Title page

Trends in cybercrime

Cybercrimes

Cybercrime is increasing rapidly in society due increased access of data to the criminals. There attacks are directed at computers and include intrusions or denial of service. ICT’s have become integral part of the business and normal life that give wider scope of attaching computers to the hackers or cyber criminals. Due to tremendous growth in technologies, criminals are also getting opportunities for committing crimes through online platforms. Cybercrimes are consistently increasing in Australia that pose threats to the safety of the society. The problem is getting more serious in Australia as in 2017 the total cost of cybercrimes was $4.5 billion (AFP, 2019). Cybercrime has deteriorating impacts on the society because it is linked to financial loss, decreased privacy, loss of reputation and psychological implications on the victims of cyber bullying. Each year industry face monetary loss when cybercriminals are blackmailing them and manage get ransom. Cyber bullying has even more negative impacts on the victims that normally include children. Psychological problems such as isolation, low self-worth and stress are common impacts. The firm also losses reputation if the hackers gains access to customers data.

Profile of cybercriminals

Online criminals are capable of committing crimes through different borders and are capable of targeting larger victims. Facts reveals that, “tools that have many legitimate uses, like high speed internet, peer to peer file-sharing and sophisticated encryption methods, can also help criminals to carry out and conceal their activities” (AFP, 2019). Profiling is recognized as an effective technique for solving cybercrimes. It is a forensic tool that helps in determining the factors that encourage criminals to commit cybercrime. This classifies criminal behavior and assist crime agents to solve crimes. The focus is on identification of criminals behavior, demographics, personality traits and geographical variables. In this technique crime control agents have to collect inferences that reveal traits of criminals behind cybercrimes. Demographic factors considered for such purpose include age and gender. Legal history of the criminal is also examined that exhibits his involvement in criminal attitudes in the past. Vocational backgrounds are also investigated that depicts the possibilities of criminals involvement in various crimes. Social activities such as hobbies, interests and social interactions are studied. Family background is investigated for identifying the factors that encourage certain criminal attitudes. Personality attributes such as aggression, tolerance and violence are examined.

Evidence suggests profile of cybercriminals as; 1) they are bright and socially inept. 2) They possess knowledge of IT, have good IQ’s and good technical skills. 3) Most of the cybercriminals are males and young boys. 4) Teenage boys with technical knowledge exhibit high likelihood of becoming cybercriminals. 5) Cybercriminals are non-violent. Lickiewicz (2011) studied the profile of the cybercriminals and revealed certain facts based on his research. Cybercriminals must possess great computer and technical skills for performing sophisticated attacks across online platforms. These people have no respect for law and they are willing to violate laws. The study of the behaviors indicate that majority commit internet related crimes for accomplishing their fantasies. They are often engaged in building new identities and portray personalities different from their reality. It is also found that young boys engaged in cybercrimes exhibit behavioral problems.

The profile analysis of cybercriminals depicts the need for understanding the motives and opportunities behind such crimes. Atkinson and Walker (2015) uncovered the common motives behind cybercrimes. These include, “sexual impulses, political motives, monetary profit, just for fun, revenge, anger, and other emotional needs, and serious psychiatric illness”. Cybercrimes are motivated by the negative feelings of offenders that include revenge, anger or psychotic problems. Mental instability or stress can be recognized as two important factors that encourage such crimes. In most of the cases cybercriminals are aiming to create realities based on their fantasies. The analysis of the personalities further reveals that these criminals are not involved in violent crimes. Such crimes are thus identified as non-violent crimes (Atkinson & Walker, 2015). The opportunities that promote cybercrimes include having increased access to internet, computers, knowledge of IT and hacking.

The profiles of the cybercriminals depicts that they care less about the social values and norms. This reflect their deviant behaviors because they act in least expected manner. Behavior analysis of teens involved in cybercrimes further reveals that they don’t listen to their parents and try to maintain their independence by engaging in such activities (Lickiewicz, 2011). Most of the teen boys have access to computers and other systems that increases the likelihood of committing such crimes.

Law enforcement and initiatives

Due to increased risks of cybercrimes it is the responsibility of the state to offer safe online environment to citizens and businesses that is important for the creation of stable and productive community. Commonwealth legislation has made laws for controlling such crimes. Criminal Code Act 1995 has recognized certain activities as cybercrimes that include; unauthorized data modifications, computer intrusions, distribution or development of malicious software, denial of services attacks. Malware, ransoms and viruses are also recognized are crimes. Australian Cyber Security Center has been involved in controlling cybercrimes by establishing guidelines. Cyber security capabilities are developed for enhancing cyber resilience and supporting economic and social progress in Australia (AFP, 2019). Crimes Act 1914 (Cth) was built for controlling online breaches and providing safe communications across online platforms. Federal legislation defined the conditions that leads to the commitment of such crimes. Crimes Act 1900 (Cth) deals with imposition of penalty depending on the personality of the offender (ICLG, 2019).

Laws have been developed that instruct companies to integrate precautionary measures for mitigating the risks of cybercrimes. Guidelines have been established by the state entities for helping businesses. Companies concerned about dealing with the issue of cybercrimes must conduct identification of legislation/ regulations. Undertaking the requirements of law for documenting activities of the cyber and information security systems are crucial for mitigating the risks of cyberattacks. Preparation of legal regulations, obligations. Statutory and regulatory compliance (AFP, 2019). Performance of compliance/ audits are essential aspects of policing. Application of accumulated knowledge highlights specific attacks and system vulnerabilities. The accuracy is good however the need for completeness is evident for updating attacks regularly. Companies are instructed to build expert system that include rules employed for the assessment of the attacks (Scarfone, 2017). Translating audit event into facts is an appropriate approach for handling the threats. Rule-based language acts as an effective tool for modelling knowledge associated with the attacks. Signature analysis is another initiative taken for detecting threats. The knowledge-based approach is used as an expert system while the information is transformed in the audit trail. Semantic level of attack description is reduced leading to efficient implementation.

Petri nets is focused on acting efficiently for mitigating the risks of cyberattacks. COATS developed IDIOT system for employing coloured Petri-nets for the detection of the signature-based intrusion. It offers many benefits including simplicity, convenience to use and graphical representation. Anomaly detections are performed weekly for determining the risks and taking timely actions (Scarfone, 2017). The anomaly detection relies on the assumption that the deviation from the normal behavior leads to the identification of the intrusion activity. The current activity is observed for detection of intrusion. User intention identification is used for setting high-level tasks needed to be performed (Scarfone, 2017).

Penalties for committing crimes

People involved in cybercrimes will receive punishment and penalties according to the law. Criminals who are suspects of unauthorized access to computers receive penalty according to 478.1 of the Code which include two years imprisonment. The suspect will receive punishment in case of `Distributed Denial of Services attack. Code 477.3 states that unauthorized impairment of electronic communication will lead to 10 years imprisonment. Laws for phishing are also developed for controlling such crimes (ICLG, 2019). Phishing style offenses leads to penalty according to the financial loss suffered by the entity. Phishing is classified as; gaining financial benefit through deception S. 134.29(1), benefit through general dishonesty S. 135.1(1), causing a loss S. 135.1(3) and causing loss to another entity S. 135.1(5). The suspect will receive 10 years imprisonment. Code 478.2 also limits cybercrime by imposing penalties on criminals who have been involved in malicious activities. Two years imprisonment is entitled to the offender who has been involved in unauthorized impairment. Code 478.3 deals with the criminals who have possessed hardware, software or other information of the entity. This law imposes imprisonment of three years. The suspect must be involved in using of the other party’s data. Laws are also established against identity theft and identity fraud. Division 372 of the code states that possession of identification information or carriage service will be dealt with punishment. The penalty imposed in this case is fiver years of imprisonment. Code 478.1 deals with electronic theft that involve breach of data or confidence by employee or copyright infringement (ICLG, 2019). The purpose of imposing penalties and giving punishments is to assure provision of safe online environment to the businesses and citizens.

References

AFP. (2019). *Cyber crime* . Retrieved 12 16, 2019, from https://www.afp.gov.au/what-we-do/crime-types/cyber-crime

Atkinson, S., & Walker, C. (2015). Psychology and the hacker – Psychological Incident. SANS Institute InfoSec Reading Room.

ICLG. (2019). *https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia*. Retrieved 12 16, 2019, from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia

Scarfone, K. (2017). *SIEM benefits include efficient incident response, compliance* . Retrieved 08 21, 2018, from https://searchsecurity.techtarget.com/feature/Three-enterprise-benefits-of-SIEM-products

Lickiewicz, J. (2011). Cyber Crime psychology-proposal of an offender psychological profile. Problems of forensic sciences, 2(3): 239-252.