Cyber Threat: Political, Socio-Cultural And Economic Perspectives

Cyber Threat

Currently, technology is one of the significant factors in business. Almost every organization relies on technology to perform most of its activities. Due to the advancement of technology, most businesses succeed as technology gives an organization a competitive advantage in the market. Since 20th century, many companies have realized the importance of technology and slowly, technology is becoming the backbone of almost every organization in the world. As they continue to take in more technology, new threats have risen which are related to technology. Today, the increase in cyber threats has been a major challenge to most of the organizations in the world. Cybercrime involves defacing a website and getting important information that leads to stealing valuable goods like money. Today the most affected organizations are the bank's institutions. They face cyber threats as technology has enabled young people to develop new software that is used to acquire information especially sensitive data like financial assets of their customers. People need to be advised on how to deal with such crimes as they are occasionally happening. Besides that, cyber threat is also connected to social, cultural, political, and economic factors that enhance the process to occur.

Political Perspectives

The political issue is a significant factor that motivates attacks. The factor involves government policies such as laws and regulations, politics and government development. Any cybercriminals involved in politically motivated attacks are mostly from members of extremist groups who take advantage of cyberspace to spread enmity and propaganda through attacking websites and networks of their political enemies. Through advanced technology, these people can steal money through cyber-crime, and the money is used to fund their activities or plan physical-world crime. The cyber threat is thus being used to fight an individual politically. Depending on the nature of the attack. Political attacks can be divided into two stages: Pro-tests against political issues and pro-tests against laws and public documents, and lastly against physical violence (Gandhi et al. 2011). The two stages are the leading cause of political cyber threat.

Pro-test against political issues involves attacking people politically, and the threat mostly happens during campaigns where politicians are engaged in a war. Those that are well advanced technologically are in a better position as they can spread propaganda concerning their political enemies thus fighting them politically. Also, a country can be attacked by another country due to its government actions. A good example was the India attack on atomic research in June 1998. Hackers known as “Milworm” from the United States, England, Netherlands, and New Zealand attacked the network of India’s atomic center claiming to protest against nuclear testing (Gandhi et al. 2011). The kind of attack was due to political issues as the other countries were not happy with India discovering the atomic nucleus.

Socio-Cultural Perspectives

Socio-cultural is another factor that contributes to a cyber-threat. Human beings tend to reason together in groups. There is a positive aspect as it helps to bring social cohesion among people. If people happen to thinks and behaves differently, social groups will not work well. In most cases, cyber-attacks are meant to destroy the relationship in a social group (Andrew, and Perlroth, 2012). The moment a social group experience the threats from cyber-attacks, the act will tend to bring some changes where the group will change its thinking. Thinking differently as a group will affect the group goals thus cyber threat becoming a major problem to people.

Also by defining socio-cultural conflict as a competition between people or groups over incompatible goals, power, and other essential resources, cyber threat can be used to interfere with the objectives of an individual or group of people. A good example of Cyber conflict on cultural reasons includes the conflicts between America and Russia. Today, the Russian government is actively engaged in effectively using cyber warfare that influences American culture thus creating a socio-cultural conflict between the two countries (Gandhi et al. 2011). The reason why Russian operatives are in a capacity to do this is that the country has sophisticated cyber warfare ability and they know that fear, intolerance, and anger divide the American people together with cultural and social aspects. Also, another advantage that Russian depend on is that Americans are known to believe in all outrageous propaganda especially to those countries they disagree with. A good example is when it was discovered that, Barrack Obama had unsuccessfully tried to turn over the U.S. government to China where the intention was to be the president for life (Andrew, and Perlroth, 2012). After thorough research concerning the issue, it was discovered that the information was not real but was in an article on the internet. The act proved how cyber threat affects people culture and way of life.

Economic Perspective

Most of the cyber threat that happens today is motivated by economic factor. Due to the fast-spreading of digitalization, more cyber threats have risen especially within the economy of a country. The impacts of these threats go beyond the damage to the properties of individual victims (Biancotti et al. 2017). Following the same track on the fast spread of technology, there is also a widespread perception of cyber insecurity that is used to slow the pace of technology thus facilitating the cyber threat which affects the trade hence hurting the productivity.

For many years, there has been damage to the automatic teller machine (ATM) in different countries. The increase of such cases has been due to the technical ability of fraudsters who use the technology to perform the damage stealing millions of money (Lis, and Mendel, 2019). ATMs have played a great role in giving an opportunity in stealing as the machines are computerized. Research carried out in the US shows that a bank experiences more fraud in their ATMs than when the client visits the bank (Biancotti et al. 2017). On economic perspective, cyber threat is mostly facilitated by poverty and advanced technology as those bring positive impact through new technology devices are the same that make the other devices that are used to acquire sensitive information.

Conclusion

Technology plays a vital role in business, but at the same time, technology remains the biggest threat in the business sector. New strategies need to be applied which will help stop cyber threats, and people be educated on how to protect their sensitive information such as financial

information as many fraudsters target those information to acquire money from banks account. Also how people relate remains to be important as social groups should stay focused on their goals despite the cyber threats that may cause them to think differently.