Aaron Young

Professor Boman

Cybersecurity

11-14-2021

Cybersecurity.

1. **Costs incurred in developing cybersecurity programs in business.**

Cyber security is one of the significant issues in today's technological world. The world is experiencing a transition that has done away with the physical storage of files and other forms of data. Information is today stored in the cloud storage spaces and the computer. The computer is easy to save and store data, and storage and space are reserved. However, cyberspace is prone to a lot of threats (Paulsen &Patricia, pp2). Security, data loss, and exposure all affect cyberspaces. Therefore, programs should be put in place to enhance cybersecurity.

Many organizations and businesses have implemented cybersecurity programs to secure data in computers. There are several costs incurred and benefits accrued from this initiative. The first is that the price of cyber security is very high. High costs are because businesses need to have software and hardware inputs for the process to be complete. Software programs are required to convert the data into storable formats. The software programs are costly, and some businesses may lack adequate resources to purchase them. Therefore, small businesses should adopt professional personnel to manage their computerized data from exposure, modification, and loss.

Benefits of business adopting cybersecurity programs.

The benefits achieved from implementing computer security are many. For instance, cyber storage is more secure as compared to physical storage mechanisms. Computers usually require one to have two-factor authentication or passwords to access vital information. This security

mechanism makes it hard for unauthorized persons to have access to them. Also, cloud storage, a form of storage in computers in the virtual, scalable space, provides the storage of large amounts of data. Cloud storage makes cyber security safe for the storage of very confidential data. When businesses develop cybersecurity programs, they will incur minimal costs in employing personnel to track lost or exposed data.

2. How to tell if your computer is safe.

A person, or rather, a computer user, can tell if his computer is safe using specific criteria. A person can look at the storage means used in storing their data. Keeping data in computers on the desktop is very risky. Placing at the desktop is dangerous because it is easy for another person to see these folders from afar. They can notice important file names and open them without the owner's permission. In the process, important information is lost and exposed. Data exposure leaves the user or organization at risk of cyber insecurity.

You can also tell if the computer is safe if it has locks. For example, passwords and biometric identifications are used to unlock computers. The presence of such looks implies that third parties are locked away from accessing some data. Locks leave only the machine owner to access them (Manyika., et al, pp0360-8581). However, if the computer lacks such locks, then it is not safe. The lack of encryption mechanisms exposes the machine to many user access and possible computer theft.

Someone can know if a computer is benign by observing the number of users present in the machine. Many computer users make the laptop unsafe to store essential data files. The less security is because many users translate to more exposure and possible loss of data. However, if the computer user is only one, then less exposure is placed on it.

References.

Manyika, James, and Charles Roxburgh. "The great transformer: The impact of the Internet on economic growth and prosperity." *McKinsey Global Institute* 1 (2011): 0360-8581.

Paulsen, Celia, and Patricia Toth. *Small business information security: The fundamentals*. No. NIST Internal or Interagency Report (NISTIR) 7621 Rev. 1. National Institute of Standards and Technology, 2016.