Quest Journals
Journal of Research in Humanities and Social Science
Volume 9 ~ Issue 12 (2021)pp: 01-09
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Understanding a Hacker's Mind from a Criminal Perspective

Dr.S. Krishnan[1] and Ms Archana Shukla[2]

ABSTRACT:
Cybercrime follows the money. In today's increasingly interconnected world they conduct digital hold-ups and cause major disruption by targeting critical infrastructure. So, how do those in the financial services industry get inside the mind of the hacker? How do they separate the signal from the noise to gain effective threat intelligence insights? If the mental picture that lights up in your mind when you hear of the young hacker is of a young, bespectacled guy sitting in a dark room, with his face lit up by the bluish glow of his computer monitor, you are not too far away from reality. That's where the journey of most hackers start—staying up in the middle of the night, trying different things, finding and learning new ways to manipulate code and find vulnerabilities.
KEYWORDS: *Cybercimes, Hackers, Cyber Security, Ethics, Social Media*

***R**eceived 02 Dec, 2021; **R**evised 14 Dec, 2021; **A**ccepted 16 Dec, 2021 © The author(s) 2021.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
-Sun Tzu, Chapter III, The Art of War

Sun Tzu's exposition about knowing one's enemy has emerged as a recondite problem for legal scholars in the face of lack of efficient rules concerning hacking and continues to haunt them due to lack of understanding of the operating criminal mind and its underlying designs and motivations. The information revolution has lead to creation of 'information highways' operating across the globe through interconnected computer networks. The change has been unprecedented but surely not without pitfalls. The rapid metamorphosis of social values and structures is resulting into a control deficit and the consequent emergence of new computer crimes like hacking which have transgressed national boundaries through a burgeoning interconnected cyberspace (which has amplified opportunities for crimes like privacy violation and the information theft). Given the presence of the networked computers in almost every aspect of modern life, the amount of sensitive information stored on networks, and the relative ease with which computer crimes may be committed, the study of computer crime demands greater attention from researchers, law enforcement agencies and legislators. Law codes throughout the world have proved ineffective in curbing the expanding domain of hacking behaviour and hence a need has arisen to re-look at the strategies for containing this emergent menace. This paper seeks to make a modest attempt to peep into the hacker's mind i.e. to understand the criminal behaviour of hackers and locate the source of the rot. I seek to deploy the traditional criminological theories based on psychology, social learning and rational choice to examine how they may be applied to develop an understanding of this new deviant behaviour. However, this paper is only a modest attempt to understand the explanations that these theories may provide for hacking and thus does not seek to delve into the empirical verifications and other abstract theoretical or logical contradictions that have been offered by the critics.

"HACKER": THE CLASSICAL CONUNDRUM OF CLASSIFICATION

In order to explore the working of the criminal mind, it is required to develop an understanding of different hacking-types so that there can be systematic deduction and analysis of behavioural differences with

[1] The writer is an Associate Professor, Seedling School of Law and Governance, Jaipur National University, Jaipur. He had worked as an Assistant Professor in Apex Professional University, Pasighat, Arunachal Pradesh. He had also worked as a Journalist in Ahmedabad. He worked as a Liaison Officer and Media Relations In-charge in Indian Society of International Law, New Delhi.
[2] The writer is 5th year student of BALLB (Hons) in Banasthali Vidyapith, Banasthali.

varied underlying motivations. Rogers (2002) argues that hackers are not a homogenous group and granulization and classification is essential to pin up researches on understanding their behaviour. Generally speaking, hacking is a successful or unsuccessful attempt to gain unauthorized use or unauthorized access to a computer system.[1] However, a lack of consensus over the connotation of the term 'hacker' has been evident over the years. Originally, the term denoted outstanding and radical programmers in the computer science fields who hailed usually from Berkley, Stanford or MIT.[2] Later, the concept underwent radical metamorphosis. Hollinger (1988), based on a progression ranging from less skilled to technically elite computer crimes, divided hackers into three categories: *pirates*, *browsers*, and *crackers*. Pirates, the least technically proficient hackers, confine their activities to copyright violations through software piracy. The browsers, with a moderate technical ability, gain unauthorized access to other people's files but do not usually damage or copy the files. The crackers, the most proficient hackers, abuse their technical abilities by copying files or damaging programs and systems. McAfee Corporation adopts the classification of hackers into *White Hats* and *Black Hats.*[3] White Hats tend to find flaws in security networks for security corporations and thus contribute to the beneficial improvement of computer

[1] Under Section 66 of the Information Technology Act, 2002, a person is said to have committed hacking if he, with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.

[2] Peter T. Leeson & Christopher J. Coyne, *The Economics Of Computer Hacking*, 1 J.L. Econ. & Pol'y 511 (2005), at 513.

3 *See* Cynthia Fitch, *Crime and Punishment: The Psychology of Hacking in New Millenium*, (Dec 16, 2003), retrieved from <http://www.giac.org/practical/GSEC/Cynthia_Fitch_GSEC.pdf> (Last accessed on July 10, 2007).

services for the users. Black Hats, the ill-intentioned hackers who abuse their skills, can be further subdivided into *angry hackers*, *script kiddies*, and *agenda hackers*. Angry hackers, motivated by hatred for a particular company or group, dedicate their resources to harm them. Script kiddies create mischief on the internet for fun and use hacking tools made by others. Agenda hackers include those disillusioned by political or economic agendas or engaging in terrorist activities through large scale disruption of computer networks. Lemos (2002) refers to a third group of hackers called *Gray Hats* who are independent security experts, consultants or corporate security researchers and are essentially reformed Black Hats like Kevin Mitnick.[4] Finally, Rogers (2002), using the findings from works of the computer security industry has categorized hackers into seven distinct groups on a continuum of lowest to highest technical ability[5] viz. *Tool kit/Newbies* (NT), *cyberpunks* (CP), *internals* (IT), *coders* (CD), *old guard hackers* (OG), *professional criminals* (PC) and *cyber-terrorists* (CT). The NTs are at initial stages of hacking with limited programming skills and use tools and information provided on internet by experienced hackers. CPs, skilled enough to write their own programs, maliciously deface web pages and send viruses, worms and junk mails. Disgruntled employees or ex-employees who hack into or attack their employer's computer systems either by abusing their privileges or special knowledge constitute the internal group and conduct a formidable 70% of all hacking activity. OG hackers have high levels of skill and understanding of computer systems and programming but are not malicious in their intent and look upon hacking as an intellectual endeavour. Lastly, the PCs and CTs, the most dangerous hackers, are highly skilled, use the latest technology and may act as mercenaries for corporate or political purposes.

II. A PSYCHODYNAMIC PERSPECTIVE ON HACKING

Psychodynamic theories of crime were built on the ashes of Cessare Lombroso's famous biological theory of crime which had conjured up a 'predestined actor model' for the

[4] Mitnick had been convicted for a four year term for his hacking spree in US and is presently acting as a security advisor forming his own security company. He is being hired by companies to break into their computer networks, reveal their security system weaknesses, and teach them how to better protect themselves at high pay packages. *See* Talya Halkin, *Legendary hacker Mitnick turns legit*, The Jerusalem Post **(**Feb. 24, 2006).

5 *See also* Cynthia Fitch, *supra* note 3.

criminal and explained criminal activity as an outcome of factors internal to human body creating inherent 'criminal dispositions'. They brought forth the 'criminal mind' as the force behind crime, operating free from differences of social milieu.[6] There seems to be a natural link between hacking activities and hacker's psychology as they indicate premeditated and learnt patterns of behaviour. I propose to discuss three prominent psychological theories viz. Sigmund Freud's psychoanalytic theory, B.F. Skinner's Operant Conditioning and Hans Eysenck's EPN theory.

(A) The New Age Hacker & Freud's Psychoanalysis

Psychoanalytic theory, as developed by Sigmund Freud, relies on the hypothetical fragmentation of human personality into unconscious and conscious forces.[7] Freud proposed that human conduct is governed by three forces viz. Id, Ego and Superego. Id represents the unconscious impulsive force which includes primitive biological needs like thirst, hunger and sex etc. He proposed a conflict of Id with Superego, which according to him, represented the inner moral agency, whose development depends primarily on satisfying parent-child relationships. The formation of superego depends on the norms and moral values learnt by the child from his parents and guardians. In this paradigm, ego represents the conscious part of personality which seeks to balance the above two opposing forces. Behaviour depends on the balance of the psychic energy system and any disturbance in this system may produce maladaptive development.[8] Thus, he highlighted two causes of deviant behaviour (1) an inadequate superego formation and functioning due to impaired parent-infant relationships whereby the individual fails to control the impulse of Id, and (2) repressed unconscious desires stemming from a failure to express strong emotional ties with another person, often the parent. August Aichhorn, another renowned psychoanalyst, stated that there was some underlying predisposition termed "latent delinquency" which causes the later criminal behaviour. A failure in psychological development accentuates the initial asocial tendency (latent delinquency) with which every child is born and thus results in deviant behaviour. Other

[6] *See* Roger Hopkins Burke, *An Introduction to Criminological Theory* (Lawman Pvt. Ltd., New Delhi, 2001) p. 77.
[7] *See* Larry J. Seigel, *Criminology* (Wadsworth, 7th ed., 2000) p.163.
[8] Burke, *supra* note 6, at pp.78-79.

psychoanalytic theorists felt that the inability to postpone immediate gratification in order to achieve greater long-term gains was a key factor in criminal behaviour.[9]

Strictly, psychoanalytic theories are more suited for crimes that result from unconscious conflicts like sexual offences or kleptomania. They are not well equipped to explain pre- meditated and planned computer crimes. The psychoanalytic theories concentrate mainly on unconscious factors and the child-parent interactions. A failed bond with a parent is unlikely to lead a child to acquire computer knowledge and practice hacking. Rogers (2000) argues that although several of the more infamous hackers had associations with dysfunctional families, this is not sufficient to explain their choice of the criminal activity to engage in as hacking does not seem to fit in the traditional view of "repressed desires" in the unconscious. Hacking is a conscious activity dependent on specific technical skills, operational knowledge of computers, networks and advanced technological understanding. To be successful at hacking the individual also has to plan the attack in some detail i.e. choose victim system or networks based on their security levels or other interests of the hacker. Thus, Freudian psychoanalytical theory fails to account for the emergent hacking behaviour due to its inherent structural constraints.

(B) Is Hacking a Conditioned Behaviour?

B.F. Skinner's has argued that human behaviour is determined by the environmental consequences it produces for the individual involved. A behaviour that produces beneficial and desirable consequences multiplies in frequency; which is called *reinforcement* of the said behaviour. On the other hand, behaviour, which produces undesirable consequences, decreases in frequency due to *punishment*. Behaviour therefore operates on the environment to produce results that are either reinforcing or punishing.[10] Thus, a rewarding criminal activity leading to increase in prestige, money, or feelings of adequacy makes the person more likely to engage in further criminal activity. If the consequences are negative viz. arrest or ostracisation, then the frequency of future criminal behaviour should be reduced. Operant conditioning can be used to explain general delinquency as opposed to focusing on specific offences where its application is structurally constrained due to uncertainty in determination of offence-specific levels of

[9] *Id*, at p.79.
[10] *Id*, at pp.83-84.

rewards and punishments. Penalties for computer crime may have minimal effect as hackers constitute a counterculture and operate in a world of anonymity where chances of being caught are miniscule. In such a scenario, penalties might serve more as a challenge to boast about eluding them. Wible (2003) also argues that punishment alone may not be the best preference-shaping model in the computer-crime context. Moreover, hackers who have been caught and repeatedly punished, with no obvious reinforcement, still continue to engage in the activity as if it was an 'addiction'.

(C) Hans Eysenck's Theory: The EPN Criteria

Focussing on influence of both social and biological factors on individual personality, this theory is based on the notion that through heredity some individuals are born with certain learning abilities which are conditioned by environmental stimuli. The theory is premised on two dimensions of personality viz. extraversion (E) and neuroticism (N) existing on a continuum. The extraversion dimension ranges from high (extravert) to low (intravert) and neuroticism dimension from high (neurotic) to low (stable). There is a separate third dimension called 'psychoticism' (P) which seeks to measure attributes such as aggression, preference for solitude, and lack of feelings for others.[11] According to the theory, children learn to control antisocial behaviour through the development of a conscience which is a set of conditioned emotional responses to environmental stimuli associated with antisocial behaviour e.g. an act of punishment from a parent for some antisocial act. The conditioning socializes the child but its nature is integrally connected with the EPN parameters of an individual's personality. High E and high N scores indicate poor conditionability and poor socialization producing an inclination towards criminal behaviour. On the other hand, low E and low N scores lead to good conditionability and effective socialization resulting in better internalisation of social norms and reduced deviancy. High scores on the third dimension psychoticism (P) would indicate hostility towards others and an inclination to more aggressive, violent criminal behaviour.

[11] *Id*, at pp. 84-85.

Rogers (2000) points out that Eysenck's theory is "geared more toward anti-social behaviour, and has had mixed results in predicting general deviancy". The development of conscience in relation to hacking activity becomes irrelevant as parents are unaware of basics of computers and thus fail to condition the children in the right direction. There are hardly any crystallised social norms or morals governing use of the new computer technology. Thus, the proposition that a conditioned moral reflex against hacking can develop in such a state of absolute moral ambiguity is untenable. Moreover, the theory would predict that hackers should be high on the extraversion scale i.e. having unstable personalities. However, Rogers (2000) argues that the majority of the arrested hackers and those, which have responded to surveys, indicate they are withdrawn, uncomfortable with other people and are *intraverts*. The theory fails on certain major behavioural explanations concerning hackers' personalities.

What makes hackers tick?

Hackers can come from wide variety of backgrounds, such as kids looking for notoriety, upset employees seeking revenge on their employer, or experts working for global cybercriminal rings. The level of their hacking skill can also range dramatically from computer whizz kids to less-capable "script kiddies" who essentially use pre-written exploits downloaded from the internet.

Broadly, hackers typically fall into three main categories:

- Cybercriminals, normally motivated by financial gain
- Activists also referred to as 'hacktivists' who are driven by political motivation
- Government-sponsored networks of hackers who carry out cyber-warfare

Hacktivists have a political agenda and want to draw attention to a perceived wrong-doing or target a high-profile organization. They normally want to achieve one of three things: expose sensitive data, alter or deface information or launch a distributed denial of service (DDoS) attack, in which a multiple compromised computer system attacks a target, such as a website or server, bringing down the service. Hacktivists range from students to those with a great deal of technical experience.

Cybercriminals are often highly sophisticated. They typically work in teams utilizing different skills sets, with members sometimes hired on the dark web. These hackers normally plan their attacks very carefully. Attacks range from distributed ransomware to SQL injections and phishing.

Group mentality

Hackers are also increasingly banding together to support each other and create new threats. For example, Morpho, also known as Wild Neutron, is a well-funded group that has carried out several high-profile hacks on international enterprises including Apple and Microsoft using a zero-day software vulnerability.

The WannaCry ransomware attack, which spread like wildfire last year, is an example of the power of these groups. WannaCry targeted an exploit in systems running older versions of Windows and installed backdoors onto infected systems, encrypting data and demanding ransom payments in bitcoins. The attack is estimated to have affected over 300,000 computers across 150 countries.

Putting personas to the test

Personas are invaluable to penetration testers or ethical hackers who help organizations find vulnerabilities and risks to their infrastructures. Threat actions and threat actors or hackers are simulated to determine the risk to an organization, its assets and data.

The data gained from these penetration tests are key to helping organizations put the right security levels in place and second guess what type of attacks are around the corner. It also helps to test the effectiveness of security teams.

An apparently lawless world of opportunity

There are many reasons why information on cybercriminals is scarce: only 11% of cyber-crimes are ever reported, and for those charged conviction rates are extremely low.[3] Indeed, part of the lure of cybercrime lies in its anonymity compared to "real world" crime. Data can be encrypted and digital footprints wiped. Added to this is the perception that policing of cyberspace is weak. According to one "old style" criminal turned cybercriminal: "no-one really seems to be on top of it. And to be honest [sic] [it] seems to be pretty much risk-free".[4] Another reports, "it's a known fact that people who commit cybercrime are hard to track down. There is less risk hacking a bank than walking in with a gun and robbing it", a perception which applies to white collar crime more generally.[5] As a result, the social profile of cybercriminals is diversifying, as increasing numbers of people are attracted to the perceived lawlessness of cyberspace. Whilst their goals may be vastly dissimilar (overthrowing governments, defrauding civilians, political activism, etc) they are united by their use of cyberspace as their method of achieving them. This shared attraction is worthy of further attention. Viewing any crime from a criminological perspective may help understand why it has been committed, and how it can be prevented. In the words of Professor Marcus Rogers, cyberforensics researcher at Purdue University: "it's about looking at the computer and the internet as an electronic crime scene, and looking for indicators of signature behaviours […] that allow us to paint a picture of the individual who's responsible".[6] It must be borne in mind, however, that a century or more of criminological study has still not led to the discovery of reliable predictive factors.

New weapons for veterans

Cybercriminals divide into two categories: those with a criminal record (Category One), and first time off enders (Category Two). Recent research[7] suggests that 60% of cybercriminals fall into the former category: "those who have criminal tendencies to begin with […] then learn about using computers [and] figure out how to apply [them] to their trade".[8] For committed criminals, cybercrime is perceived as 'low-risk, high reward' without requiring sophisticated computer literacy.[9] YouTube channels and online forums offer guidance on how to initiate hacking and Distributed Denial of Service (DDOS) attacks: the recent Police and Crime Committee report concludes that extending criminal activity into cyberspace requires "no more skill than to be able to log on".[10] However, young people are digital natives. It is likely that, in future, those with criminal impulses will

[3] Warrell, Helen, 2015, 'Britain's crooks take criminal careers online', Financial Times [online]: http://www.ft.com/ cms/s/0/e3c8e486-ece7-11e4-a81a-00144feab7de.html.

[4] 6 King's Bench Walk seminar, 14th May 2015, 'Cybercrime: Facing the Legal Risk'

[5] Ibid.

[6] Bednarz, Ann, 2004, 'Profiling cybercriminals: A promising but immature science', Network World [online]: http://www. networkworld.com/article/2327820/lan-wan/profilingcybercriminals--a-promising-but-immature-science.htm

[7] Police and Crime Committee, 2015, 'Tightening the net: The Metropolitan Police Service's response to online theft and fraud' [online]: https://www.london.gov.uk/sites/ default/files/Tightening%20the%20net.pdf

[8] Bednarz, Ann, 2004, 'Profiling cybercriminals: A promising but immature science', Network World [online]: http://www. networkworld.com/article/2327820/lan-wan/profilingcybercriminals--a-promising-but-immature-science.htm

[9] Prince, Rosa, 2015, 'Traditional crooks including violent off enders turn to cyber crime', The Telegraph [online]: http://www.telegraph.co.uk/news/generalelection-2015/11579044/Traditional-crooks-includingviolent-off enders-turn-to-cyber-crime.html

[10] Police and Crime Committee, 2015, 'Tightening the net: The Metropolitan Police Service's response to online theft and fraud' [online]: https://www.london.gov.uk/sites/ default/files/Tightening%20the%20net.pdf.

be more inclined to turn to cybercrime earlier as their technological skills become sophisticated at a younger age and they feel instinctively comfortable within an online space. Keith Bristow, head of the National Crime Agency, predicts that the next generation of criminals will operate more or less exclusively online rather than "smashing windows and grabbing television sets". [11] No doubt this transition will present a serious and growing challenge to law enforcement agencies as the skills and expertise of the young continue to outstrip our policing capacity. Resources will need to be enhanced and redistributed. The current police tactic of targeting "potential young cybercriminals with home visits [and] letters to parents" is unlikely to sufficiently counter the threat.[12]

Young guns

The second category of cybercriminals arrive at the computer before they arrive at the crime. Again, reports show that these perpetrators subdivide into two categories: those with a dishonest intent to pursue an ill-gotten - often monetary - gain, and those who, in the experience of Branigan, "get into computers first and […] start hacking [through] curiosity".[13] Former Lulzsec hacker Ryan Ackroyd describes his trajectory: "I wanted to learn how computers worked. Then it snowballed out of control. It started with cheating in online games […] The next thing I know I'm breaking into services. It's addictive".[14] According to the Deputy Mayor for Policing and Crime, there are 28 organised cybercriminal groups in London who "specialise" in "banking and credit card fraud, account takeover, phishing, identity theft and payment card crime", all of which are "traditional" crimes within an online space.[15] The second subgroup are more interesting, and are broadly defined by their thirst for recognition (if not actual identification) and their disassociation from traditional criminality. Whilst the success of the committed cybercriminal lies in their ability to fl y under the radar (the widely publicised JPMorgan hack was enabled by malware that lay undetected in the bank's computer system for months, gradually harvesting the data of 76 million clients), hacks that are ethically or politically motivated are often measured by the publicity they attract.[16] Hacks, like terrorist attacks, are "claimed" by particular "hactivist" groups in order to further their cause. Hactivism is championed by its perpetrators as a disrupting force against existing power structures: "for the young and disillusioned, it's an effective way to lash out at the system, be it video game companies employing unpopular business models, or governments that teenagers feel powerless to [influence] in any other way".[17]

Here is a short list of great hackers of the world.

The most famous hacker in the history is Kevin Mitnick. At the tender age of 17 in 1981, he hacked into a phone exchange that allowed him to redirect subscriber calls in any way he wanted. In 1983, he accessed a Pentagon computer. In 1990s, he cracked/hacked/broke into the computer systems of the world's top technology and telecommunications companies like Nokia, Fujitsu, Motorola and Sun Microsystems. He was arrested by the FBI in 1995 and later released on parole in 2000.

Gary McKinnon, an Englishman, was arrested in November 2002 on the accusation that he had hacked into more than 90 US military computer systems in the U.K.

Vladmir Levin, a Russian computer 'expert' is said to be the first to hack a bank to steal money. In early 1995, he hacked into Citibank and robbed US$ 10 million. He was arrested by Interpol in the U.K. in 1995, after he had transferred money to his accounts in the US, Finland, Holland, Germany and Israel.

A Los Angeles radio station announced a contest that would reward the 102nd caller with a 'Porsche 944S2'. Kevin Poulsen took control of the entire city's telephone network and ensured he was the winner being the 102nd caller. He also hacked into 'Arpanet' that was the precursor to the Internet. Arpanet was a global network of computers.

---

[11] Peachey, Paul, 2015, ''World of Warcraft' fraudsters: cybercrime chief warns of new threat', The Independent [online]: http://www.independent.co.uk/news/uk/crime/worldof-warcraft-fraudsters-cybercrime-chief-warns-of-newthreat-10030202.html

[12] Ibid.

[13] Bednarz, Ann, 2004, 'Profiling cybercriminals: A promising but immature science', Network World [online]: http://www. networkworld.com/article/2327820/lan-wan/profilingcybercriminals--a-promising-but-immature-science.htm

[14] 6 King's Bench Walk seminar, 14th May 2015, 'Cybercrime: Facing the Legal Risk'

[15] Police and Crime Committee, 2015, 'Tightening the net: The Metropolitan Police Service's response to online theft and fraud' [online]: https://www.london.gov.uk/sites/ default/files/Tightening%20the%20net.pdf

[16] Business, 2014, 'JP Morgan sees 76 million customer accounts hacked', BBC [online]: 'JP Morgan sees 76 million customer accounts hacked': http://www.bbc.co.uk/news/ business-29470381

[17] Parkin, Simon, 2014, 'Inside the mind of Derp, a hacking group with a taste for cyber chaos', Th e Guardian [online], http://www.theguardian.com/technology/2014/aug/28/ derp-inside-hacking-group-cyber-attacks-phantomlord

US based hacker Timothy Lloyd planted a malicious software code in the computer network of Omega Engineering which was a prime supplier of components to NASA and the US Navy. Omega lost US$10 million due to the attack by which its manufacturing operations were impaired.

Cyber Crimes related to Finance

The Price Waterhouse Coopers organization, which deals with the economic crime survey, has defined economic crime in cyber world as "an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cyber crime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."[18] According to the findings of survey on Economic Crime in India in Global Economic Crime Survey 2011. The use of the internet in India is growing rapidly. According to a recent Telecom Regulatory Authority of India (TRAI) survey, we currently have 354 million internet subscribers.[19] While burgeoning growth in the use of internet provides multiple options to cyber citizens in all possible spheres from entertainment to education, it has also given rise to cyber crime. This new breed of tech-savvy fraudsters poses a new set of challenges. 24% of the respondents, who reported economic crime, have experienced cyber crime in the last 12 months. We believe that this data alone shows how serious the risk of cyber crime is to organizations. In the background of the recent incidents of cyber crime on multinational companies and financial institutions, a greater number of organizations are becoming victims of cyber crime. One potential reason that may explain this sudden rise in cyber crime is the rise in the volume of e-business, greater penetration of internet and e-commerce.

Economic crime does not discriminate. It is truly global. No industry or organization is immune. We have seen that despite fraud being a serious business issue, 10% of the respondents in 2011 as compared to 6% in 2009 was not aware if their organization has been a victim to economic crime in the last 12 months. The reason for awareness levels being low can be attributed, to an extent, to the frequency of performing fraud risk assessment. One third of the respondents to the survey do not perform fraud risk assessment due to a perceived lack of value. This trend is exposing more organizations to the risk of fraud. The fallout isn't just the direct costs: economic crime can seriously damage employee morale, brands or tarnish reputation, leading organizations to lose market share. As society becomes less tolerant of unethical behaviour, businesses need to make sure they are building – and keeping – public trust. Today, most people and businesses rely on the internet and other technologies. As a result, they are potentially opening themselves up to attacks from criminals anywhere in the world. Against a backdrop of data losses and theft, computer viruses and hacking, this survey looks at the significance and impact of this new type of economic crime and how it affects businesses worldwide. Cyber crime ranks as one of the top four types of economic crime. More than half (58%) perceive Information Technology department as a high risk department with respect to committing cyber crime. The Financial Cybercrime includes cheating, credit card frauds, money laundering, forgery, online investment frauds etc. such crimes are punishable under both IPC and IT Act. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts. Most cases involving computer related fraud have been prosecuted under existing criminal legislation and this has been adequate to cope with these offences.

Impact of Ethical Hacking

Ethical Hackers systematically attempt to penetrate a computer system or network on behalf of its owners. Their sole purpose is to find security vulnerabilities that a malicious hacker could potentially exploit. In the past companies used to rely on the basic built-in security of the system, to prevent attacks. But this approach is no longer effective and sensible. The skills of the attackers as well as the variety of tools in their arsenal make a static security system obsolete. The system must steadily keep getting better with the help of a helpful White Hat hacker in order to weather the new and innovative attacks. Ethical Hacking to strengthen system security has become one of the most essential parts of software development life cycle. Cyber Laws strongly recommend inclusion of a cyber security team, with a White Hat Hacker in it, in a Software Development Team, when the said software would be dealing with public data. The practice of Ethical Hacking has allowed the evolution of security systems at an unprecedented rate. But if the allegiance of the employed ethical hacker is compromised, then the company in question stands to lose a lot. This is an issue, along with the presumable incompetence of the hired hacker that companies must always be mindful about. The sense of never truly being safe is prevalent, with respect to their cyber properties and rights.

[18] As defined in the Global Economic Crime Survey 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer

[19] http://www.trai.gov.in/.

As the system security steadily improves, the attackers themselves improve their attacking techniques, by coming up with new and innovative attack strategies. They continuously persevere to find new vulnerabilities in the system's security. This makes the job of ethical hackers a perpetual cycle of system protection from the endlessly developing attacks. According to surveys conducted by cyber security firms in the country, Indian firms lost more than $4 billion in 2013 alone because of hackers. With more and more companies entering the e-commerce ecosystem and adopting new technologies like cloud computing, the threat from imminent security breaches is clearly demanding the need for efficient information security systems. The rising threat from cyber-attacks has exposed the severe shortage of talent in this sector. The demand for ethical hackers is at an all-time high. According to NASSCOM, 59% of organizations have vacant cybersecurity positions suggesting a shortfall of 1.5 million by 2020 globally. As per 2015 figures reported by NASSCOM, India needed more than 77,000 white hat hackers as against only a mere 15,000 certified professional ethical hackers in that year. This figures increases at an alarming rate with each year. This huge demand, in turn, has led to a sharp increase in the pay package of professionals who can fit the cybersecurity roles. Professionals are being paid anything from double their IT salaries to 10 times the average salary of an IT engineer to fill up this gap.

III. CONCLUSION

There can never be a perfect 'accounting for all reasons' theory for a new unconventional crime like hacking. As Katsh (1995) puts it, the emerging legal landscape in relation to cyberspace is not very easy to see and thus to understand the changes, it is necessary to "look beyond the surface of law" to recognize "so much that is hidden from view". These latent elements may contribute in structuring the laws and increase their efficacy by providing the missing policy links. A common thread running through all theoretical explanations is the system of 'rewards', both pecuniary and non-pecuniary, to the hackers. It is necessary to efface this system by limiting the ability of big corporations to hire notorious hackers for hefty benefits. Secondly, there is an urgent need to somehow regulate hacker communities operating on the internet. A separate online world has come into existence and governments need to divert their resources to check the growth of hacker cultures through prohibition of hacker magazines and websites. Though such a step may be accused of overreach but ultimately the social benefit will far outweigh the minimal inconvenience caused and in fact, right to speech and expression is subject to the need for social order and classes like 'hacktivists' who claim to represent the voice of subalterns in majoritarian societies cannot claim immunity from general law on moral grounds. Social learning theories emphasize on proper law enforcement as learning essentially takes place through imitation and reinforcements through rewards. Thirdly, there is a need to shed the 'one-size-fits-all' approach in devising punishment schedules as hacker motivations differ over a wide spectrum. Legal responses to crime are ineffective or prove to be worse if they do not account for the social context in which they are applied and are not careful about the social meaning that a particular penalty may convey in that context. A differential targeting of hacker classes, as Leeson & Coyne (2005) put it, will make the punitive law more effective and rationalized. Lastly, we live in an age of absolute moral uncertainty where no consensus exists about the definitions of right or wrong and the judgmental criteria to place any behaviour in either of the categories. Hacking produces rewards and seduces the youth and the lack of internal controls in form of ethical standards facilitates the commission. Thus, a suggested alternative strategy may include education concerning computer ethics at early stages of school to condition young minds. Active teaching through proper channels induces 'differentiation' capabilities paving way for responsible behaviour. On the whole, there is a need for behavioural sciences to focus more attention on hacking and uncover the distinct motivations for hacking through empirically verified propositions, which traditional criminological theories may not completely explain, and thus contribute towards increasing the efficacy of existing legal regime.

Selective References

Articles

[1]. Adamski, A. (1999), "Crimes Related to the Computer Network, Threats and Opportunities. A criminological perspective", retrieved from <http://www.ulapla nd.fi/home/oiffi/enlist/resources/HeuniWeb.htm> (Last accessed on July 10, 2007).

[2]. Ferrell, Jeff (1997), "Criminological Versthen: Inside the Immediacy of Crime", Justice Quarterly 14(1997), pp.3-23 at 12.

[3]. Fitch, Cynthia (2003), "Crime and Punishment: The Psychology of Hacking in New Millenium", retrieved from <http://www.giac.org /practical/GSEC/Cynthia_ Fitch_GSEC.pdf> (Last accessed on July 10, 2007).

[4]. Foster, David Robert (2004), "Can The General Theory Of Crime Account For Computer Offenders: Testing Low Self-Control As A Predictor Of Computer Crime Offending", retrieved from <https://drum.umd.edu/dspace/handle/1903

[5]. /1536> (Last accessed on July 10, 2007).

[6]. Grabosky, Peter (2000), "Computer Crime: A Criminological Overview", p.19, retrieved from <http://www.aic.gov.au/conferences/other/grabosky_peter/2000- 04-vienna.pdf> (Last accessed on July 10, 2007).

[7]. Himma, Kenneth (2005), "Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?", retrieved from <http://ssrn.com

[8]. /abstract=799545> (Last accessed on July 10, 2007).

[9]. Hollinger, R. (1988), "Computer hackers follow a guttman-like progression", Social Sciences Review, Vol. 72, pp.199-200.

[10]. Leeson, Peter T. & Coyne, Christopher J., "The Economics Of Computer Hacking", 1 J.L. Econ. & Pol'y 511(2005).
[11]. Lemos, Robert (2002), "New Laws Making Hacking a Black and White Choice", CNET News, retrieved from <http://news.com.com/2009-1001-958129.html> (Last accessed on July 10, 2007).
[12]. Rogers, Marcus (2000), "Psychological Theories of Crime and Hacking", retrieved from <http://homes.cerias.purdue.edu/~mkr/> (Last accessed on July 10, 2007).
[13]. Rogers, Marcus (2001), "A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study", University of Manitoba, Canada.
[14]. Rogers, Marcus (2002), "A New Hacker Taxonomy", retrieved from <http://homes
[15]. .cerias.purdue.edu/~mkr/hacker.doc> (Last accessed on July 10, 2007).
[16]. Spafford, Eugene H. (1992), "Are computer hacker break-ins ethical?" Journal of Systems and Software, 17(1), pp.41–48.
[17]. Still, Brian (2006), "Hacking for a Cause", ICFAI Journal of Cyber Law, Vol V, No.1, February, 2006, p.22.
[18]. Turgeman-Goldschmidt, Orly (2005), "Hackers' Accounts: Hacking as a Social Entertainment", Social Science Computer Review, Vol. 23, No. 1, pp.8-23, retrieved from <http://ssc.sagepub.com/cgi/content/abstract/23/1/8> (Last accessed on July 10, 2007).
[19]. Wible, Brent (2003), "A Site Where Hackers Are Welcome: Using Hack-In Contests To Shape Preferences And Deter Computer Crime", 112 Yale L.J. 1577 (2003).

Books

[20]. Gottfredson, M. R. & Hirschi, T. (1990), A General Theory of Crime, Stanford: USA.
[21]. Katsh, M. Ethan (1995), Law in a Digital World, Oxford University Press: New York.
[22]. Katz, Jack (1988), Seductions of Crime: Moral and Sensual Attractions in Doing Evil, New York: Basic Books.