*Available online at http://www.journalcra.com*

*International Journal of Current Research*
*Vol. 4, Issue 08, pp. 135-139. August, 2012*

**INTERNATIONAL JOURNAL OF CURRENT RESEARCH**

**ISSN: 0975-833X**

## RESEARCH ARTICLE

# EMERGENCE OF CRITICAL INFORMATION ASSETS AS A CHALLENGE FOR AN ORGANIZATION

***,[1]Abubakar Aminu Mu'azu and [2]Ibrahim A. Lawal**

[1]Department of Mathematics and Computer Science, Umaru Musa Yar'adua University Katsina, Nigeria
[2]Department of Computer Science Federal College of Education Kano, Nigeria

**ARTICLE INFO**

***Article History:***
Received 18th June, 2012
Received in revised form
19th July, 2012
Accepted 25th August, 2012
Published online 29th September, 2012

***Key words:***
Information assets;
Critical Information assets;
OCTAVE Allegro.

**ABSTRACT**

The emergence of information asset hails from information resource management which had been to regulate and design all of the pre-requisites necessary for information production. It considered becoming an expressible chunk of information of which organizations reconsider as valuable. It takes resurgence after some organizations realized the importance of information assets with the aim of avoiding larger losses in the event that its business activities cannot continue to function due to loss of IT infrastructure and data. The basic goal of information management is to harness the information resources and information capabilities in order to enable the organization to learn and adapt to its changing environment. Critical information assets are regarded as any essential piece of information, stored in any manner which is absolutely necessary for the success of an organization. It is considered as a component of critical infrastructures that covers both physical and information infrastructures while the definition is limited to the information infrastructure. The main problem facing organizations is the ability to provide information that could potentially be used to their disadvantage if it were disclosed. This paper discuss some means by which an organization would be able to know and indentify the critical data that yields useful information and must understand why it is important to it day-to-day business functions.



## INTRODUCTION

It is a widely accepted that business and commerce are increasingly becoming information-based; the need to identify the organizational critical information asset has grown accordingly. The main problem facing governments/ organization is the reluctance of business to provide information that could potentially be used to their disadvantage if it were disclosed (Orlowski, 2001). A number of organizations have privately expressed concern that they may expose themselves to legal action if it became known that they were aware of security vulnerabilities to the organization". Conversely, computer, software, databases, files, applications, systems software and computer networks are all part of your information technology (IT) assets (Haag, Cummings *et al*., 2004). Like most other public and private organizations, depend extremely upon IT and would find it impractical if not almost impossible to function without it. Any temporary or extended loss to any portion of these IT assets could have tremendous impact on organization's financial and economic stability and to its own security (Lester, Postlewaite *et al*., 2008).

However, the term assets tend to be considered of only tangible possessions to which we can attach a financial value (Haag, Cummings *et al*., 2004). As we move towards identifying what business functions or records are essential to organizational operation, knowing their value is important.

***Corresponding author:** abuaminum@gmail.com*

It is therefore vital for organizations to identify assets which might not appear to have a monetary value, but are often irreplaceable and can result in great financial lost to their owners. Organizations need to be vigilant and conscious that piece of information does not disappear if it is copied, even if that copying is a form of theft; neither does a computer file change or disappear if it is duplicated. With the increasing importance of information technology for the continuation of business critical functions, combined with a transition to an around-the-clock economy, the importance of protecting an organization's data and IT infrastructure in the event of a disruptive situation has become an increasing and more visible business priority in recent years (Whisenant, 2009).

Additionally, information forms the cornerstone of any critical infrastructure and it is important to recognize that only a certain segment of the organization's information may warrant protection (Uhl, Warshaw *et al*., 2002) . It is estimated that most large companies spend between 2% and 4% of their IT budget on disaster recovery planning, with the aim of avoiding larger losses in the event that the business cannot continue to function due to loss of IT infrastructure and data". Of companies that had a major loss of business data, 43% never reopen, 51% close within two years, and only 6% will survive long-term (Aminu Mu'Azu, 2010). Additionally, the integrity and usage of information assets are significant for any business towards avoiding larger losses in the cause of any occurrences of discontinuity of their business function. As such, it is highly important for an organization to establish a

regular and organized technique to understand and manage its information resources. The information audit provides the mechanism to discover, monitor and evaluate an organization's information status in order to implement, maintain or improve the organization's information management. The main aim of this paper is to identify the emergence of critical information assets of an organization which become an essential for many reasons. An organization will come to know what is critical and essential for the business. It will be able to take appropriate decisions regarding the level of security that should be provided to protect the assets in case of disaster. All of the assets identified may have attributes that have impact on the effectiveness and survival of an organization in business landscape.

## RELATED WORK

### *A. Overview of Information Assets*

The concept of information asset appears to be an important issue for an organization in realising the potentials involve in managing its resources. (Oppenheim, Stenson *et al*. 2003) mentioned that "The concept of information as an asset has its origins in information resource management (IRM). He added that IRM treated information as an organizational resource, which has a life-cycle of creation, distribution, use and disposal, and just like any other resource; information could be assigned a cost and value. As in(Aminu Mu'Azu 2010) this approach was particularly suitable for application to the corporate information resources of organizations where the cost of information is often high and where there was a growing need to justify such costs by the positioning of information as a business asset".

### *B. Definition of Information Asset*

Information has been defined by many professionals as one of the most organizational vital needs in carrying out its business functions. Not all information assets are technology dependent, but the focus of this advice is on electronically held information assets. Care must be taken when applying this advice to non-ICT dependent assets. According (Choo 2002) defined information assets as; "Definable piece of information, stored in any manner which is recognized as 'valuable' to the organization. However, (Cost Information Assurance 2002) defined information asset as data critical to daily operations and sustaining competitive differentiation. More so according to (ASIS INTERNATIONAL JANUARY 2010), information asset is defined in their guideline as "An information asset is a collection of data that has recognized value to an agency in performing its business functions and meeting agency requirements. Information assets can be documents, electronic messages, a row in a database (or the database table itself), collections of metadata, or a table or figure within a document".

However, it was further mention that "Information assets may include all forms and types of financial, business, and scientific information, customer related information (including identification, preferences, and pricing), business strategies, manufacturing processes, research and development, personnel data, etc. Such information may be electronically generated and processed, stored on some form of storage media, printed on paper or on other mediums whereby information may be recorded and communicated.
As business and commerce becomes increasingly information-based, the need to identify the organizational critical information asset has grown accordingly most especially in education context.

### *C. Identification and Classification Information Asset*

The best practice in identifying and classifying of organizational assets is actually to address the assets that need a safeguard for the exciting aspect of information security for business continuity. According to (Kadam 2002) , the task of identifying assets that need to be protected is a less glamorous aspect of information security. But unless we know these assets, their locations and value, how are we going to decide the amount of time, effort or money that we should spend on securing the assets?"

Identifying, understanding and assessing the current information asset status and value have become significant activities of an organization. This perhaps would assist in making the operational activities to continue functioning.

## CRITICAL INFORMATION ASSETS (CIAS)

It is clear that identifying critical information asset should not be treated lightly in any organization. What should happen when interrupted damage or lost? How would it cost to restore the system in order? To use information effectively in their operations, there is need for an organization to identify the critical data that yields useful information and must understand why it is important to it day-to-day business functions.

Consider the different forms that information can take. Information at its most basic level is in the form of raw data — ones and zeros in a computer; documents in file cabinets; fax transmissions. Data can come from a variety of sources and can exist in a wide range of formats, such as an employee's handwritten notes, an e-mail message, a customer relationship management (CRM) database, and photographs or drawings that have been scanned into electronic files. This disparate, raw data remains relatively useless and insignificant until it is compiled, interpreted and transformed into relevant information, so its needs to identify the critical data (Aminu Mu'Azu 2010). Moere so, according the definition of information assets by (Choo 2002), critical information asset means essential piece of information, stored in any manner which is absolutely necessary for the success of an organization in order to adapt its changing environment.

Critical information assets requiring protection include critical and sensitive information- financial information, library automation, financial student records, payroll, purchasing and other confidential information- as well as computer-communications system in which they reside.

In the past, critical information asset protection has meant:

- Keeping it confidential, providing access only to those having a legitimate need for it
- Maintaining its integrity, assuring that all changes are authorized and intended.
- Ensuring its availability.

Traditionally, security practitioners concern themselves with the confidentiality, integrity, availability, and auditability of information assets. Information assets vary in how critical they are to the business. Some organizations value confidentiality of data most highly, while others demand integrity and availability. In highly regulated contexts, it might be important to audit access and modification to sensitive information. Without knowing what assets need protection, and without knowing what happens when the protection fails, the rest of the risk analysis techniques cannot produce worthwhile results. An asset is referred to in threat analysis parlance as a threat target. The owners of any organization need to know the value of its critical information assets and to be aware of its weakness, need to identify, examine and understand the threats facing the information assets. This must be prepared fully to identify those threats post risk to the institution and the security of its information assets by conducting risk analysis.

### *RISK ANALYSIS/ ASSESSMENT*

Most of companies rely so much on their systems; they need to ensure that the systems are always available. Risk analysis is important in determining the likelihood of defeat organizational critical information assets will face. (Michael E. Whitman and Herbert J. Mattord 2008), 2008 defined risk analysis as "An analysis of the probability of loss faced by information assets within its context". Recognizing and identifying information assets to be protected, and evaluating the risk to those assets could also be regarded as risk analysis. However, Risk analysis is the process of defining and analyzing the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events. In IT, a risk analysis report can be used to align technology-related objectives with a company's business objectives. (Alberts, Dorofee, 2003). Another definition from (wishes from SIGMA 2002) stated that risk analysis is a systematic process for assessing and integrating professional judgments about probable adverse conditions and/or events. According to (Saint-Germain, 2005) risk analysis is identifying the information assets to be protected, and evaluating the risk to those assets. For effective operation of any organization, (Clark, Dawkins *et al*. 2005) mentioned that; performing a risk analysis involves finding and documenting the vulnerabilities in critical information assets. They also stated that pinpointing these vulnerabilities can be a time-consuming task that will require the assistance of experts in the hardware and software used (operating systems, communications, and applications). If the analysis or entire assessment is to be performed by a group of people outside the agency, it is important that the agency have realistic expectations about what the process will accomplish. It should be understood that the quality of the assessment will be directly related to the degree of cooperation and participation that the agency provides to the assessment team.

When changes are made to the information assets, or if the risk to the information assets is varied, risk analysis is made again for the relevant information assets, and the Policy is reviewed as required. Also in respect to regular review of the Policy, the work should begin with risk analysis. In addition, if vulnerability is found in any information assets, action should be promptly taken if necessary. The figure below illustrating the flow of risk analysis/assessment and is adopted from (Saint-Germain 2005)

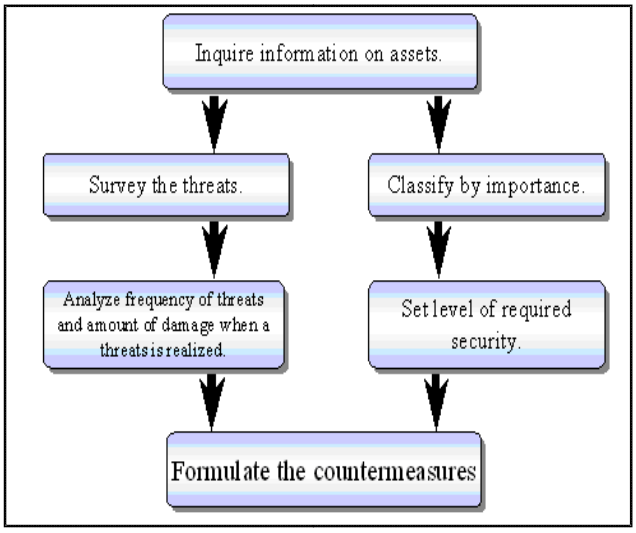


**Figure 1: Flow of risk analysis**

### *RISK ANALYSIS MODELS*

There are a number of risk analysis models, including those from NIST, NSA, ISO 17799, and ISO 27001. Another commonly used risk analysis model is Facilitated Risk Analysis Process (FRAP). However, none of these models was designed with the needs of higher education in mind. The NIST methodology was developed for federal government IT systems as indicated by the definition of risk: Two models developed at universities, called OCTAVE and STAR are summarized here.

### *OCTAVE*

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method is a risk-based, asset-driven model developed at the CERT Coordination Centre at Carnegie Mellon University. This comprehensive model has been adapted to small organizations (OCTAVE-S). In OCTAVE, assets are defined quite generally to include people, hardware and software, information, and systems. OCTAVE emphasizes the need to "focus on the critical few," which are identified through a process of ranking key assets based on their importance to the business goal of the organization, likely threats to these assets, any associated vulnerabilities (technical or organizational), and the impact of a problem involving each asset. One aim of the OCTAVE method is to develop a global perspective of security within an organization, involving perspectives from all levels to ensure that solutions are not too narrowly focused or technologically driven.

### *STAR*

The Security Targeting and Analysis of Risks (STAR) model, developed and used at Virginia Tech, provides a decision aid to help colleges and universities perform a cursory risk analysis of their IT systems. The aim is to simplify the risk analysis process and help institutions or departments prioritize their IT risks and identify which effective security practices they should concentrate on first (they might find that one

priority is to perform a more complete risk assessment). There are seven steps in the STAR process:

- Identify information assets
- Aggregate and prioritize the assets (using an Excel spreadsheet to facilitate voting on the priority of each asset)
- Identify risks
- Prioritize risks (using an Excel spreadsheet to facilitate voting on the priority of risks)
- List and define risks
- Reference risks to critical assets
- Recommendations for resolving risks

An organization typically faces variety of threat and the ultimate goal of risk assessment is to assess the circumstances and setting of each information assets to reveal any vulnerability.

## *IDENTIFYING CRITICAL INFORMATION ASSET*

At a high-level asset view, a certain system might be identified as being critical. But closer examination reveals that it's actually particular data on the system that is critical. The system is just one of potentially many places where that data is stored, transported, and processed, both inside and outside the organization. These places are referred to as containers. They are usually some type of technical asset; hardware, software, or system but can also be a physical object such as paper or even a person. An information asset's containers can become points of vulnerability where it is at risk. So an important part of the Allegro method is identifying each information asset's containers.

For an organization to be effective, it should be able to establish a security guidelines related to its resources, then identify critical assets, conduct appropriate risk assessments, and review the multitude of possible security enhancement measures, using risk management principles. According to the (Jones, Ashenden 2005) could be every piece of information about your organization falls in this category. This information has been collected, classified, organized and stored in various forms which include:

- Databases: Information about your customers, personnel, production, sales, marketing, finances. This information is critical for your business. It's confidentiality, integrity and availability is of utmost importance.
- Data files: Transactional data giving up-to-date information about each event.
- Operational and support procedures: These have been developed over the years and provide detailed instructions on how to perform various activities.
- Archived information: Old information that may be required to be maintained by law.
- Continuity plans, fallback arrangements: These would be developed to overcome any disaster and maintain the continuity of business. Absence of these will lead to ad-hoc decisions in a crisis.

The level to which information assets impacted on the ability of the organization to become more or less effective depends on the extent to which they encourage specialization and uniqueness. (Dmcker 1993) describes an effective organization as a; "Special purpose institution" and also says

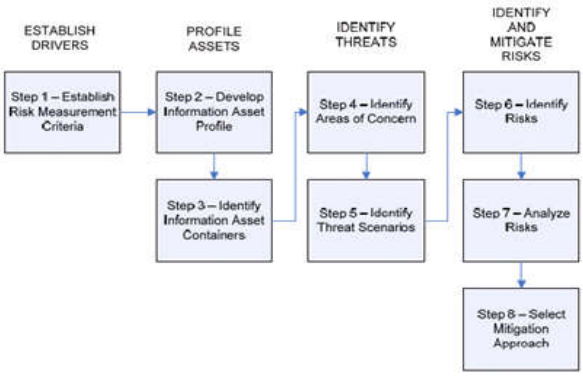


**Figure 2. OCTAVE Allegro Roadmap (Caralli, Stevens *et al.* 2007)**

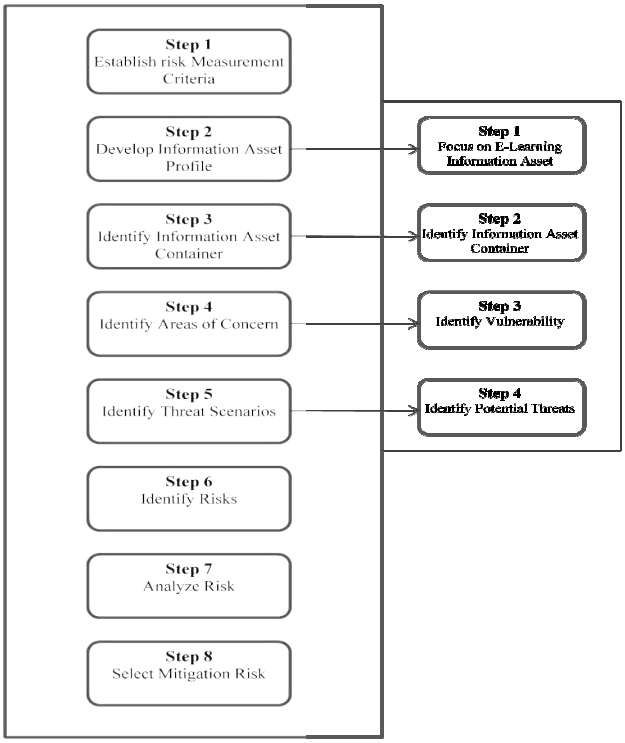


**Figure 3. Comparism between OCTAVE Allegro and Adopted Steps**

"organizations are effective because they concentrate on one task". Therefore, the characteristics or attributes of information as an asset can be identified and perhaps measured. For effectiveness and efficiency of emergence of organizational operation, the researcher adopted the methods of identifying organizational information assets stated in (Caralli, Stevens *et al*. 2007) OCTAVE Allegro model.

## *OCTAVE Allegro Method*

OCTAVE Allegro is a streamlined variant of the OCTAVE method that focuses on information assets. Like previous OCTAVE methods, OCTAVE Allegro can be performed in a workshop-style, collaborative setting, but it is also well-suited for individuals who want to perform risk assessment without extensive organizational involvement, expertise, or input.

Because the primary focus of OCTAVE Allegro is the information asset, the organization's other important assets are identified and assessed based on the information assets to which they are connected. This process eliminates potential confusion about scope and reduces the possibility that extensive data gathering and analysis is performed for assets that are poorly defined, outside of the scope of the assessment, or in need of further decomposition. There are eight steps of the OCTAVE Allegro methodology according to (Caralli, Stevens *et al*. 2007) and are organized into four phases, as illustrated. From the outputs of each steps mentioned in the process above, it's relevant as for this research to select some steps that best suit the research findings. Thus, begins from step two (2) till five (5) which sequentially assist in identifying critical information asset in an organization. This is shown in the Figure 3. For any organization that wants to exploit their information assets and address issues surrounding information overload in order to achieve their efficiency, transparency and differentiation objectives need to coordinate information management strategies in place.

## CONCLUSION

Information is a valuable asset for any organization and it's an important strategic asset for the organization as important as people, capital and technology. Like other corporate assets, information must be managed. The goal of managing information as an asset is to maximize its value by improving its consistency, accuracy, accessibility, utility, safety and transparency. When managed as an asset, information can improve supply chain performance and strengthen the relationships with customers, suppliers, partners and employees.

Yet for many organizations, information remains a liability, requiring additional rigor and focus at the enterprise level. Often seen during compliance or efficiency drives, information as a liability reflects the lack of coordinated information management actions, resulting in an increase in risk and exposure. Manifestations of information as a liability include inaccurate or unreliable reporting, out-of-date information, or content that is hard to find. Information as a liability acts as a barrier to the successful execution of the business strategy.

## REFERENCE


Alberts, C.J. And Dorofee, A.J., 2003. *Managing Information Security Risks: The Octave Approach.* Addison-Wesley Professional.

Aminu Mu'azu, A., 2010. *Critical Information Assets Disaster Management Audit Model For Utm Student Information System.*

Asis International, January 2010. Standards Developmentprocedures

Caralli, R.A., Stevens, J.F., Young, L.R. And Wilson, W.R., 2007. *Introducing Octave Allegro: Improving The Information Security Risk Assessment Process,*

Choo, C.W., 2002. *Information Management For The Intelligent Organization: The Art Of Scanning The Environment.* Information Today Inc.

Clark, K., Dawkins, J. And Hale, J., 2005. Security Risk Metrics: Fusing Enterprise Objectives And Vulnerabilities, *Information Assurance Workshop, 2005. Iaw'05. Proceedings From The Sixth Annual Ieee Smc* 2005, Ieee, Pp. 388-393.

Cost Information Assurance, 2002. The National Center For Manufacturing Sciences, University Of Michigan Tauber Manufacturing Institute.

Dmcker, P., 1993. Post-Capitalist Society.

Haag, S., Cummings, M. And Dawkins, J., 2004. Management Information Systems. *Multimedia Systems,* 279, Pp. 280,297-298.

Jones, A. And Ashenden, D., 2005. *Risk Management For Computer Security: Protecting Your Network And Information Assets.* Butterworth-Heinemann.

Kadam, A., 2002. Writing An Information Security Policy. *Network Magazine.Indian Express Group, Mumbai, India,* .

Lester, B., Postlewaite, A. And Wright, R., 2008. Information, Liquidity And Asset Prices. *Pier Working Paper Archive,* .

Michael E. Whitman And Herbert J. Mattord, 2008. Management Of Information Security. *Kennesaw State University Course Technology Cengage Learning,* Second Edition.

Oppenheim, C., Stenson, J. And Wilson, R.M.S., 2003. The Attributes Of Information As An Asset. *Advances In Library Administration And Organization,* 20, Pp. 123-147.

Orlowski, S., 2001. Information Management: Protecting Critical Information Assets. *Computer Law & Security Review,* 17(3), Pp. 182-185.

Saint-Germain, R., 2005. Information Security Management Best Practice Based On Iso/Iec 17799. *Information Management Journal,* 39(4), Pp. 60-66.

Uhl, W., Warshaw, A., Imrie, C., Bassi, C., Mckay, C.J., Lankisch, P.G., Carter, R., Di Magno, E., Banks, P.A. And Whitcomb, D.C., 2002. Iap Guidelines For The Surgical Management Of Acute Pancreatitis. *Pancreatology,* 2(6), Pp. 565-573.

Whisenant, J.L., 2009. *Extending A Database Recovery Point At A Disaster Recovery Site.*

Wishes From Sigma, B., 2002. Eu Accession On Course. *Newsletter,* , Pp. 2.


*******