accuracy.

(iii) Summarizing

This step involves summarizing of the data collected by using various types of tools such as Pareto in order to get the proper understanding of the information. For example, every bulky and lengthy information is summarized and stored in a tabular form for proper understanding.

(iv) Analyzing

The data collected is analyzed at this stage in which the information is studied very well in order to find any relationships, redundancies and patterns in the data. This stage requires an experience personnel that can reason and analyses information efficiently and accurately.

(v) Synthesizing

Information becomes knowledge at the synthesizing stage. The results of analysis for the reports are collated together to get different types of concepts and pattern because a behaviour of one entity could be applied to another thereby helping an organization to have set of knowledge elements to be used.

(vi) Decision Making

The knowledge is used for decision making at this stage. For example, the knowledge related to previous estimates can be used when estimating a specific project or a task thereby adding value to the knowledge management of an organization and saving money on the long run.

3.4 How KM is stored

Knowledge must be stored in a certain manner which include:

(i) Plain or structured

(ii) Hyperlink form using XML

(iii) Database structures

(iv) KM representation systems

(v) Combination of the above

4.0 INFORMATION MANAGEMENT PROCESS CYCLE

Information management allows organizations to perform more efficiently with the help of a reliable, accurate and timely information. Information management process encompasses various cycle of different functions which are described below;

(i) Collection

Information collection can be in different form and they include; oral, electronic, written, audio or video. In this category of activities, only the information that is needed and trusted are collected. Every other irrelevant information and data are discarded.

(ii) Storage

This aspect is very important as the stored information are make use of during analysis, legislative requirements and historical trends. Therefore, it is crucial that, the right sets of people have access to the information as well as back-ups of such information wherever they are stored.

(iii) Curation

Within this cycle, curation is defined as the process of gathering and organizing information which are relevant to a particular discipline or topic with the primary intention of adding value.

(iv) Dissemination

As the name implies, this handle the process of how information is shared and with who they are shared with. It also handles the type of format, how often, and under what criteria and circumstances, bearing in mind the available security protocols.

(v) Archiving

Information needs to be archived regularly based on the Organization policy and procedures. Therefore, it is imperative to have an effective classification strategy in place that forecast future uses.

(vi) Destruction

This is the process of destroying or deleting organizational information that have come to the end of its usage or life cycle which have no use to the organization anymore. Although, such information may be important for now but may not have any value in the nearest future. A good example will be privacy laws which allows an organization to archive information for a particular time or period.

5.0 INFORMATION MANAGEMENT POLICIES

These are type of rules that enables organizations to manage and track things such as; how long a content is retained and what action(s) users can take with such content. Thus, it helps organizations to adhere and comply with legal regulations.

These policies also give organization's staff direction to create, capture and to manage organizational information assets such as; records and data in an attempt to satisfy business, legal and stakeholder requirements.

5.1 Features of information management policies

(i) Auditing policy feature

It assists organizations to assess how their content management systems are used. This is done by logging the events and operations that are carried out on documents and all listed items. It can be configured in such a way that; events are logged when a document is altered, viewed and deleted. Audit information is stored naturally in a single audit log placed on the server which can be queried at any given time.

(ii) Expiration policy feature

This feature helps organizations to delete or remove all the outdated contents from their sites in a trackable manner. It also assists in managing the cost and risk linked with archiving outdated content. Expiration policy feature can be configured to states that, a particular content expires on a certain date after the document was created or last edited or modified.

(iii) Custom policy features

This can also be created and deployed by an organization to meet specific functions. An organization who engages in manufacturing may want to create and define an information management policy which will not allow users from printing copies of these documents on a non-secure printer.

6.0 INFORMATION MANAGEMENT BEST PRACTICES

6.1 Ease of Use

To start with, an information management system must be easy to use. So, if the user interface is not designed very well, it may make both the managers and the employees get frustrated and confused and therefore make them to find other ways to share information which may be contrary to following security protocols.

6.2 Get User Buy-in

This comes hand-in-hand with ease of use which makes it very important to consider users' needs.

6.3 Plan and Design at the Enterprise Level

This is widely believed to start at enterprise level instead of allowing each department to manage its information management process

6.4 Enterprise-wide Reuse

Data and information must be made available across all departments which will allow better decision making and feedback.

6.5 Data Management

Formulate policies which will guide organization to change, distribute, archive and delete information.

6.6 Centralized Data Management and Governance

This is the overall management of the availability, usability, integrity and security of data which an organization makes use of.

6.7 Metadata Management

It arranged and categorize data in such a way that, it can be compared with data from other systems. It also helps track who an access to data should be given.

6.8 Data Quality Management

Carrying out a quality check will prevent the use of bad data, so, data quality management creates a process that corrects errors as soon as they are found, thereby keeping the quality of data very high.

6.9 Make Data and Information Available

The primary purpose of information management is to manage the way data and information is shared; therefore, any information management program should maintain this as a core principle.

6.10 Training and Accountability

Training must be organized for those who access data and create information on the policies. In a case where policies are broken, both the managers and the employees must be held accountable.

6.11 IT and Business Collaboration

There should be a cooperation between data owner and those who store and process the data.

6.12 Plan for Continuous Improvement

As business needs and data changes, there should be a plan to design a technology that supports it so that it can accommodate new inputs in order to create new outputs.

6.13 Audit Trails

A robust and well-designed information systems must be able to reveal who accessed information, when it was accessed and what was done with such information. This prevents breaches in security and ensures that everybody follows the established and documented policies.

7.0 PRINCIPLES OF INFORMATION MANAGEMENT

There are so many principles of information management in the IT world today but the most well-known and respected are the principles outlined by the Information Management Body of Knowledge otherwise known with its acronym IMBOK. IMBOK outlines a framework which divided management skills into knowledge areas and process areas.

7.1 The knowledge areas

(i) *Information Technology (IT):* Comprises of both the Hardware and software

(ii) *Information Systems*: This is a system built to meets business needs and policies

(iii) *Business Information*: Created by analyzing data using tools such as the information system

(iv) *Business Processes*: It shows how to assess and evaluate information in order to make decisions

(v) *Business Benefit*: This will reveal the desired advantage that the business information will provide

(vi) *Business Strategy*: This is the master plan which gives an organization a direction.

7.2 The process areas

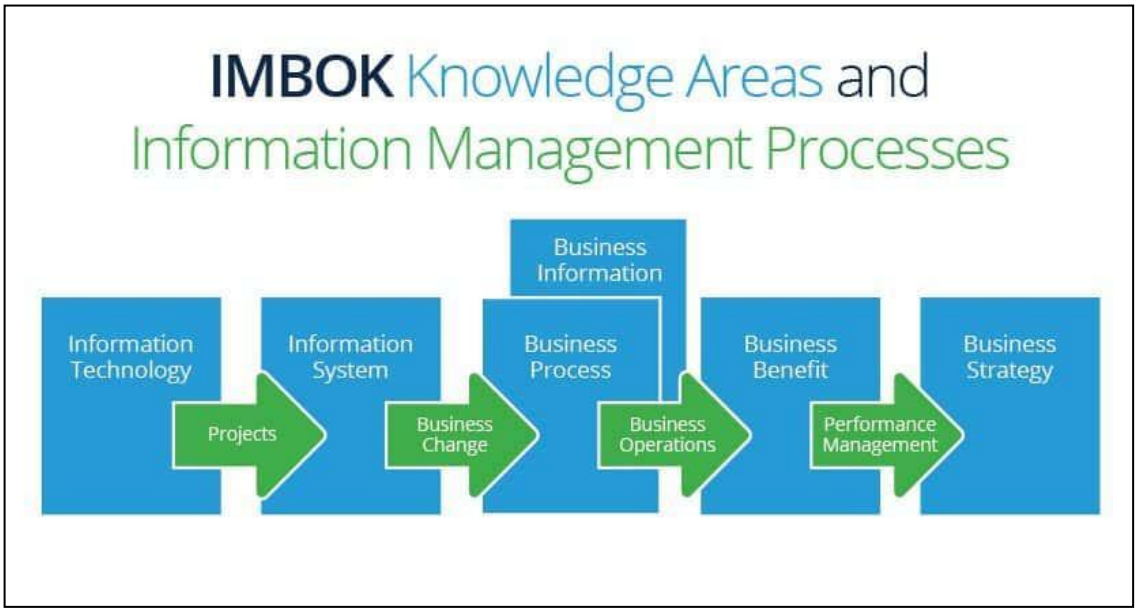
(i) *Projects*: Addition of software and hardware to information systems

(ii) *Business Change*: Assessment of information in order to drive improvements in processes

(iii) *Business Operations*: This is the daily running of a business

(iv) *Performance Management*: This is a process of making sure that business operations are running as specified.

Figure 1



(Smartsheet, n.d.)

(Figure 1: IMBOK knowledge areas and IM process)

8.0 INFORMATION SECURITY

Information is defined as, a knowledge communicated or received concerning a particular thing or situation such as; news concerning a crime, an invention, knowledge gained through study, communication and even research.

Information Security is an act and the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information which can either be physical or in electronic format Information can also be anything on social media, data in mobile phone, biometrics etc. So, information security extends to many research areas such as; Cryptography, Mobile Computing, Cyber Forensics and even social media.

The process of protecting any internet based connected systems such as hardware, software and data from cyber threats and attacks is known as Cybersecurity. A good and well-planned cybersecurity strategy should provide a strong security posture against malicious attacks designed to access, alter, delete, destroy an organization's or user's sensitive data or information. It is also an effective way in preventing or mitigating attacks that is aimed to destroy system's or device's operations.

8.1 Information Security Objectives

Basically, information security architecture is built around three main objectives commonly known as CIA which is an acronym for; Confidentiality, Integrity and Availability.

(i) Confidentiality

Confidentiality in the CIA trad simply means that, information is not in any way or form disclosed to any unauthorized individuals, entities and process.

For example, if a user mistakenly exposed his/her login details to another person or someone saw while the details are being keyed in to login, then we say that, login details which comprises of such information as; login name, password and any other form of authentication has been compromised, hence the confidentiality of those details has been breached.

Therefore, an effort must be made to establish and to enforce appropriate authorization controls in order to allow only the legitimate users to have access to network resources, in other words, only users who need access should get access.

(ii) Integrity

This basically describes the maintaining accuracy and completeness of data, that is to say that, data cannot be edited in an unauthorized way. For example, when an employee leaves an organization, his existing data in all departments such as accounts and HR should be updated to reflect status to 'Resigned' so that he does not have access to those data and that only authorized person should be allowed to edit the employee data.

Therefore, efforts must also be established and to enforce controls that will not allow alteration of any kind to information without a proper permission from the data owner. This helps to maintain the originality of the data.

(iii) Availability

As the name implies, information must be readily available as at when needed. For example, if there is need to access information of a particular employee in an organization for a particular reason or information, data must be readily available to be queried in order to get such information required. However, an attack known as Denial of Service (DoS) attack is a factor that can hamper the availability of such information.

Availability forms the backbone of any Information Technology operations. As the name implies, efforts and controls must be focused on making sure that systems, networks and software are always available in a timely fashion and must never be out of service in order not to disrupts IT operations and service delivery.

Apart from the above-mentioned security programs, there are other principles that governs information security programs as described below:

(i) Non repudiation

This simply means that, one party cannot deny receiving and sending a message or a transaction. A good example will be in the transaction of crypto currency where it is sufficient to show that, message matches the digital signature which is signed with sender's private key and that sender could have a sent a message and no one else could have changed or manipulated it in any way in transit. Therefore, data integrity and authenticity are pre-requisites for Non repudiation.

(ii) Authenticity

This means that, verification is made against users to actually confirm the authenticity of who they say they are and that each input arriving at destination is from a trusted source. This principle if properly followed will guarantee the validity and equinity of message received from a trusted source through a valid transmission.

(iii) Accountability

This principle means that, there should be a possibility of tracing the actions and activities of an entity uniquely to that entity. For example, not every employee should be allowed to alter or to amend other employee's data if not authorized. All alterations and amendments should be left for the particular department and the authorized staff concerned; thus, we can say if a change is implemented in this way, then it will be possible to trace the actions uniquely to an entity thereby enabling accountability.

Furthermore, at the centre of information security is what is known as Information Assurance which means, the act of maintaining CIA of information by ensuring that information is not compromised in any way when critical issues such as natural disasters, computers, networks and server's malfunctions happen.

9.0 AUTHENTICATION, AUTHORIZATION AND ACCESS CONTROL

9.1 Authentication

Authentication is defined as any process by which a system verifies the identity of a user who wishes to have access to the system. For the mere fact that control is typically based on the identity of the user who requests access to a resource, authentication is necessary to effect security.

In a nutshell, authentication is the security practice of confirming that someone is who they claim to be. User authentication is typically implemented via credentials which at a barest minimum consist of a two form of identity such as; user ID and password.

9.2 Authorization

Authorization is a process by which a system either grants or revokes the right to access some data or perform some action on a system. Normally, a user must log in to a system by using some form of identities.

9.3 Access Control

Access control is described as a security term that is used to refer to a set of policies to restrict access to information, tools and physical locations.

The primary function of access control mechanism is to determine which operation(s) a user can or cannot do by comparing the user's identity to what is known as an access control list (ACL). Access controls comprises of;

(a) File permissions - grant such right as to create, read, edit or delete a file.

(b) Program permissions - grant such right to execute a program.

(c) Data permissions - grant the right to retrieve or update information in a particular database.

However, physical access control is a collection of policies used in controlling who is granted access to a physical location. In a real-world scenario, examples of physical access control include the following:

(a) Bar-room bouncers

(b) Subway turnstiles

(c) Airport customs agents

(d) Keycard or

(e) Badge scanners in organization

10.0 TYPES OF ACCESS CONTROL

After a successful authentication process has been completed, then user authorization can be determined in one of several ways described below:

10.1 Mandatory Access Control (MAC)

This establishes a strict security policy for individual users and the resources, systems, or data they are allowed to access. A system administrator is typically in control of this operation as individual users are not permitted to set, alter, or withdraw permissions in a way that goes against the existing policies. Both the subject known as the user and the objects such as the data, system and other resource must be assigned a similar security attribute in order for them to interact with each other.

10.2 Role-based Access Control (RBAC)

This type of access control establishes permissions based on groups like; defined sets of users such as bank employees and roles such as; defined sets of actions a branch manager might perform.

Like Mandatory access control (MAC), users are not permitted to alter or change the level of access control which has been assigned or granted to their role.

10.3 Discretionary access control (DAC)

The moment a user has been granted permission by a system administrator to access an object, then he can also grant access to other users on an as-needed basis. This type of access control has been noted in many cases to have introduced security vulnerabilities into an IT environment. So, when considering which method authorization is most appropriate for an organization, security needs must be seriously taken into account.

Therefore, organizations such as banks, government establishment that require a high level of data confidentiality will obviously opt for a more stringent forms of access control like MAC, while others who favor more user or role-based permissions will settle for RBAC and DAC systems.

10.4 Virtual Private Network (VPN)

A VPN is another popular tool used for information access control. This service allows remote users to access the Internet as though they were connected to a private network.

For example, corporate networks will often use VPNs to manage and monitor access control to their internal network across a geographic location.

A company may have offices in San Francisco, USA and another in Leeds, UK as well as other remote employees scattered across the globe, can make use of a VPN so that all of these employees can securely log into their internal network, regardless of where they are located.

11.0 INFORMATION SECURITY THREATS & VULNERABILITIES

Despite all the efforts of cybersecurity professionals to close security gaps, attackers are always looking for new ways to exploit emerging vulnerabilities and weaknesses. Those emerging and evolving threats include:

11.1 Malware

Malware refers to malicious software such as worms, viruses, Trojans and spyware which allows unauthorized access with the aim of causing damages to a computer. They are designed by attackers to avoid familiar detection methods such as antivirus tools which can scan malicious file attachments.

11.2 Ransomware

This type of malware is designed by attackers to lock down files, data or systems in order to threatens the owner or an organization of deleting their sensitive data if certain conditions are not met. Mostly, attackers use ransomware to demand money from their victims.

11.3 Phishing

Phishing is an attack in the form of a social engineering which tricks users into making available their sensitive information. In this type of attack or scam, emails or text messages which appears to originate from a genuine company asking for sensitive information such as credit card details or login information.

11.4 Insider threats

Either current or old employees, business partners, contractors or anyone who has at one time or another had an access to a system or networks in the past can be considered as an insider threat if they abuse their access rights or permissions.

11.5 Distributed denial-of-service (DDoS) attacks

The main aim of a Distributed denial-of-service (DDoS) attack is to make an attempt to crash a server, website or network by flooding it with traffic which usually comes from multiple and coordinated systems. DDoS attacks floods enterprise networks through a protocol known as the simple network management protocol (SNMP) which is used for such devices like modems, printers, switches, routers and servers.

11.6 Advanced persistent threats (APTs)

In an Advanced persistent threat, an intruder or group of attackers penetrate a system and remain undetected for a long period of time. The primary aim is to spy on business activities and to steal sensitive data while avoiding a pre-defined defensive countermeasure.

11.7 Man-in-the-middle attacks

This is an eavesdropping attack whereby a cyber-criminal highjack messages between two parties in order to steal data. For example, an attacker can intercept unencrypted data on an unsecure Wi-Fi network which is being transmitted between guest's device and the network.

12.0 INFORMATION SECURITY TRAINING & AWARENESS

12.1 Awareness Training

'Hackers' perpetrate their cyber-attack by first by tricking 'less-knowledgeable' members of an organization into providing or revealing some sensitive information such as a 'login name' and 'password' or some form of access control combination 'coordinates' to them in order to have an access to the organization’s systems and networks. This type of cyberattack is known as "phishing” or “social engineering.”

A typical social engineering trick will probably send an email to employees that is made to look as if the CEO or any other line manager boss sent it by asking them to click on a bogus or fake link in order for them to carry out an installation on their computer.

The best way to avoid these types of attacks is by educating employees about cybersecurity and create an awareness so that when they see these types of emails, they will be able to know that they could be a potential security threat.

Putting together an effective cybersecurity awareness and training will make sure that all employees get training related to cyber threats, this process should be the basis of every organization’s cybersecurity risk management plan.

Employees should not only be educated on what to look for but also be equipped with the knowledge of what to do and who they should contact if they see something suspicious.

13.0 CONCLUSION

Intruders perpetrate their cyber-attack by first by tricking 'less-knowledgeable' members of an organization into providing or revealing some sensitive information such as a 'login name' and 'password' or some form of access control combination 'coordinates' to them in order to have an access to the organization’s systems and networks. This type of cyberattack is known as "phishing” or “social engineering.”

The best way to avoid these types of attacks is by educating employees about cybersecurity and create an awareness so that when they see these types of emails, they will be able to know that they could be a potential security threat. A good example will be a security training organized for users on how to delete suspicious and malicious email attachments and to avoid using or plugging in an unknown USB device found somewhere into a system

Therefore, putting together an effective cybersecurity awareness and training will make sure that all employees get training related to cyber threats, this process should be the basis of every organization’s cybersecurity risk management plan.

Employees should not only be educated on what to look for but also be equipped with the knowledge of what to do and who they should contact if they see something suspicious.

Finally, many organizations are now migrating their applications, data, and identities to the cloud which means that, users are connecting directly to the Internet to access the data. Cloud security can help protect the usage of software-as-a-service (SaaS) applications and the public cloud.

A good and strong IT security strategy provides layers of protection to protect against cyber threat and crime such as gaining access to sensitive information with the aim of altering or destroying data, extorting money from users or organizations and an attempt to disrupt business operations.

14.0 BIBLIOGRAPHY

Smartsheet. (n.d.). *Principles of Information Management*. Retrieved from Principles of Information Management: https://www.smartsheet.com/information-management