International Journal of Management, IT & Engineering
Vol. 9 Issue 02, February 2019
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A CRITICAL STUDY ABOUT THE MODEL FOR CYBER LAW PROBLEMS AND CYBER CRIME PREVENTION AND ENHANCEMENT

Vineet Kumar, Research Scholar, Dept. of Computer Science, Himalayan Garhwal University, Uttarakhand
Dr. Harsh Kumar, Associate Professor, Dept. of Computer Science, Himalayan Garhwal University, Uttarakhand

ABSTRACT

Cyber crime is rising at an exponential pace in the current scenario, as computer technology is growing at enormous high speed, which is why the cyber crime investigation process is also becoming a tedious process without a good model/framework for cybercrime investigation. A good model/framework for cyber crime investigation is critical because it offers an abstract reference framework/model that is independent of any specific technology or organisational context and promotes the development of new investigation techniques and tools. As all of their actions/activities are subject to judicial review should the case be brought in court, it is really very important for the cyber crime investigation to perform their work properly. There are several types of cyber crime or forensic analysis that are being proposed by different investigators. As per observation, most of the models incorporated either one feature or a few aspects of the cybercrime investigation process from different levels. Most of the exit model does not cover significant cyber crime problems or security risks that may impact the process of investigation. Only processing, such as selection and analysis, is concerned with the current models. While this is necessary and beneficial, it is not sufficient for the investigative process to be thoroughly explained in a way that helps to process the investigation. Many of the digital forensic investigation processes have been developed either by conventional forensic scientists focused on rigorous handling of evidence or by digital evidence capture technologists, making it difficult for law enforcement personnel to recognise and adopt them. Another downside of current models is that they have placed more emphasis on the compilation and analysis of evidence, which is essentially the middle stage of the model. For a good cyber crime investigation model, however the earlier and later phases must be taken into account. Overall, it can include the proposed model.

Key Words: cyber crime, Internet, Commercialization, investigation model

INTRODUCTION

After oral, verbal and gesture-based records, the Internet is the key mode of communication. For marketing and comp randomization, which relies on computer-based systems, the knowledge is most relevant. There is a need for strict regulation or implementation of rules due to increased internet usage.

Information services and systems are beginning to have a major impact on the economy, trade and commerce of the world. All types of transaction rule based on performance from as advised by the sanctioning bodying and transmission of information through the Internet are carried out by the stock exchange in the country. Examples of Internet use are all electronic commerce solutions such as Commercialization to Commercialization (B2B), Commercialization to Customers (B2C) and Commercialization to Body (B2G) relationship, Database-driven shopping cart, appliances, and the amount to be charged by credit card. Cybercrime has the power to shake societies, such as hacking, online financial fraud and planting computer viruses. Cybercrime is rising at a high pace, posing a threat to technology and the system of criminal justice. So one should understand the question like what is cybercrime, before the generation of cyber law. What are the various forms of cybercrime? How does cybercrime vary from ordinary crimes such as murder and abduction? What are the most efficient techniques of coping with cybercrime? What kind of legal assistance is being given to cybercrime victims? Other than cyber criminals, no web site owner can afford to neglect these problems, because cybercrime can be directly or indirectly victimised not only by the IT community but by random citizens of the planet. In India, some type of crime is very popular, such as selling pirated audio CDs that are protected by copyright law, people send the abuse e-mail to the other person, some individuals use the Internet to sell the illegal item such as narcotics and cocaine, some computer experts use the Internet to steal the confidential information pass from one computer. While India's cybercrime scale is nowhere close to the developed world, it threatens to become pervasive and to rise to a shocking level. Some hackers hacked and defected Indian website numbers like Indian Science Congress, Asian Age newspaper, National Research Center, Indian Technology Institute are among many others in the previous year.

Implementation Short comings and drawbacks of Cyber Law:-

While most countries in the world, such as the US, Canada, UK, Australia and others, have their own cyber law, cyber law is not completely functional in the cyber space due to the following reason.

1. One of the key reasons for the implementation of cyber law is the lack of provision in the cyber environment. Like in India, online shopping sites have made a lot of transactions, but the Information Technology Law based on results as recommended by the sanctioning body does not include random provision of the sections related to credit card fraud. And if this kind of case happens in India, the case is tried instead of IT-Act under the current rule based on performance as recommended by the sanctioning body such as Fraud and Forgery and Section 420 of the IPC refers

to performance based on that rather than random section of said IT-Rule as advised by the sanctioning body.

2. The cyber-crime is the outside the jurisdiction. The criminal will then commit the crime through the Internet from a random part of the world and that's why it's more difficult to track the criminal than traditional crime.
3. There is a lack of consistent international law on cybercrime, so he/she will not be adequately prosecuted by the local court by a random individual committing the crime in another country. Therefore, the need of the international uniform law and international court is important in the cybercrime.
4. It is far from the traditional crime to search the suspect here because the criminal does not leave and tangible evidence in the cyber crime. The gathering of evidence is therefore a very difficult problem in cyberspace and it took a lot of experience and ability to look for the evidence against cyber criminals.
5. Another issue is the understanding of cybercrime and cyber law among police, lawyers and judges, since it requires computer and internet skills to understand cybercrime, whereas law expertise is necessary for prosecution and both skill in the individual is rarely found.

Network Security:

As we know that "prevention is better than cure," our first duty is to build the secure framework before we begin rule-based success as instructed by the computerised system's sanctioning bodysuit use. The software professional must therefore set standards to avoid cybercrime and take all precautionary measures such as firewall and data encryption strategies for the random computerised framework. Other than that, such policies and procedures must be developed by the computer industries to avoid cybercrime.

Cyber Crime Detection:

Another primary concern for the elimination of crime is to locate the crime at an earlier stage before the chaos among Internet users is generated. But one should know when the attacker's abuse of the machine begins.

Case Filing:

The case filing and sending the victim's cybercrime is also a significant cybercrime problem, so the victim can come forward and report to the cyber cell about the cybercrime instead of thinking about random stuff.

Proof Collection:

The evidence is in the digital form in the cyber rather than the tangible form such as paper or arms. Since the overwhelming amount of information on small media is processed by the computer, it is much harder to find digital evidence from the vast information stored in the same media. The investigator should then use special techniques to examine the particular type of media information to make the proof collection method simple.

Some live detection tools are also available during the use of the computer to control and track user rule-based output as recommended by the sanctioning body. It is not enough to gather the evidence here but it is equally important to store and show the evidence in front of the court during the prosecution.

For the gathering of evidence, there should be a suitable model that allows the investigating officer the ability to gather and store the evidence.

RESEARCH METHODOLOGY

In general, the word "forensic" means the use of science and technology, as instructed by the sanctioning bodies in court for legal prosecution, to investigate and develop ferule-based results.

Category of Investigation

Internal: - This is a very straightforward inquiry in which I try to find the employee who violated the corporate policy. I don't want to rely on random other resources here to search this kind of person or even it is not necessary to get a search warrant or discovery order because all resources are available within the comp random premises and that can be used at random time by the investigator. So some time comp unexpectedly, committed by the internal investigation and search of the suspects, do not want to approach the cybercrime court.

Civil: - The civil investigation is identical to the internal investigation, with the exception of the two comp random inquiries instead of one comp random. Therefore the disadvantage of victim comp random is that on the basis of suspicion, they can not examine the resources of other comp random, so the comp random needs to contact the civil court and on the basis of that the judge gives the discovery order that the investigator can try the opposite comp random resource.

Criminal: - This form of investigation also requires the highest sticks. One line is the suspect's livelihood, and each part of the case is scrutinised and reworked numerous times. Here last week, months and even years could be the time period of the investigation is not relevant procedure.

The Role of Investigator:

Bias: - A cybercrime investigator is a neutral person. The investigator is a third party in most cases, but he is not part of the suspect comp random or the supposed comp random that perpetrated the cybercrime. It is also required; in the past and present, there should not be a random direct or indirect relationship with alleged comp random.

Qualification: - Because cybercrime in the court of law is very difficult to identify and difficult to prove cyber crime. It is very important that investigator sound have knowledge of the computer technology especially in area of Internet, network management, operating system and its storage management. This is not necessary for the prosecutor, but he also has knowledge of the legal system and legal procedure, in particular the law of evidence, the law of civil and criminal procedure based on performance as advised by the sanctioning body. In addition, the prosecutor needs to collect the details according to the case he manages and the legislation should be kept in his mind, such as taxes, electronic commerce, restriction rule based on performing as advised by the sanctioning body, copyright law, etc.

Use of Proof: - The prosecutor is therefore obligated to store and collect the evidence to be produced for trial in court. The investigator must then consider what the valid records are for today and tomorrow and how the facts must be produced to the court as a valid electronic or written document. So beginning the investigation from zero is advisable. Investigators may use various forms of investigative methods. There is also possible random absence of evidence that is disproved by the opposing party in court, so it is also also important to cross-validate the evidence by several tools and it is only accepted as valid evidence if more than one tool offers the same evidence

Investigator Liabilities: - It is also the duty of the investigator that random harm to a random resource or entity does not occur at the time of the investigation phase. Here the investigator can also use multiple comprehension services during the investigation and run multiple software on the accused devices, so that data from those resources can also be lost. In short, the prosecutor should know his limit of the investigation process and he must take the court's prior authorization for complicated and dangerous inquiries in a randomly complex situation.

Forensic Investigation Life Cycle (FILC)

The FILC is concerned here with how the investigation will perform the ideal investigation process to catch cybercrime offenders. The effectiveness of the investigation depends on how the chain of evidence is used to prove the cyber crime in court. Therefore the era of forensic investigation determines both the technical and legal aspects of forensic investigation. There is a 5R policy here that facilitates the investigation in order to aid in a legal case. There are the 5 R's as follows.

1) Requirement investigation
2) Retrieval of Data
3) Reliability
4) Review of proof
5) Repository of data

If all five phases are correctly implemented, the investigation process provides the optimal outcome, so it is first of all important to personally understand all phases in detail.

This study's data collection approach includes the use of papers, conference proceedings, books, blogs, workshops and seminars to understand digital forensic cybercrime and security threats and vulnerabilities.

RESULTS AND DISCUSSION

Phases of Cyber Crime Investigation Process Model

Promptness Phase:

The aim of the Promptness Process is to ensure infrastructural and operational readiness to support investigations into cyber crime.

Collection

Evidence from where the incident happened is obtained in this process. Using digital forensics to classify, document and mark data from different heterogeneous sources of relevant data.

Identification

This stage includes the recognition of the offence or incident.

Authorization

This stage authenticates and authorises the incident and cyber crime to be investigated.

Preparation

This stage consists of different methods and procedures for planning, as well as incident tracking and management.

Strategic Planning Phase:

The purpose of this step is to identify, alter, devise, audit and deploy the cyber crime investigation process

Classification:

The classification stage is determined by the occurrence of different kinds of cyber crime incidents. It will be graded according to the classification of crime.

Transformation:

After crime classification, the information and data are obtained from multiple sources and this data is converted so that they can be used in the next step.

Formulate:

It will be formulated using transformed data in such a way that it will be specifically used for the implementation phase and investigation process.

Auditing:

It needs auditing prior to the deployment of the procedure or investigation.

Deployment:

The main aim of this stage is to provide a detection and conformity system for the incident of cyber crime.

Analysis and Experimental Phase

There are several activities taking place in this process, where different studies and tests are carried out on the evidence collected.

Evaluation:

In this step, the assessment method is carried out on the evidence obtained.

Comparative Implementation of Cybercrime Investigation Process Model (CCIPM)

Software engineering is integral part of the Information Technology and random new creation for custom requirement of commercialization organisation or body agency or educational institute are now doing there commerce. Exchange of information and provision of services by means of the Internet. Instead of the stand-alone application, there are a range of technical innovations for the Internet-based or web-based application. The unique aspect of web engineering is that it can provide dependency, availability, honesty, expansiveness, protection and productivity. The individual does not build the web application and works are split between the skills, so they can do well in the domain areas there.

CONCLUSION

That's not enough to draught the cyber law because it's crucial stuff because it doesn't tell the court how cybercrime can be prosecuted. That implies that the cyber law dimension is very high and complicated and the gathering of proof is also difficult to conduct from as advised by the sanctioning body, the current procedure rule based on performance from as advised by the sanctioning body, such as the civil procedure rule based on performance from as advised by the sanctioning body, and the criminal procedure rule based on performance from as advised by the sanctioning body is not sufficiently adequate So along with the significant law that is often appropriate in cyber space to render some procedural law.

Therefore the cyber process is nothing but complete execution of the court procedure and case handling, which in some respects is distinct from the current court system. The basic principle is almost identical, but one of the main issues or issues of the effective implementation of cyber law in a country and universe is the necessity of the competent individual in the investigation and the uniform law in cyberspace. The cyber procedure here means a complete collection of proceedings, containing the complete legal process from the accusation of the victim to the penalty of the perpetrator. The successful implementation of the cyber procedure involves multiple stages here, few of which are different from the current procedure, such as the civil and criminal procedure. The key concern here is to clarify how cybercrime can be tried in the court of law and how the prosecution is made less and more common in the world. I am trying to understand what kind of protocol I should follow here in the chapter of the cyber procedure to put the offender behind the bar or get compensation from the offenders. Cyber crime is also increasing increasingly worldwide as technology increases. There are no more charges for internet facilities nowadays, it is so inexpensive that anybody can use it at a very low rate. People are more savvy technologically. Most individuals do not have security value, so cyber crime is easier to conduct with innocent individuals. So law enforcement is required to prosecute each and every step of the cyber crime incident. Here in this report, the different modern technologies of cyber crime investigation are likely to be applied to recognise the danger, incident, and also provide the necessary solution to resolve cyber crime. During the entire cyber crime investigation process, various problems as well as activities are found.

The new model was split into different phases that were useful. Each stage was also split into a number of sub stages. Each stage has its own significance. It is possible to adjust and understand the model quickly. One of the most popular toolkits for carrying out theories and experiments is the FTK.

REFERENCES

1. Ahmad, I, Abdullah, A, Alghamdi, An and Hussain, M 2013, _Optimized interruption discovery instrument utilizing delicate figuring procedures'. Media transmission Systems, pp. 1-9.
2. Ahmed, M, Mahmood, AN and Hu, J 2016, _A overview of organization inconsistency identification procedures'. Diary of Network and Computer Applications, vol. 60, pp. 19-31.
3. Al-mamory, SO and Jassim, FS 2015, _On the planning of two grains levels network interruption identification framework'. Karbala International Journal of Modern Science, vol. 1, no. 1, pp. 15-25.
4. Altwaijry, H and Algarny, S 2012, _Bayesian based interruption recognition framework'. Diary of King Saud University-Computer and Information Sciences, vol. 24, no. 1, pp. 1-6.
5. Amiri, F, Yousefi, MR, Lucas, C, Shakery, An and Yazdani, N 2011,
6. Mutual data based element determination for interruption identification frameworks'. Diary of Network and Computer Applications, vol. 34, no. 4, pp. 1184-1199.
7. Aslahi-Shahri, BM, Rahmani, R, Chizari, M, Maralani, A, Eslami, M, Golkar, MJ and Ebrahimi, A 2016, _A half breed strategy comprising of GA and SVM for interruption recognition framework'. Neural Computing and Applications, vol. 27, no. 6, pp. 1669-1676.

8. Atzori, L, Iera, An and Morabito, G 2010, _The web of things: An overview. PC organizations', vol. 54, no. 15, pp. 2787-2805.
9. Axelsson, S 2000, _Intrusion recognition frameworks', A review and scientific classification, Technical report, vol. 99.
10. Aziz, ASA, Azar, AT, Salama, MA, Hassanien, AE and Hanafy, SEO 2013, _Genetic calculation with various component determination methods for inconsistency locators age'. In Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on IEEE, pp. 769-774
11. Balakrishnan, S, Venkatalakshmi, K and Kannan, A 2014, _Intrusion Detection System Using Feature Selection and Classification Technique', International Journal of Computer Science and Application, vol. 3, no. 4, pp. 145-151.
12. Bijone, M 2016, _A Survey on Secure Network: Intrusion Detection and Prevention Approaches'. American Journal of Information Systems, vol. 4, no. 3, pp. 69-88.
13. Boulaiche, A, Bouzayani, H and Adi, K 2012, _A quantitative methodology for interruptions recognition and anticipation dependent on measurable n-gram models'. Procedia Computer Science, vol. 10, pp. 450-457.
14. Catania, CA and Garino, CG 2012, _Automatic network interruption location: Current procedures and open issues'. PCs and Electrical Engineering, vol. 38, no. 5, pp. 1062-1072.
15. Chandrashekar, G and Sahin, F 2014, _A review on element choice techniques'. PCs and Electrical Engineering, vol. 40, no. 1, pp. 16-28.