TECHNOLOGY, CRIMES AND ITS CHANGING PATTERNS

[1]Virgilio Mendes Fijamo, [2]Irene Adjovi Sokegbe
[1]Student, [2]Student
[1] Computer Science Department,
[1]Alakh Prakash Goyal Shimla University, Shimla, India.

Abstract : The world of technology keeps coming up with new innovations. From these new technologies, come new empowers to improve the daily experience by providing a computer system on growing ladder. Instead of making life easier, sometimes they are used for purposes that undermine human security. Against these crimes commit by using technology, new way to secure goods and human life are developed.

Talk about cybercrime today attracts a lot of looks, the internet has become one of the most vital part of our life from work to entertainment there is no other option now but comes with a price of our privacy.

The objective of this study is to explain in proper way the topic" technology, crimes and its changing patterns" and To focus on several crimes discovered in organizations and what kind of security system is required today. The methodology use to achieve this work was the bibliographic review and previous studies of some research or scientific investigations including the protection of the organizations or companies.

Cybercrime is also rapidly expanding, making our confidential data used without our permission. By the definition of cybercrimes much more depends on the politics of each country, since cybercrimes cause huge losses to the attacked, in cases of moral, financial and even can damage the bankruptcy of the organization. To solve this problem, our recommendation for companies is at the first time to sensitize workers about cybercrime and at second time to provide strong security architecture of their computer system.

Companies to protect their property and ensure the safety of its employees, they must attach great importance to the security branch of the company build a computer system with a high level of security.

***IndexTerms* - Cybercrime, Technology, Crime, Company, Security.**

I. INTRODUCTION

This article presents an expanded model of confidential data types, and such as its own initiative to raise awareness of the organization's employees and those responsible for the organization's confidential information on cybercrimes, which identifies the activities of the data re-routing process and internal e-mail, keys, restricted access and the main data flows in this process, an important aspect of the development of support tools. Literature models are tracked and compared to the new model. Note that the model is broader in the technical strategy than those dealing with digital data processing in the legal area; this is aware but organizations are more likely to focus on preventing future disasters from attacks that are more common or frequent in recent years.

Meanwhile, cybercrimes are executed to generate profits for cybercriminals; some cybercrimes are run for the purpose of generating profits for individuals who lose or lose their freedom, while others use glasses or networks for malware, illegal information, images, or other materials. Some types of programs are, in turn, like computers to infect viruses, which are then distributed to other machines and sometimes to entire networks of organizations.

II. LITERATURE REVIEW

G. Graham, Anita Greenhill, Vic Callaghan, [5] Tells about predictive technology and social change in the field of information and communication technologies making predictions on the evolution of business models or the famous digital marketing based on the emotional prototyping of users. The digital marketplace, and it has not lacked a futuristic or holistic view of trends and technological advances in the areas of artificial intelligence, robotics and cloud computing has brought very significant changes in today's society. Previous studies of some works have turned more against creativity, invention, and technological innovation as a lever for futurism, less attention has been given to the challenges and threats of cybercrime.

Bulgakova, E., Bulgakov, V., Trushchenkov, I., Vasilev, D., & Kravets, E. [6] According to the authors, they make a thorough analysis of the use of Big Data for investigations and prevention of cybercrimes in digital data because of its breadth in areas such as health, education, economics, culture, construction, commerce, computing and more, which are part of human activities without taking coherent measures to combat cybercrime using specialized professional systems, robust criminal investigation software Digital data theft could compromise the performance of everyday services or even the future generation. [6] The company as IBM has developed a cybercrime reduction system using statistical histories; this system provides US police with information on areas or areas with the highest potential for cybercrime threats by tracking vulnerability sites and monitoring their distances of the attackers, and by creating predictions of the days and months with the highest trends of criminal growth, this system made a significant decrease of almost 15% in the reduction of serious crimes, despite the data produced between 2012-2019, many of them are not being controlled by people but by machines or systems. This author's suggestion is to take steps to safeguard privacy and protect Big Data users with new legal laws for cyber criminals.

Wright, S [7], from this Author's point of view prior to the discovery of the internet or cyberspace there were no cybercrime, no computer viruses or less hacking, criminals performed these unethical acts physically, but with the arrival of the internet in the 60's the scenario Completely changed at another point brought many advances in socialization there is humanity, shortening of border barriers in communication and knowledge sharing but on the other hand brings a discomfort leading to huge concerns over the numbers of fraud and cybercriminal violations and the [7] highlighted Alan Turing as the great hero for the evolution of this technological age of intelligent machines and big data.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A., [8] The most common legal principles of data security are Confidentiality, Integrity, and Availability when one of the principles is violated refers to the vulnerability of According to Wall (2005), the Internet has created a criminal cibe opportunity classified into three levels namely low, medium and high depending on its impact, [7] due to the demand for large volumes of data flowing into networks. Computer and distributed systems The technology for the monitoring of attackers makes it very difficult whose data protection laws are not applicable almost everywhere due to the lack of training of men of justice in cybercrime matters or the tendency of new criminals of the century of the technology age.

- Technology is "*a body of knowledge devoted to creating tools, processing actions and the extracting of materials*".[1]
- A crime is "*an offence that merits community condemnation and punishment, usually by way of fine or imprisonment*" [2].
- The topic "*technology, crimes and its changing patterns*" refers to these crimes that are commited by the help of technology and how it change human mind regarding the several actors of this talking such as victims, authors of crimes and actors who fight aigainst these crimes. the technical term for these crimes are cybercrimes.
- Cybercrime is any criminal activity that involves a computer, networked device or a network.

III. TYPES OF CRIMES

We can define crimes in two ways: according to criminal law and then list the types of cybercrimes.

3.1 Types of crimes according to criminal law

We can divide this in two 4 categories:

- ✓ **Personal crimes**

"*Offenses against person*". These are crimes which reach the physical or moral aspect of human being. These are: Assault, Battery, False Imprisonment, Kidnapping, Homicide (crimes such as first and second degree, murder, and involuntary manslaughter, and vehicular homicide), Rape, statutory rape, sexual assault and etc.

- ✓ **Property crimes**

Are "*offenses against property*". Its directly reach human goods. These are:
Larceny, Robber, Burglar,Arson, Embezzlemen, Forgery, False pretense, Receipt of stolen goods.

- ✓ **Inchoate crimes**

Incomplete crimes are crimes whose participation is judged to be minor, i.e., the participation is not total in the targeted crime. These are:
Attempt – any crime that is attempted, Solicitation, Conspiracy.

- ✓ Statutory crimes cries related to non-respect of State, statute like alcohol-related and selling alcohol to minor.

3.2 Types of crimes related to Internet

These types of crimes are known as Cybercrimes and they are committed using Internet.
Six types of Cybercrime are listed here.

- ✓ **Hacking**

It is the unauthorized accessing to a computer or electronic or computer network. The persons related to these crimes are called hackers.

- ✓ **Online child abuse**

The sexual exploitation of minors on the Internet. This includes selling the distribution of child pornography through the web.

- ✓ **Ransom ware attack**

This involves injecting viruses into the network or computer. Often access is blocked against a payment of ransom.

- ✓ **Cyber stalking**

This categorizes the crimes concerning harassment blackmail, tracking by Internet. And that leads sometimes to suicide and murder.

- ✓ **Online Identity theft**

It's identity theft across the net. This results in the appropriation of personal information such as banking and other information.

- ✓ **Internet frauds**

It is the fact of extracting money in a fraudulent way that is to say dishonest.
For example, creating fake sites to collect donations to people who are sick or in difficulty or to support public action.

IV. VULNERABILITY TECHNOLOGIES

As we use Internet we are directly open for the cybercrime attacks but among technologies there some kinds that are mostly involve crimes.

4.1 Social network

Social network is defined like a platform which permits people to interact on common interest. For example we have Facebook, What Sapp, twitter etc. social networks are very vulnerable to the theft of personal information that can be used to commit crimes.
On that platform we post, share information like pictures, personal documents. And sometimes we share critical information with a badly intentioned person and then come crimes like harassment, identity stolen. People use social networks to create fake profiles and act with them to harm a person or an organization also to create conflicts between natural or legal persons.

4.2 Mail box

V. Mail is used in professional manner to exchange information. The unwanted people take ownership of your email account and do what they want with such as sent messages making it look like you and even steal your banking information etc. For organization or for important purpose sharing information through email is not carefully for the confidentiality statement.

4.3 Weak security computer network

Not isolating critical data from public data is dangerous for the company. It means a computer network whose internal media is the Internet is more vulnerable to attacks. The private network parts of the company's third parties are unfortunately not protected from these accesses and this only increases the risk of vulnerability to data breaches. Using also a public mail system for sharing information among workers of companies is not a good way to prevent cybercrime. To affirm that this technology is vulnerable, it depends on how you are use it.

VI. PREVENTING CYBERCRIME

According J.R. Clark and W.L. Davis, Preventive measures are "*available that help deter cybercriminals, including passwords, firewalls, encryption, and other security policies and procedures*". Since preventive measures are not always successful, cybercrime detection is a necessary last line of defense regarding loss prevention, or at least loss minimization. Detection techniques include tripwires, configuration - checking tools, and anomaly detection systems.

A tripwire is a software program that takes snapshots of critical system characteristics that can be used to detect change critical file changes. Tripwires provide evidence of electronic crimes, since most intruding hackers make modifications when they install backdoor entry points or alter file system and directory characteristics in the course of hacking the system.

A configuration – checking tool, also referred to as a "*vulnerability assessment tool,"* is a software program that detects insecure systems. Configuration – checking tools are primarily preventive in nature but, when used as monitoring devices, they can also provide evidence regarding electronic crimes.

An anomaly detection system focuses on unusual patterns of system activity.

Anomaly detection systems develop and analyze user profiles, host and network activity, or system programs in order to identify deviations from expected activity.

Experienced cybercriminals can obscure their actions through various methods. For example, cybercriminals may spread their intrusive behavior over a number of hosts on a network in order to defeat a single host intrusion detection procedure. Selecting and merging data from independent intrusion detection techniques, as well as the network itself, is necessary to identify this type of behavior.

Cybercrime is unlikely to be identified by random and intensive searches for evidence of criminal activity. If a cybercriminal can convince an intrusion detection system to continually and uselessly increase its use of computer resources, the criminal has effectively accomplished denial of service, a particularly destructive type of cybercrime. In such a case, computer resources are wasted and cybercriminal are not detected.

Since cybercrime is detrimental to business operations, companies and their stakeholders clearly benefit from stopping cybercrime. Unless properly and continuously " fine-tuned," a single intrusion detection technique may tend to under – report cybercrimes or over – report incidents, such as excessive false alarms. In most cases, companies find it necessary to employ multiple intrusion detection techniques to efficiently and effectively detect electronic crimes.

Appropriate actions must be taken by qualified professionals to successfully resolve cybercrime. Since some companies may lack qualified computer security personnel, hiring outside professionals, such as forensic accountants, may be necessary. For a company with computer security personnel, outside professionals may still be needed if the electronic crime resulted from negligence on the part of the company's computer security personnel. Law enforcement agencies can help with cybercrime investigations; however, many law enforcement agencies lack the technical expertise to investigate electronic crimes. Most can obtain warrants and seize computer equipment, but may be unable to find the evidence needed to resolve the cybercrime.

VII. Conclusion

We cannot live without Information and Communication technology. it is in our household (IOT), in our activities, in our relationships (smartphones). Solutions against cybercrime are progressing day by day from physical and architectural facilities (alarm system, video surveillance etc.) to software installations (viruses, tracking software, flow control over a network etc.). Also on the side of the law, investigations continue to be conducted to fight against this scourge.

For any organization, to protect its employees and good, the need is to make a strongly security system and also sensitize employees about how to use Information and Communication technology in good way.

We cannot avoid technology but we can prevent attacks by means of technology.

References

[1] A.Salkever, 2003,"'Phishing' Is Foul on the Net," Business Week Online

[2] D. Bank and R. Richmond, 2005, Where the Dangers Are: The Threats To Information Security That Keep The Experts Up At Night—And What Businesses And Consumers Can Do To Protect Themselves, Wall Street J., p. R1.

[3] R. Anderson and B. Schneier, 2005. Economics of Information Security, IEEE Security & Privacy, vol. 3, no. 1, pp. 12–13.

[4] Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A., 2014. Cybercrime classification and characteristics. Cyber Crime and Cyber Terrorism Investigator's Handbook, 149–164

[5] G. Graham, Anita Greenhill, Vic Callaghan, 2013, Technological Forecasting and Social Change Special Issue: Creative prototyping, Technol. Forecast. Soc. Change .

[6] Bulgakova, E., Bulgakov, V., Trushchenkov, I., Vasilev, D., & Kravets, E., 2018. Big Data in Investigating and Preventing Crimes. Studies in Systems, Decision and Control, 61–69.

[7] Wright, S., 2017,. Mythology of Cyber-Crime—Insecurity & Governance in Cyberspace: Some Critical Perspectives. Advanced Sciences and Technologies for Security Applications, 211–227.

[8] Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A., 2014. Cybercrime classification and characteristics. Cyber Crime and Cyber Terrorism Investigator's Handbook, 149–164.

https://www.useoftechnology.com/what-is-technology/ [1]

https://lawhandbook.sa.gov.au/ch12s01.php [2]

www.businessweek.com/technology/ content/oct2003/tc20031021_8711_tc047.htm.