Practical security principles

Government agencies and private businesses, both domestic and foreign are becoming more dependent on information and technology to satisfy their several basic functions. Despite these reasons, the advancement to digital economy has led to information and information technology turning into a business asset that is valuable and therefore needs to be protected. It has come to recognition with this development that achieving these basic functions needs a well designed, a comprehensive course matter and information system programs for security that is reliable.

Programs of information system guidance, standards and strategies of implementation are being or have been developed by private and public organization sectors. These efforts which are widely ranging have been made to meet several aspects of information security. In seeking to guide and support these several efforts, the public and private organizations have come up with a number of implicit and explicit security principles concerning the information system of the organization.

There is a great potential in these security principles to become users', engineers' and the designers' canon to be considered during the designing of the programs for information system security (Wood, Smith, 2005, p. 23). Practically, to establish any information infrastructure security principles, one should first identify the person responsible for the information security. The organization should analyse the possible threats to its newly established information assets which it may encounter from the threat agents.

The vulnerability of the assets must be identified and analyzed on how it might be exploited. The organization must ensure regular reviews and

assessments as a security policy that makes sure that the information of the organization is well protected. The major duties of information security are achieved from the organization levels that are lower and moving upward. This is an approach that is referred to as bottom-up approach. The benefit that arises from the use of this approach is that the employees at the bottom level have got the technical expertise that enables them to know how information is secured.

Another approach that can be used in an organization to ensure security for information infrastructure in an organization is the top-down approach. This kind of approach begins with the organizational level that is higher and does its way downward. A security plan that has been initiated by those managers at the top level contains the backing that ensures that the plan works well. The chief information security officer in this case assists in the development of the security plan and makes sure that it is carried out well. Human firewall can also be used as an approach to ensure information infrastructure security.

This one ensures security by describing the enforcing role of security to every employee (Wood, Smith, 2005, p. 27). Before the application of the practical security principles, an organization should first understand the security principles. This can be achieved through knowing the avenues with which the information can be attacked. Some of the ways through which the information security can be threatened are; crackers which can establish distributed denial of service attacks via the internet; social engineering that can be used by the spies, guessing of other users’ passwords by the employees and through back doors created by the hackers.

Thus, for an organization to provide strong and well established security to its information infrastructure, it must therefore adopt defense mechanisms. These mechanisms will protect the information infrastructures in the organization against the above possible causes of information threat. It is in this case where the organization should apply the practical security principles. Such practical security principle includes the following. Firstly, is the layering.

This kind of approach or principle has the benefit to the organization in that it creates multiple defenses barrier that can easily coordinate several types of attacks that are likely to be of threat to the organization information. In the same way, the information security must be made inform of layers. These layers that are created must be coordinated properly so as to be effective (Wood, Smith, 2005, p. 34). Secondly, is the limiting practical security principle. In this case, what the organization can do to secure its information is to limit the access to its information.

The access should be allowed to the individuals who must use the data, that is, the staff members and other stakeholders to the organization. The limitation to the access should be done for a subject that is in a computer running program on the system or a person credible to have an interaction with an object in form of a stored database on a server or a computer. The granted amount of access to someone must have limitations to the requirements of doing or knowing that person. Thirdly, is the diversity. This type of practical security principle is closely related to that one of the layering.

Diverse security layers should be used to protect the data in an organization such that if one layer is penetrated by the attackers, the similar technique they have used to penetrate that one layer cannot be used to pass through the other layers. In this situation where diverse layers are applied as mechanism for defense, it implies that when one security layer is breached, the whole system is not compromised. To filter a specific traffic type, a firewall can be established and on the same system, a second firewall can also be set to filter another type of traffic.

A greater diversity can even be created by vendors that are differently produced by the use of different firewalls. The fourth practical security principle is that of obscurity. Obscuring what moves inside an organization or a system and avoiding behavior pattern that is clear makes it difficult for attacks from outside (Wood, Smith, 2005, p. 54). The last and not the least security principle is that of simplicity. It is hard to comprehend security system that is complex, feel secure about it and troubleshoot it.

Making the system simple in this case is the greatest challenge from the inside but a challenge from outside. Behind the five basic practical security principles it is also vital for an organization to consider other factors that can ensure the infrastructure security of the information. The organization should ensure that it uses the effective authentication methods. In this case, there are three major pillars unto which the information security rests. They include the access control, authentication, and auditing. Authentication here means the process of giving identity.

This one can be categorized into three major classes, that is, the password or the personal identification number, an identification device or smart card and finger print. Giving unique secret password and the username to the information system user is a common method for ensuring security to most data and information in several organizations. It has been evidenced that password authentication protocol does not provide true security to information infrastructures. The Password and the username values are checked and clear text for a match to the server.

The user in this case is granted the access if they match. In many implementations of the modern times, the password authentication protocol favors more methods of authentication in information security (Wood, Smith, 2005, p. 41). An organization can use another protocol known as challenge handshake authentication protocol. This kind of protocol has been considered by many organizations as a more lucrative procedure to offer security for the connection of a system instead of using passwords. In this case, the password is entered by the user in which he connects it to the server.

The server will then send challenging massages to the different users' computers. The probable response is then checked by the server by doing the comparison of the calculation of its own on the value that is expected. The authentication will the therefore be accepted if there is a matching of the values, otherwise, there will be a termination of the connection. Any organization can also use tokens to provide security for its information infrastructure and the systems. Token in this case is a device that by been

embedded to the token itself and with permission for the information that is appropriate, authenticates the user.

This kind of security has a common similarity with the certificates. Token contains access and the right privileges of the bearer of the token as the token part. Since the password is based on what one knows, the tokens in this case are based on what one has. To sum up, there it is advisable for an organization to make use of the practical security principles together with other security measures so as to ensure adequate and efficient security provision to its information infrastructures and information systems.