Pros And Cons, And General Concept Of Cyber Security

· Abstract:

In this task we will present many important aspects. First, I will learn about the general concept of cyber security, which is one of the broad concepts, in addition to the pros and cons of cyber security. Then, I will sweat the general realities involved, then, I will identify a variety of recommendations related to cyber security.

· Introduction:

Technology is an important source all over the world, and is the active source of our daily business. In addition, different people are using technology for a variety of sources. For example, some are used to know the news of events and developments in the world, and we see some use technology to end business, and we see some use technology for shopping, study and other things. In addition to the above, technology is witnessing rapid and frightening developments that in turn require high security means in the present day. moreover, Technology is also an integral part in many different aspects, for example the use of technology in facilitating communication or retention of different and multiple information. In addition to the above. There are many ways of working to secure data and software from the various factors of our time. We are in dire need of security steps to preserve the contents of our privacy, whether as individuals or organizations. Moreover, most people rely on technology on a large scale, as evidenced by their heavy reliance on important parts and processes through technology. There are also many activities that do not allow us to use different methods, because technology is one of the most widespread and used methods.

· Discussion:

· Cyber security:

Cyber security is defined as a branch of technology long known as information security, so it has been applied to different networks and computers. In addition, there are several goals in cyber security, for example, to protect property and various information from piracy, disaster , corruption and theft. It is also known as the process and the basic pillar that protects sensitive services and valuable information, from other unauthorized factors for the use of that information or property.(Schatz, Daniel; Bashroush, Rabih; Wall, Julie ,2017)

· History of Cyber Security:

The first computer virus was established in 1988, in the early seventies of the last century, these viruses are one of the first computer worm to gain high attention from the media, so after that, these viruses developed and spread widely, which became one of the harmful and complex attacks. So many attacks have appeared in different forms through the virus. Thus, cyber attacks occurred in a very rapid development in the last quarter of the last century, so the breakthroughs by secondary students emerged. Therefore, there are emerging ways to protect

and combat attacks or security problems such as cyber security.

· Advantages of cyber security

Cyber security has many different advantages that are important to different individuals or organizations. Therefore, they provide effective means in the important aspects, the first force that works to achieve security care for the various actors. So one of the most important pros of cyber security: It is the main and important source that provides comprehensive protection against harmful and offensive viruses. It also provides great protection for spyware, hacking programs or various programs that harm the privacy or data. Therefore, it takes strong steps in the knowledge, treatment and protection of various phenomena suffered by owners of organizations or individuals. Also, Provides effective and robust protection against data theft, because sometimes there are many private data theft for the purpose of threat or other things. So it shows the implementation of the security protocol, which is defined as a means that focuses on breaking all theft by different people by breaking the process and rejecting it through the application. moreover, It is characterized by the protection of all systems, applications and computers from the phenomenon that dates back to previous years known as piracy, so we find that it works to protect against this phenomenon with a high degree of concentration through the application of protection for all systems and system for computers. Therefore, it is one of the broadest means of security in protecting important systems and applications from hacking. However, it works to provide a huge amount of privacy for the system and data, through the implementation of good policies, for example, such as the policy of security protocols in systems or network (Risen, Tom 5 June 2015).

· Negatives Cyber security:

Despite the advantages of cyber security, there appear to be some downsides that contribute to important data or other losses. So we will present some of the negative axes: Is a costly and well-known means of high price for ordinary users. Therefore, we find that cost is a negative factor that prevents individuals from applying them. There is a lot of slow in the systems that are possessed, so we find the slow form means a barrier for users, which will lead to a large loss. Also, Updates new software to the security hub, which may cause errors such as data deletion or the like. (Palilery, Jose (24 December 2014).

· Facts:

Hackers attack appears, every 39 seconds The (University of Maryland's Clark School) is one of the first studies to determine the overall rate of hacker attacks on various electronic devices such as an Internet-connected computer. So every 39 seconds of hacker attacks appear and affect one in four Americans every year - so general hacker attacks reach users with unsafe accounts. (Bart Elias 18 June 2015). Also, in 2021, total spending for cyber security is expected to be around $ 6 trillion for the world level, most modern or old organizations need comprehensive data security measures and approaches and a complete rearrangement of budgets to keep pace with events. Moreover, About 95.11% of total cyber security violations resulting from human errors Attackers exploit hackers, cyber criminals for organizations' vulnerabilities and simple mistakes for large or small organizations to take profits or infringe on the organization's public privacy. However, more than 77% of different global institutions have no plans or strategy for cyber security incidents, it is estimated that approximately 54% of the

various organizations have been continuously attacked and violated the privacy of data and information, and have been attacked in more than the past eleven months.

· Recommendations

There are many recommendations included in cyber security, the most important of which is the installation of programs that maintain the security and general protection of electronic devices from viruses. Also, stay away from connecting to unknown wireless networks, thus avoiding people accessing your device or taking your public data. In addition, the overall security of your device or portable electronic devices means that no one can take information or sneak into your private data. Additionally, respond to unknown emails only after confirming. So to avoid being threatened by online scammers or hackers. In addition to the above, keep away from personal mistakes to a great extent, so as not to show a chance to cyberattacks. In addition, the authorized and legal programs should be downloaded in various electronic means, so as not to be vulnerable to modern attacks. In addition, the general avoidance of downloading data or privacy to multiple computers or devices, so that there is no indication of attackers or hackers or thefts that occur by multiple people.

· Conclusion:

Cyber security is one of the means or software that gives enormous security power to computers or electronic devices that protect data from many hacking factors, cyber attacks or thefts. Therefore, there are many advantages that characterize this process, the most important of which is the wide protection of different organizations or privacy. In addition to the above, although there are positive axes, we find that there are also negative aspects, for example, the cost of ordinary and slow people. Also, there are many known scientific facts of cyber security. In addition, cyber security has broad recommendations to avoid factors that may affect data, privacy, etc.

· References:

1. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). 'Towards a More Representative Definition of Cyber Security'. Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.
2. Palilery, Jose (24 December 2014). 'What caused Sony hack: What we know now'. CNN Money. Archived from the original on 4 January 2015. Retrieved 4 January 2015.
3. James Cook (16 December 2014). 'Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far'. Business Insider. Archived from the original on 17 December 2014. Retrieved 18 December 2014.
4. Risen, Tom (5 June 2015). 'China Suspected in Theft of Federal Employee Records'. US News & World Report. Archived from the original on 6 June 2015.
5. Bart Elias (18 June 2015). 'Protecting Civil Aviation from Cyberattacks' (PDF). Archived (PDF) from the original on 17 October 2016. Retrieved 4 November 2016.
6. Clayton, Mark (7 March 2011). 'The new cyber arms race'. The Christian Science Monitor. Archived from the original on 16 April 2015. Retrieved 16 April 2015.
7. Treglia, J., & Delia, M. (2017). Cyber Security Inoculation. Presented at NYS Cyber Security Conference, Empire State Plaza Convention Center, Albany, NY, 3–4 June.