Security Consideration in Information Management of Organization

Dr. Orok B. Arrey[1]

[1] Federal Unversity Wukari Taraba State Nigeria.

Received: 12 December 2013 Accepted: 3 January 2014 Published: 15 January 2014

Abstract

Information has become today the life-wire of every organization having the potential of determining the success or failure of the organization, irrespective of size. More so, it has become so valuable an as as assets which is constantly under threat of attack by modern technology. There is need for proper management information, for maximum 'utilization and benefit this paper thus discusses the security in information management, especially in corporate organizations. The operational environment of institution)' and organizations has become highly competitive, with each actor aiming at outsmarting others. Only enhanced knowledge of security, with its full implications understood would help any organizations to survive the competition and not washed out.

Index terms—

1 Introduction

n the past few decades, there have been some breakthrough in science and technology, which have greatly revolutionized communication. The scientific and technological revolutions in communication have transformed every facet of the business world in particular and impacted seriously on the society, in general. Today, the complexion, quality, quantity and role of information in human society as well as its effective dissemination no doubt have greatly changed.

Nearly in all epoch and civilization, the important role of information as a vehicle of peace, of war, commerce, within the family, village, or among villages and other groups, had long been understood and appreciated. It has developed from the face-to-face and person-to-person transmission or information to breath-taking level or sophistication collapsing the widewide world into a global village with easily accessible communities. Event that have serious implication on the human society happen in any part of the world, and are seen at the same time. The war on terror, operation desert storm, the capture of Saddarn Hussein, earthquakes and the dismantling of the twin towers in New York, all were seen as they happened.

Earlier the ancient Persians were said to have built towers or call posts on which they placed men with shrill, loud voices to relay messages by shouting from one tower to the next. The Romans themselves operated an extensive messenger service called the 'CURSUS PUBLICUS.' In all these, there was neither privacy nor security about whatever information that was shouted from the towers or transmitted by those who operated the Cursus Publicus.

So much has changed and the society has developed to appreciate the need to control and protect information, Today there arc personal identifying numbers for bank accounts, computers and cell phones. All these are geared towards the protection of stored information. In this regard, Toffler, A, (1980:49), has observed that: ... While face-to-face information exchange was open to all, the newer system: used for carrying information beyond the confines of family or village were essentially closed and used for politico! control. They were, in effect, weapons of elite.

In the above statement, Toffler has defined the new information environment and pointed to the need to protect and secure information, which today has become a weapon in the hands of the possessor. That the elite uses it as a strong weapon for social and political control does not come as a surprise to anyone who realizes that the elite desires always to live above the society, Organizations must always recognize their operating environment and be quick in noticing the changes their environment is undergoing. This appears to be the key that unlocks the wings of any organization to soar far above the nebulous and highly competitive clouds of business and aspire to succeed. The old chips characterized by unrestricted openness must be thrown out and the new system, which is closed to, unauthorized access firmly introduced. This imposes great responsibilities on the managers of these organizations, especially and every other staff of the organization. This is so, because the environment in which many managers operate is fundamentally different from that of a few years ago as clearly illustrated above. Now there exists the potential for serious damage to the well being of the organization for which they have a responsibility. This danger arises from the nature and importance of information processing and communication systems in today's organization security outfit for the protection of the information bank in the light of the threats and vulnerabilities of their system. Common criminals terrorists and even military interventions succeed, depending on the information available to them. Unprotected bank of information For the survival of the organization, an efficient security system is a sine qua non. Security is indeed a people problem as. ”Computers don't steal, but people do.” We could use Langley 's definition of data security to give a dimension to, as well as explain the importance of information security as Langley (1989:1) defines information security as ?the protection of data from accidental or malicious modifications, destruction, or disclosure: it is the science and study of methods of protecting data in computer and unauthorized disclosures, transfer delay, modifications or destruction, whether accidental or intentional.

Here, we observed that the very idea of disclosure, transfer delay, modification or even destruction are the actions of persons. It is in the light or this understanding that it has become very necessary to pay more than lip service to security management of corporate information. What is the role of the personnel in this? What implication would insecure information of an organization have on the image and integrity or such an organization; and how does that affect the staff. What must be done?

The interest in information security had come as a result of several factors. In the first instance, information has become a very valuable asset of every organization, which, like most other assets, is the target or intruders. The cost or building an info-bank upon which the organization depends is today very high, and not securing this vital asset will mean wasting much resources as well as destroying the integrity and credibility of the organization. For instance, the secret of the success of a company like coca-cola is its ability in firmly securing and protecting the information regarding its production, whatever forms the concentrate and in what percentage and combination, and secret not only to the outside world, but to most staff of the company.

The composition in this area of business is so high that any unauthorized disclosure of transfer of this information” is able to seriously under-cut coca-cola. The point emphasized here is not particular with cocacola rather to every institution and organization that hopes to last very long as a business. The point has been corroborated by Caelli, Langley and Shain in their very interesting book, Information Security for Managers. The trio believes that the importance of information systems, which has made them to become very valuable to their users, has by the same token. ?become consequent more attractive targets for criminal and terrorists groups holding the possibility of high rewards from minimal effort and with little chance of detection until it is too late. This point is even better appreciated when it is realized that by simply compromising or disclosing a password, a major fraud running into several millions of naira, involving electronic funds transfer will have been successfully executed. Most banks and other corporate organizations have gone under water and tagged ”distressed” through the careless handling of their information system. There is espionage in nearly every area, of human endeavour. Academic records in Universities have become very juicy targets of cultists and some staff who are ready to compromise their job. Certain recent developments in information technology dictate that matters of information security should be considered priority area by organizations. 'These include among others:

i. The replacement of paper-based processing by main frame computer,

ii. The integration of organization files into data base: and iii. The development of complex, real time information processing system with highly volatile and valuable data.

These developments do not require much explanation since we know that manual information processing has a high level of redundancy and associated safeguards. All those clerks in charge of a process like invoicing would be aware of normal suppliers and be likely to recognize, suspect documents, or significant variations from usual patterns. However, these days, when once the secret information is accessed, documents or sets of documents that are identical to the one held by the organization, and hard to detect as fake will be produced from any street corner.

Database can readily provide unauthorized users with access to integrate information that would be difficult to obtain from a variety of computer files held by different departments.

The speed at which information is relayed especially in international trading and money transfer is amazing. This makes such delays or even errors that in previous systems, which could have been managed without much-loss or damage to assume disastrous consequences in the present environment and system.

The reason for this is simple. Such information asset developed by an organization over a period of time could have a corresponding value to a rival competitor, which would eventually affect the continued existence of the organization that first built up this information asset. It is in this respect that Alvan Toffler (1980: 172) explains the importance of security in organizations as he highlights the role of spies. He says:

For the spy's basic business is information and information has become perhaps the world's fastest growing and most important business. The spy is a Year ( )1 2014

living symbol of the revolution now seeping the infosphere.

It is readily acceptable that the information really has become the world's fastest growing and most important business as pointed out above by Toff1er.

Information is money and money information, one would say. Caelli, Langley and Shain suggest that:

2 In the financial world, money and information can be almost synonymous. The exchange of financial assets as achieved not only by the physical transfer of billions or paper currency by the exchange of messages over data communication on links?

If anything happens with the information to the sent out, or the communication links, unauthorized by the organization, then it is possible that the entire system would be messed up to the disadvantage of the organization. Here again lies the need for security of information.

3 II.

4 Security Considerations in Information Management

The very high level of computerization and the sophistication in communication gadgets and cryptographic system in use currently would have ensured maximum information security. However, these have increased the risks and urgently call for security. The management apart from formulating and religiously implementing security policy should also get every staff of the organization to be aware of his/her responsibilities in security matters. It is not only the organization that suffers, the individual members also suffer, when the organization's integrity is violated and as a result It, its business fortunes begin to nose dive. Even when the individual leaves to join another organization, surely he/she has following him a trail of negative reputation acquired. Information security is organizational thing and not something that effects a section of the organization. Security thus becomes a swimming together and drowning together affair in which the survival of the organization becomes the survival of every member of staff. Every staff becomes a stakeholder.

5 III.

6 Separation of Duties

Even when such orientation has been given to the staff, there is the need also to separate duties so that there are not concentrated in one person or group of persons. If this is overlooked" the chances are indeed high that an outside attacker could easily penetrate the organization by buying over the person in whose hands these functions are concentrated.

Similarly, they could infiltrate the small group and steal whatever information they are interested in. It could not be put differently in this way, that those with expertise be separated limn those who man the operations. All those staff with expertise to affect operations should be prevented from doing so. In the same way operations staff should not have assess to the knowledge or expertise necessary to modify system. It is important that knowledge of security controls should be restricted to a need-to-know basis.

IV.

7 Staff Recruitment and Security

Still at the point of recruiting a staff, the organization could send the prospective staff for psychological testing. Such tests have been known to reveal the social attitude, party affiliations and general stability of the prospective staff.

Finally, when a staff is terminated, there should be changes effected in the secret codes and other security combinations, which the stair was aware of before he was terminated It is necessary also to protect the computers and other communication gadgets very well. It should be the responsibility of a senior member of staff to control the entry into the computer rooms as well as authenticate every information going out or those coming in.

V.

8 Conclusion

Information is the live wire of any organization and requires adequate protection since it is a major asset of the organization. We have discussed above certain developments, which while transforming and revolutionizing the info-sphere have imposed in organization information managers a high security responsibility. Notwithstanding the sophistication in information technology in the use of a secret passwords, codes and cryptographic systems, there have been leakages, unauthorized disclosures, modifications, etc., which have had tremendous consequences on these organizations and their staff. If some of these controls are brought to bear in the functions of such organizations as West African Examinations Council (WAEC), Independent National Electoral Commission (INEC), Examinations and Records Departments in the Universities, etc, the scandalous leakages of classified information, alteration of figures ere would be controlled at least. Information security would not deal with the communication gadgets alone, but the staff too, from recruitment through management to retirement or termination. The character of the staff is indeed a major factor in the security of the institution. However, this too rests by and large on the attitude of management to the stall the incentives available as well as what training programmes or facilities available to staff. The organization must be ready to pay its staff very well. AII these may be done and yet without success if there is no security Policy or if the information to protect is not clear or protectable. It will then be useless These are very interesting steps to take in information security, but they require a dynamic and non-compromising management team to work. Over dependence also on a few key computing personnel without adequate supervision is more risky and should not be allowed, it must be noted that the image and reputation of any organization arc on the line and suffer great damage if the organization lacks information security. [1] [2] [3]

[1] ( )© 2014 Global Journals Inc. (US)

[2] © 2014 Global Journals Inc. (US) surrounding a rotten egg with cotton wool, the goal of information security is primarily to check occurrences outside system specifications. If this happens, then it must be promptly discovered and the source too, detected, with a view to preventing similar future occurrences.

[3] Global Journal of Management and Business Research A Volume XIV Issue III Version I Year ( ) © 2014 Global Journals Inc. (US)

[Danziger et al.] , James N Danziger , Kenneth L Kraemer , Deborah E Dunkle .

[West ()] *Churchman, the Systems Approach*, C West . 1968. N. Y. Dell.

[John Lesile] ‘Enhancing the Quality of Computer Services: Technology, Structure and People’. King John Lesile . *Public Administration Review* p. 53.

[Langley and Caelli Shain (ed.) ()] D Langley . */ormation Securityfor lvfanagers*, Langley Caelli, M Shain (ed.) 1989. Stockton Press Ltd. (Data Security)

[Rhae ()] *Office Automation in Social Perspective Oxford: Basil Blackwell*, H A Rhae . 1968.

[Bogusjaw ()] *The New Utopains: A Study of Systems Design and Social Change, Englewood Cliffs, 1’1 . .I*, Robert Bogusjaw . 1965. Prentice Hall.

[Toffler ()] A Toffler . *The Third Wave*, 1980. William Morrow and Company Inc. N. Y.