**IT Security and risk management**

**Dec 2020**

**1. A device or an application needed to track a network or system for malicious activities or violation of policies is known as Intrusion Detection System. Whereas, the testing that examines the security of an organization prior to an attack on the network by a hacker is known as penetration testing. What are the challenges and benefits of Intrusion detection system and penetration testing for an organization in their security? Also is it necessary to have both these strategies implemented in a single organization? Justify your opinion**.

**Answer**: **Role of data security in organizations**

Modern organisations are rich with data. Owing to large-scale computerisation efforts, almost all processes, activities, and interactions within the organisation are available in accessible databases. This rich data environment has spawned a variety of software applications that rely on the principles of decision support systems (DSS) and enable organisations to change their competitive strategy. Company has good amount of important data but there is no security in the company to keep that data secure and confidential. There should be proper information system in the company and that should be fully secured. Employees should have limited access to the data as per their designation and resp Its Half solved only

Buy full from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session December 2020,**

your**last date is 15th Dec 2020**.

Lowest price guarantee with quality.

Charges**INR 199 only per assignment.**For more information you can get via mail or Whats app also

Mail id is [aapkieducation@gmail.com](mailto:aapkieducation@gmail.com)

Our website www.aapkieducation.com

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

whatsapp no 8791490301.

* Contact no is +91 87-55555-879

**2. MSME companies over the last decade have invested in various cyber security detection and prevention policies. These include, corporate firewalls, antivirus, malware removal tools, and many others. In the current pandemic situation, all these investments which were done for providing security to specific locations (office space) have proved to be redundant. Majority of the workforce is working from home and hence a review of these investments is being undertaken in preparation for the new normal. Discuss the technologies and policies which would help organizations to meet the challenges of an increasingly distributed work environment. Kindly remember to factor in budgetary and other resource constraints which the MSME sector faces while making your recommendations**

**Answer**: The network structure can be either a centralised or a distributed type of network. In a centralised network, all the users are connected to a central server, and the server performs the activities required for communication. Then the user accounts and communication information are stored in this server. Almost all the instant messaging platform and the social networking sites use a centralised network, and this network is called the centralised server architecture. The distributed network, on the other hand, does not perform the functionality of a client-server architecture. In this type of network, all the facilities are spread over the network to different clients, and a

**3. Mrs. Sharma felt all was not well with her 79-year-old father who used to live alone in his hometown. When they talked on the phone, he would tell her about a woman he met online and occasionally sent money to via his mobile phone. Even though her father never met the woman in person, she had gained her father’s confidence through instant messaging and voice chats, she would ask him to send her money to feed her and her daughter. Mrs. Sharma told her father that he was being conned, but he would not listen and continued to send the woman money anyway. It was only after Mrs. Sharma went to her hometown to check on her father due to ill health that she realized the extent of the scam. She found numerous messages from the woman asking for money, including receipts from wire transfers on her father’s phone. After doing a little digging, Mrs. Sharma found that her father had sent the woman more than Rs. 9,00,000 over a course of two years; practically his life’s savings. Majority of these transaction were done by gaining access to her father’s provident fund account. The attacker had hacked the account using the private information gained through chat and voice messages. Unfortunately, this is not uncommon. According to research by the Stanford Center on Longevity and the Financial Industry Regulatory Authority’s Investor Education Foundation, those over the age of 65 are more likely to have lost money due to a financial scam than someone in their 40s.**

**a. Why are elderly frequent targets of cyber fraud? What tactics the fraudsters use to gain access to bank accounts of elderly?**

**b. What are the ways and measures to protect people especially seniors from such attacks?**

**Answer**: a) In the present era, it is tough to imagine anything that we do without involving the use of the Internet. We use the Internet for information exchange, business transactions, entertainment purposes, social networking, etc. However, the Internet is a double-edged sword. Along with a variety of benefits, it also has certain security threats associated with it.

**Why are the elderly frequent targets of cyber fraud?**

**Not tech savvy**: Most of the elderly individuals are not tech savvy, because of the trend and convenience, they perform some basic activities over the internet like funds transfer, bill payment, other banking activities etc. They do not know much about suspicious transactions or how hackers can steal the personal information with just one click. Due to lack of knowledge, they often click or reply on suspicious message or email and later suffer financially.

**Emotional factors**: