What kind of threats are there from using information technology

Technology

Originally, important paperwork and confidential documents were stored in locked file cabinets so that even if someone did gain access to the room where the files were maintained, their access would be limited to a lock. Thieves that wanted to retrieve the Information would need to break or bypass the lock to retrieve the Information. In information technology, a computer is used in place of a filing cabinet (although there are still a number of firms that rely on old technologies or combinations of the two).

Like the filing cabinet, the computer Is only able to give access to those who have a " key" or password. A computer can also have a secondary security system in which different users have different access limits. This is equivalent to only having certain people in the office having access to different information. Furthermore, files In the computer can be locked by a particular user which Is equivalent to locking a file In a filing cabinet which delays or prevents theft. At this point we discuss why a computerized information system is either more or less secure than traditional methods.

One of the primary Ideas behind computers Is that the computer key or password Is unique for each person or group and can be changed as often as necessary with no cost other than time. Changing a real lock, forever, is difficult because all of the keys for that lock must be changed which requires more time and of course money which Is not as effective for running a business. If a user loses a real key for a real lock, somebody else could pick it up and get access, but if a user loses a key or password, it can't fall into someone else's hands.

This is true provided that the user has not held a physical copy of their password (for example: written It down on a piece of paper). It Is at this point, that the user has 'damaged' the information system by creating a physical key like in the old system ether than remembering what the key looked like. We see here a fatal flaw and hence a threat in Information security: if users are not familiar enough with the new technology, then the system becomes worse rather than better. OFF main door's lock of the building, passwords should vary for different purposes such as computer user access and file access, however because of non-familiarity of the system, many users use the same password for all protection making it simple for a thief to steal information. To visualize this, consider a locked filing cabinet. Some of the files in that cabinet are inferential but the same lock is used as the one to open the cabinet. Does this make sense? Of course not.

If the thief can open the first lock, they can certainly open the second. One of the advantages of using an information system is that if the lock varies slightly in the physical case, the thief will likely access the information, however even the slightest change in a computer password can make the largest difference in security. So far I have been speaking about thieves of information, however information is not always stolen, it can be copied, sold, or even changed. Consider a criminal that has a rather extensive criminal record.

If they change records, they can change the sentences of friends in prison from life to 6 months or delete thousands of dollars worth of fees in parking tickets. This is a downside of a computerized information system. Unlike a physical file which can detect if any changes have been made and recognize the handwriting, a computer file does not have this advantage. The computer time and data can be changed to match the last edited date and the new information can be entered provided an adequate password is used to access the information to begin with.

Once again, we see the example of how access must be prevented to secure the information. In the above example, I spoke of a data record being changed. This is called a breach of data integrity or a false change in the true data. Another example of this kind of breach is simply removing a user or file completely from the system. This means that the user or file 'doesn't exist' and can cause the person to be fired from their Job or can cause a loss of customers in a business.

Consider a bank that 'loses' the account of a millionaire. Of course, sometimes the account may be deleted in a different sense. Consider a bank that 'loses' the account of someone massively in debt. In both of these cases the bank 'loses' and so must ensure that the data is kept secure. I have spoken in all of the above examples as though a person is directly responsible for the loss of the data, however this is not always the case. Other examples include fires, water damage, viruses, power surges and power failures and so on.

In fact, there are so many ways that the data could be damaged, its almost common sense to eve a backup of the data with almost the same level of security. Backing up the data is the best way of recovering the data and so even if the 'working' data is destroyed, the actual data damage is more or less prevented. I say more or less because it wouldn't make sense to back up the entire system every time a new file is created or a file is edited. Technologies including laptops or other computers to backup the data whereas others continue to use filing cabinets at other locations.

Networking is also used so that data from several different sources is stored at a very secure location which is armorial where the server resides in a server-client relationship network. A network is not always the best solution when viruses are brought into the picture of security. Viruses, particularly worms which travel through networks and self-multiply, are incredibly dangerous which is why many firms prefer to store their data on removable media such as CD-ROOMS, non-networked computers and even filing cabinets as in the examples at the beginning of this essay.

While virus-scanners do what they can to prevent viruses, most virus prevention can only be 100% effective if he anti-virus update is released immediately after the virus itself. One of the last issues which I wish to address is not the internal threat. Many firms base an assumption that their staff will be smart, reliable, trustworthy and responsible which is a very poor assumption to make. How secure do you feel when you read out your surname and password to someone over the phone when you ring up an ISP (Internet Service Provider).

They could Just as easily be writing it down on paper to use in their own time without you even realizing! The same goes when oh use a credit card at a restaurant and various other forms of service. This brings me to my final point which is Internet Security. As I have already mentioned, giving your password to anyone is the most fatal flaw in computer security and so provided that different passwords are used, your system is relatively safe. Internet Security is no different. In fact, provided that the data you send over the internet is secured (and web pages tell you when it is and isn't), you will not come across any problems.

This is because even if someone intercepts the data being sent, he only way they can decode the data is if they know which kind of method was used to encrypt the data and even knowing that it is very likely impossibly without a quantum computer. Many internet security systems use public key cryptography which provides a large number, usually millions of digits long and this number if the product of two prime numbers. The computer can unscramble the data relatively quickly because it will be passed the two numbers, but the two numbers will not be passed to the interceptor of the message.

This will make the unscrambling process incredibly long and tedious and by the time the interceptor does know the message, it will most probably be useless to them. In this case, the means of preventing information from being received by a third party is by using encryption security. Encryption security is also used to protect unregistered software from being used past a 30-day trial period for example. Despite these various threats in information technology, it is still more advanced than primitive information technologies and provided that it is understood and used correctly, all threats can be prevented.