УДК 004.056:811.111

Kubarskiy M., Borodin A., Bankovskaya I.

Importance of Information Security in Organizations

Belarusian National Technical University
Minsk, Belarus

Information is one of the most important organization assets. For an organization, information is valuable and should be appropriately protected. Security is to combine systems, operations and internal controls to ensure integrity and confidentiality of data and operation procedures in an organization. Information security history begins with the history of computer security. It started around year 1980. In 1980, the use of computers has concentrated on computer centers, where the implementation of a computer security focuses on securing physical computing infrastructure that is highly effective organization. Although the openness of the Internet enabled businesses to adopt quickly its technology ecosystem, it also proved to be a great weakness from an information security perspective. The system's original purpose as a means of collaboration between groups of trusted colleagues is no longer practical because the usage has expanded into millions of frequently anonymous users. Numerous security incidents related to viruses, worms, and other malicious software have occurred since the Morris Worm, which was the first and shut down 10% of the systems on the Internet in 1988. These incidents have become increasingly complex and costly. However, the information security awareness has been increases. Many organizations have implemented the information security to protect their data.

In general, information security can be defined as the protection of data that owned by an organization or individual from threats and or risk. According to Merriam-Webster Dictionary, security in general is the quality or state of being secure, that is, to be free from harm.

Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure.

The information security performs four important functions for an organization which is enables the safe operation of application implemented on the organization's Information Technology (IT) systems, protect the data the organizations collects and use, safeguards the technology assets in use at the organization and lastly is protect the organization's ability to function.

There are five theories that determine approach to information safety management in organization:

- *Security policy theory*

Aims to create implement and maintain an organization's information security needs through security policies.

- *Risk management theory*

Evaluates and analyzes the threats and vulnerabilities in an organization's information assets. It also includes the establishment and implementation of control measures and procedures to minimize risk.

- *Control and audit theory*

Suggest that organization need establish control systems (in a form of security strategy and standard) with periodic auditing to measure the performance of control.

- *Management system theory*

Establishes and maintains a documented information security management system. This will include information security policies that combine internal and external factors to

the organization that scope to the policy, risk management and implementation process.

- *Contingency theory*

Information security is a part of contingency management to prevent, detect and respond to threats and weaknesses capabilities of internal and external to the organization.

Employees should know their boundaries. They should know to differentiate their personal life and their job. They should not taking advantages by used company facilities for their personal. This is because they can encourage the threat attack and makes the organizations' information is in risk. Organization should explain about this to the staff to let the staff know what they can and cannot. The employees should be explained about the rules and ethics in the workplaces before they start their works. The organization should establish, implement and maintenance the policies about the information security. This is to ensure the employees follow the rules to access to the information. In order to increase the awareness on security issues among the employees, the organization should take several steps to improve the employees' awareness and understanding on the important information security. Method that could be taken by the organization is by give education to their employees about the protection of data and gives the training to the staff about the way to protect the data. By implement these methods, the employees can have better understanding about information security and also can protect the information well. Employees must understand and accept the risks that come with using technology and the Internet in particular.

The employees and organizations' personnel must ensure that the organizations computer network is securely configured and actively managed against known threats. IT network professional also should help organization maintain a secure

virtual environment by reviewing all computer assets and determining a plan for preventive maintenance. This includes routinely cleaning up unnecessary or unsafe programs and software, applying security patches such as small pieces of software designed to improve computer security, and performing routine scans to check for intrusions. Organization also may review access rights and have the IT professional set up an automated procedure that requires the employees to change their passwords at regular intervals to further protection organization information assets. Besides that, the computer system should install updated and latest protected program such as the updated antivirus to protect the computer from viruses attacks. To protect and secure the confidential information well, the organization should hiring the IT experts and employees that have the right qualification to protect the data. This is to ensure the employee know what to do if problem occurs and to protect the data as well. Besides that, the IT expert or the qualification staff have better understanding of information security and know the steps to ensure the information is always keeping safely. When employees is lack of information security knowledge in term of keeping their information, the organization is easy to be attacked by hackers or another threats that try to stole or get the organization confidential information [1].

In conclusion we may summarize that it is crucial and important to all staff in an organization to have knowledge and understanding about the importance information security practice in an organization to protect the confidential data.

References:

1. Mode of access: https://www.uniassignment.com/essay-samples/information-technology.php. – Date of access: 07.03.2018.