Research Paper
Impact Factor: 6.089
Peer Reviewed Monthly Journal
www.ijmdrr.com

Special Issue

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

THE CASE STUDY ON CYBER SECURITY

Sruthi.C*   N.Nivetha *
**M.Com,St Joseph's College for Women, Tirupur.*

Abstract

Cyber security plays an important role in the field of Information Technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is "cyber crimes" and increasing immensely day by day. Various governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Introduction

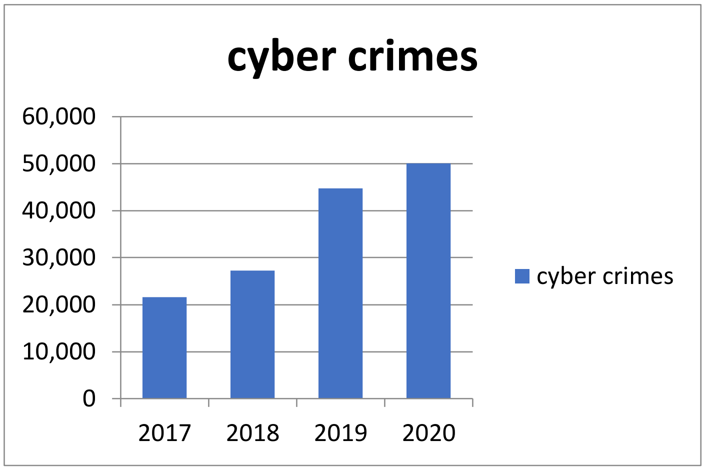
Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence on these days, cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

2. Cyber Crime

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cybercrime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

Cyber Security

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.



Case 1:

A hacker has allegedly leaked customer data of pizza brand Domino's, according to information shared by a cyber security expert. The company has admitted to the data breach, but said customers' financial information remains safe. As per cyber security researcher Rajshekhar Rajaharia, people who have access to a portal developed by the hacker are using it to spy on customers by checking their location along with order date and time. "Data of 18 crore orders of Domino's India have become public. Hacker created a search engine on Dark Web. If you have ever ordered @dominos India online, your data might be leaked. Data include Name, Email, Mobile, GPS Location etc," Rajaharia tweeted. When contacted, Jubilant Food works, which owns Domino's, said the company had recently experienced a security incident but no financial details of customers have been breached. "Jubilant Food works experienced an information security incident recently. No data pertaining to financial information of any person was accessed and the incident has not resulted in any operational or business impact. "As a policy we do not store financial details or credit card data of our customers, thus no such information has been compromised. Our team of experts is investigating the matter and we have taken necessary actions to contain the incident," the company spokesperson said. Rajaharia said the hacker has created a search engine for the database which is being misused by people. The worst part of this alleged breach is that people are using this data to spy on people. Anybody can easily search any mobile number and can check a person's past locations with date and time. This seems like a real threat to our privacy," Rajaharia said.

Alternate solutions:

- Domino’s should always updates their websites so they can find any bugs in their website.
- After receiving the online order from the customer the recipient, can call them for the confirmation.
- Most of the customers are fear to fail the amount through online, provide cash on delivery for those customers to retain.

Best solution:

- Domino’s should always updates their websites so they can find any bugs in their website

Case 2:

Cyber Attack on Cosmos Bank.

In August 2018, the Pune branch of Cosmos bank was drained of Rs 94 crores, in an extremely bold cyber attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and debit cards. The switching system i.e. the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred. According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out. This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

Alternate solutions:

Customer data must be regularly secured and backed up.

- Every employees should have a separate user account and with a policy that stipulates the changing of passwords every three months.
- Every banks must send out alerts and automatic messages to customers confirming the validity of a transaction.
- Customers must be provided with guidelines for checking the authenticity of any sources that are asking for account details.
- Customers must also be provided with guidelines for taking precautions while using the bank’s websites.
- Best solution: Every bank must send out alerts and automatic messages to customers confirming the validity of a transaction.

Conclusion

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.