WHY ARE CYBERCRIMINALS ATTRACTED TO COMMIT CRIMES

FADI ABU ZUHRI

Introduction

Cybercrime has emerged as a new form of crime following the introduction of the internet. The actions of these crimes range from petty theft to destruction with malicious intent. Individuals who engage in cybercrime have a psychological mindset that is attuned to it. Like other forms of physical crime, cybercriminals are drawn to committing cybercrimes because of certain factors. As such, to curb cybercrime, law enforcement officers must understand their nature, why they get attracted to it, and how they can effectively reduce criminal behaviour. This paper discusses the motive behind cybercrime and what makes cybercrime attractive to cybercriminals.

Cybercrime attracts individuals with a will and ability to choose between right and wrong. The will to choose is influenced by the environment and heredity factors. Rogers (2010) believes that characteristic such as personality traits and socio-demographics and others correlate with the type of crime a cybercriminal commits. Rogers (2010) asserts that psychologists can develop taxonomies of criminals and their profiles based on these common features. These categories can be useful to law enforcement officers when developing effective and practical approaches to help reduce cybercrimes.

Nine models of cybercriminals

Rogers, Smoak and Jia (2006) categorizes cybercrimes into nine models: Scrip Kiddies (SK) or Novice (NV), Cyber Punks (CP), Hachtivist (H) or Political Activists (PA), Thieves (T) or Petty Thieves (PT), Virus Writers (VW), Internals (IN), Old Guard Hackers (OG), Professional Group (P) or Professional Criminals (PC), Cyber-Terrorist (CT) or Information Warriors (IW).

The Novice (NV) criminals have limited programming and computer skills. They can only conduct their attacks when they have toolkits. Their motives for committing a cybercrime is primarily media attention. Cyber-Punks (CP) have advanced technical skills and can write their own software. They are well informed about the system they attack with many engaging in telecommunication fraud and stealing credit card numbers. Internals (IN) include the disgruntled ex-employees or employees, Petty Thieves (PT), Virus Writers (VW), Information Warriors (IW), Professional Criminals (PC), and Old Guard Hackers (OG). Virus Writers (VW) are coders that write script and use automated tools. They basically mentor Novice (NV). They seek to gain prestige and power. They have the capability of using strong malware such as Trojans to commit cybercrime. Disgruntled ex-employees or employees with technological know-how pose a security
threat. They use the privileges of knowing the system to commit cybercrime (Rogers, Siegfried, & Tidke, 2006).

Hactivist (H) or Political Activists (PA) comprises individuals or a group that justify their behaviour on moral grounds like political issues. However, it is very difficult to ascribe whether these motives are political as their actions have aspects of revenge, power, greed or just public attention (Rogers, Siegfried, & Tidke, 2006).

Petty Thieves (PT) are opportunistic computer literate people who take advantage of the organization’s poor internal security. Old Guard Hackers (OG) seem not to have the intention to commit a crime and are disinterested in intellectual activities. They disrespect personal property. Professional Criminals (PC) are specific in their activities. They hire guns and engage in corporate espionage. They have access to the necessary state-of-the-art equipment. They are also highly trained. Lastly, Information Warriors (IW) are well funded to participate in cyber attacks that may be politically motivated (Rogers, Siegfried, & Tidke, 2006).

Rogers (2010) combines the skill level and motivation into a circumflex model as shown in Figure 1. The four motivational aspects are (1) revenge, (2) financial, (3) notoriety and (4) curiosity. Information Warriors (IW), Professional Criminals (PC), Political Activists (PA) and Old Guard Hackers (OG) are at the highest level of skills. Internals (IN) and Virus Writers (VW) are motivated by revenge; Information Warriors (IW), Petty Thieves (PT) and Professional Criminals (PC) are motivated by financial motives; Cyber Punks (CP) and Political Activists (PA) are motivated by notoriety; and Novice (NV) and Old Guard Hackers (OG) are motivated by curiosity.

![Figure 1: A circumplex model describing nine models of cybercriminals, their skill level and motives [Source (Rogers, 2010)]](image-url)
Social Learning Theory

Various theories from criminology, sociology and psychology explain why people offend. These theories suggest that the aetiology of cybercriminal behaviour is influenced by diverse factors: social control, industrialization, learning, psychopathologies, class strain and physiological deficiencies. Moral Disengagement and Social Learning Theories are the most popular theories used to explain what attracts cybercriminals to commit their criminals’ activities (Rogers, 2006).

Social Learning Theory posts that a high-level learning process can produce conforming or deviant behaviour. These theories view learning process as operating within the context of interactions, social structure and situations. It is suggested that the conforming or criminal behaviour resulting from the learning process is a function of reinforcement and other variables associated with social learning process. In view of Akers cited in Rogers and Siegfried and Tidke (2006) an individual is more likely to engage in cybercrime when the following circumstances exist. Firstly, the individual is differently related to other individuals who support, commit or model the legal and social norms. Secondly, the individual is less exposed to conforming models and more exposed to deviant models. Thirdly, the individual’s learning favours engaging in deviant acts. Lastly, the individual’s violative behaviour is supported and reinforced at the expense of the behaviour that supports the conformity to existing norms.

Social Learning Theory also suggests that differential imitation and reinforcement are the primary learning mechanisms for a cybercriminal. From this perspective, the learning mechanisms are influenced by and operate through differential association process. The social environment for the criminals is created through differential association (Rogers, 2006). The social environment exposes these offenders to imitation and definitions of models. While in a social environment, cybercriminals acquire definitions by observing, learning and imitation. Similarly, external and internal sources create differential reinforcement that presents themselves in the form of tangible rewards of the criminal activity. The rewards may include social rewards, money and increase in the status of the peer. Over time, the actions’ consequences and reinforcement prominently determines the probability with which the criminal activity will be sustained as imitation become less important. Social Learning Theory suggests that errant behaviour is likely to increase and continue unabated where there is very high ratio of two variables namely positive reinforcement and punishment. In view of this theory traditional learning mechanisms namely operant and classical learning influence the offender’s criminal behaviour. Again, it becomes difficult for law enforcement officers to neutralize the criminal’s errant behaviour where the there is a resilient learning paradigm that is caused by variation in the ratio of positive reinforcement to the punishment administered (Rogers, 2006).
Moral Disengagement Model

The Moral Disengagement model by Bandura (1996) examines the process via which criminals justify and rationalize their aberrant or deviant behaviour. The moral engagement asserts that individuals tend to participate in behaviour that goes against their moral standards, and that these actions may lead to self-sanctions and possibly self-condemnation. Bandura (1990) argues that individual behaviours are influenced by moral standards. Bandura (1990)'s self-regulatory system only functions when activated. Bandura (1990) held that it is possible to disengage self-sanctions from behaviour. From the Social Cognitive Theory perspective, these mechanisms are viewed as Moral Disengagement (Bandura, Barbaranelli, Caprara, & Pastorelli, 1996).

In view of this theory, cybercriminals may defeat their internal moral control in the self-regulatory systems by ensuring their internal moral control decoupled from detrimental conduct in four ways identified in Bandura et al. (1996). These include obscuring personal causal agency, disregarding or misrepresenting the action’s negative consequences, re-construing the conduct, and vilifying the victims, blaming them and mistreating them. Evidence show that cybercriminals often reduce self-censure by using these four methods of Moral Disengagement. It is believed that these criminals often misconstrue or minimize the consequences.

It is also believed that individuals who engage in cybercrimes demonstrate higher rates of differential reinforcement, differential association, and moral disengagement as compared to non-criminals. It is also believed that a combination of these three (i.e., moral disengagement, differential reinforcement and differential association) better predicts the behaviour of a cybercriminal (Rogers, Siegfried, & Tidke, 2006). Social Learning Theory posits that the continuation of a criminal activity may be influenced by the interaction between the reinforcement and the neutralizing definitions.

Social Control Theory

Social Control Theory on the other hand provides an explanation on why people obey rules and how behaviour conforms to expectations in society. Social Control Theory suggests that internal constraints develop during childhood and crime occurs because of inadequate constraints. In other words, the free will gives offenders the choice and consequently responsibility for their deviant behaviour (Kempf-Leonard & Morris, 2012).

Social Control Theory supports the assertion that online anonymity encourages permissiveness. According to Social Control Theory, individuals are compelled to refrain from criminal and deviant behaviours where social controls, including social ostracisation and laws are present. However, the deviance grows where the controls or assumed power of controls are missing or diminished (Rogers, Siegfried, & Tidke, 2006).
Anonymity

Lastly, a unique factor in cybercrime that attracts cybercriminals is anonymity. Internet protocols allow individuals to operate virtually anonymously. The anonymity afforded by Internet has been leveraged by cyber-predators and paedophiles that gain the victims’ trust by pretending to be young females. Internet's underlying protocols and technology allows these criminals to make it virtually impossible for victims to track them by obfuscating their physical locations. Studies on individuals’ behaviour online have revealed that individual’s real world behaviour differs from online behaviour. It is believed that people reflect their true nature in the real world where self-control and societal pressures and norms regulate behaviour (Rogers, 2006). It is believed that real world moderate individuals’ behaviour is based on social identity that incorporates cultural morality and social norms.

Conclusion

As technology becomes pervasive in our connected world, it has brought certain deviant characters along with it. These cybercriminals have developed their skills to a level where they can cause massive destruction to social life and commerce. This article tries examines the motives behind cybercriminals to understand who engages in these activities and why they do it.

Even though cybercrime is considered a new type of crime, the motives behind it are not new. A model was presented that classifies cybercriminals based on their skill levels and their motives. Motives have been broadly categorised in four - revenge, financial, notoriety and curiosity. Four different social theories were examined - Social Control Theory, Moral Disengagement Theory and Social Control Theory. Anonymity is also seen as a contributor to deviant behaviour.

References


