LEGISLATIVE FRAMEWORK OF ETHICAL HACKING IN INDIA

Nishtha Wadhawan & J Tanisha, Amity Law School, Noida

ABSTRACT

Our modern lives in the computer age are a constant interplay between cybersecurity and cyberthreats. Hacking, where an unauthorised person enters a computer or network using his computer knowledge and skills, is the bitter truth of this era. In order to accomplish a goal that is deemed to be contrary to the creator's original intent, hackers modify or alter computer hardware and software. In contrast, ethical hacking entails discovering weaknesses and flaws in computer and information systems by imitating the goals and behaviours of malicious hackers. Within minutes, we receive updates from all across the world. However, the internet is keeping a plethora of our data with it in return. Furthermore, these data are open to abuse by an individual, a group of individuals, or an organisation. There are many ways to steal someone's data in the online environment for those with malice inclination. However, not all hacking is carried out with malice aforethought or animosity. Hacking can be carried out legally and with the intention of reducing or eliminating the risks associated with becoming the target of online harassment. Ethical hacking is lawful, but there is some disagreement about this. Malicious hacking has given the practise a terrible reputation over time, yet hacking was never meant to be a criminal activity. Hacking can be morally corrupt, yet it can also be morally right, legal, and acceptable. A number of laws have been passed to safeguard citizens' rights and keep internet transactions secure. India is placed third among nations that are facing the widest variety of cyber dangers. The same research also came in second place for focused attacks. Considering these facts, it is far from justified to downplay the necessity and significance of ethical hacking in the current legal climate. Ethical hackers need to be aware of the numerous laws and regulations that have been implemented by our government.

Keywords: Cybersecurity, ethical hacking, information systems, malicious, lawful.

Introduction

Hacking is the process of taking control of an organization's system without the users' awareness. To steal private information that is available on a network, such as credit card numbers, phone numbers, home addresses, bank account details, etc., is referred to as breaking security. This demonstrates how security is a discipline that safeguards the availability, confidentiality, and integrity of resources. It refers to this time period as the "Security Era" owing to the greatest demand for security rather than because we are particularly concerned about it.[1]

In reality, ethical hackers are computer programmers who utilise their abilities in a positive way to assist government authorities or organisations in protecting and preventing any damage to the network security. Hacking has traditionally been associated with negative implications. In reality, ethical hackers—also known as crackers—are the ones that deter cybercriminals. In the modern world, where technology is developing quickly and cybercrimes are following suit. The role of ethical hackers has become extremely important in the fight against cybercrime.

Data security is a big problem in the modern world since the internet is expanding so quickly and so much data is being transferred online. The danger to data security has increased as a result of the increased digitalization of many operations, including banking, online transactions, online money transfers, and online sending and receiving of many types of data.

Concept of Hacking

Finding weak points or security gaps in computer systems or networks and exploiting them to access data without authorization or modify the characteristics of the target computer systems or networks is known as hacking. Hacking is the term used to describe the alteration of computer networks, software, or hardware in order to achieve objectives that are not in line with user objectives. In contrast, it is also referred to as breaching security and stealing a person's private or confidential information, such as their phone number, credit card information, address, online banking passwords, etc.

In the popular media, a person who uses bugs and exploits to breach another person's security, or who uses his professional knowledge to engage maliciously or destructively, is referred to

[1] Kumar Utkarsh, "System Security and Ethical Hacking", 1 *International Journal of Research in Engineering & Advanced Technology* 1, (2013).

as a "hacker." The hardware and software experts in computers are hackers. A hacker is an expert in programming languages, networks, security, and computers in general. He is the type of person that enjoys learning new technologies, computer system specifics, and improving his capabilities and talents.

An ethical hacker, sometimes known as a **"white hat hacker",** is a computer security expert who penetrates protected networks or computer systems of a business or organisation to identify defects and fixes them to increase security. Before hostile or bad hackers uncover the organisation and cause any harm to the business or the organisation, white hat hackers use their skills and knowledge to protect it. White Hat hackers are the approved individuals in the field; even if the techniques they use are identical to those of bad hackers, they are allowed to do so by the group or business that hired them.[2]

Rules of Ethical Hacking

- The hacker is required to follow the ethics of hacking. It would be risky for the company if they didn't adhere to the rules.
- Execute strategy: Patience and time are more crucial for ethical hackers.[3]
- The organisation must be the ethical hacker's primary goal, not for them to be harmed.
- Because privacy is the main issue for an organisation, ethical hackers must keep their activities hidden because they could be used for dangerous or criminal purposes.[4]

Benefits of Ethical Hacking

Benefits include combating malicious hacking as well as threats to national security. The advantages include:

- It helps us to take preventive action against hackers;
- It helps to build a system which prevents any types of penetration by hackers;
- Ethical hacking offers security to banking and financial establishments;

[2] Aman Gupta & Abhineet Anand, "Ethical Hacking and Hacking Attacks*"* 6 *International Journal of Engineering And Computer Science* 21042-21050 (2017).
[3] K Bala Chowdappa, S.Subba Lakshmi & P.N.V.S.Pavan Kumar "Ethical Hacking Techniques with Penetration" 5 (3) *International Journal of Computer Science and Information Technologies* 3389-3393 (2014).
[4] Deepak Kumar, Ankit Agarwal & Abhishek Bhardwaj, "Ethical Hacking" 4(04) *International Journal of Engineering and Computer Science* 11466-11468 (2018).

- It helps to identify and close the open holes in a computer system or network.[5]

Limitations of Ethical Hacking

Every perk has its drawbacks, just like every coin has two sides. The risks of ethical hacking include the following:

- It could damage an organization's files;
- Information obtained could be used maliciously. Therefore, reliable hackers are required for this system to work;
- Hiring these individuals would increase the company's costs; and
- The method may jeopardise someone's privacy.

Work Plan of an Ethical Hacker

The following steps are involved in an ethical hacker's work:

1. Following the Ethical Hacking Tenets: There are a few fundamental rules that every ethical hacker must adhere to. Things could go wrong if he does not follow. The majority of the time, when creating or carrying out ethical hacking tests, these guidelines are disregarded or neglected. The outcomes are even quite risky.

2. Working ethically: By working with strict professional values and ethics, the term "ethical" is meant. Everything you do as an ethical hacker must be approved and must serve the company's objectives, whether you're conducting testing against your own systems or for someone who has hired you. No underlying motives are permitted. The ultimate goal is to be trustworthy. Information misuse is not at all acceptable.

3. Respecting Privacy: Show the data you collect the utmost deference. You must keep all information you discover confidential, including clear-text passwords and Web application log files.

4. Avoiding system crashes: One of the biggest errors individuals make is crashing their own

[5]Shivanshi Sinha & Dr. Yojna Arora, "Ethical Hacking:The Story of a White Hat Hacker" 8 *International Journal of Innovative Research in Computer Science & Technology* 131-136 (2020).

systems when they attempt to hack them. Ineffective planning is the main cause of this. These testers either failed to read the manual or had a poor understanding of the capabilities and applications of security tools and methodologies. When testing, it's simple to make life terrible for your systems. System lockups are frequently caused by running too many tests on a system too soon. Many security assessment solutions allow users to choose how many tests are run simultaneously on a system. If you need to conduct the testing on the production systems during regular business hours, these tools will come in particularly handy.

5. Implementing out the plan: It takes time and patience to hack ethically. When conducting your ethical hacking testing, exercise caution.[6]

Evoloution of Ethical Hacking

Around 1960, at MIT, the first hacking incident occurred, giving rise to the term "hacker." The market had accepted the internet by the year's end in 1980. People had started using the internet for their businesses, and there were now advertisements, e-commerce, and other web-based enterprises. This time, people were also concerned about hackers because if the system were compromised, they might lose control of sensitive data relating to the company's clients, employees, and business partners. So, at that point, people began to recognise the value of ethical hackers and considered employing a computer professional who could access their systems with their consent but wouldn't do any harm, preferring to assess the system's security and alert them to any weaknesses. Penetration testing is another name for ethical hacking. They would also offer guidance on how to apply those remedies. The United States Military carried out initial ethical hacks to assess their operating systems and decide whether to use a two-level (secret/top secret) classification system.[7]

Legality of Ethical Hacking in India

The terms hacking and ethical hacking should not be used interchangeably, it is important to note before diving into the laws of ethical hacking. Hacking is considered a felony in India, although ethical hacking has not been specifically addressed by Indian law. Although it is a

[6] Deepak Kumar, Ankit Agarwal & Abhishek Bhardwaj, "Ethical Hacking" 4(04) *International Journal of Engineering and Computer Science* 11466-11468 (2018).
[7] Lokesh Vyas, "Legality of ethical hacking in India", (May 31, 2018) *available at:* https://blog.ipleaders.in/legality-of-ethical-hacking-in-india/

rapidly expanding area, ethical hacking is currently not widely used in India.[8]

Governments and businesses have started using a method to address the issue of network security in which computer security experts break into their systems to evaluate their security. This method is a component of an information risk management programme that ensures higher security.

Since ethical hacking lacks mens rea, or evil intent, which is a necessary element in any crime, it is not a crime. An ethical hacker must go by a set of rules, including getting permission from the computer system's owner, respecting the privacy of the organisation or person disclosing the identified flaws, and notifying the proper hardware and software providers of the reported flaws.[9]

As long as the owner of the specific network gives his or her consent, it is legal. The subject of ethical hacking is taught in a number of colleges. However, it can be difficult to teach ethical hacking as a course because no one can be confident of the students' motives for enrolling in it. Their objective is the only thing that can set them apart from cybercriminals.

A number of laws have been passed to safeguard citizens' rights and keep internet transactions secure. Ethical hackers need to be aware of the numerous laws and regulations that have been implemented by our government, such as the Information Technology Act of 2000. The information act of 2000 was primarily passed to protect the security of data that was exchanged and made available online.

Sections 43 and 66 of the Information and Technology Act of 2000 address a variety of cybercrimes perpetrated in the nation, including hacking. However, because ethical hacking is now accepted, the term "hacker" was dropped in 2008.

The Information Technology Act of 2000's Section 43 addresses fines and financial compensation for computer system damage. In the event that the data is not protected, corporate entities are responsible under Section 43A of the IT Act, which also addresses the appropriate damages to be paid. When the intent or liability of the cracker to damage the system or steal any crucial information is established, criminal culpability for cracking ensues. If the cracker

[8] Dr. B. Mahammad Rafee & Prof. Shuaib Ahmed Shariff, "Good and Bad about Ethical Hacking in Indian Perspective" 5(2) *International Journal of Technical Research & Science* 12-18 (2020).
[9] Jas Singh, "Hacking Legal or Illegal? (Ethical Hackers Hactvists)", (Sept. 15, 2021) *available at:* https://cybersecuritykings.com/2021/05/27/hacking-legal-or-illegal-ethical-hackers-hacktivists/.

simply violates the system without intending to cause harm, it is largely a civil liability under section 43A. However, legal trespass can lead to other criminal behaviours that are punishable under the Indian Penal Code, such as computer theft, which is penalised under section 376.[10]

Anyone who tries to violate the laws outlined in Section 43 of the Information Technology Act and is found to be dishonest or fraudulent will be sentenced to three years in prison, a fine of five lakh rupees, or both. Any hacker who violates or makes an effort to compromise an organization's confidentiality and privacy is subject to punishment under section 72 of the Information Technology Act of 2000, according to section 66 of that law.

Even if ethical hacking is not specifically addressed by Indian law, it is nevertheless a crime here. Hacking is against India's law system's fundamental principles. Moral hacking enjoyed a neutral status under Indian criminal law because it was no longer directly addressed by Indian laws. It is explained in detail as follows:

A. Constitutional Conflict

According to constitutional principles, hacking violates Article 21, which deals with the right to life and private liberty, including the right to live with dignity. Additionally, hacking violates an individual's right to privacy, which is considered a fundamental right. A criminal offence must have two elements in order to be considered valid.

1. mens rea i.e. Bad aim
2. actus reus i.e. Bodily act.

Moral hacking lacks the first and most important component, known as mens rea, hence the issue of whether it is a crime does not come up. Moral hacking is also essential because it is done with the goal of keeping you from hacking. Trespass is mostly split into two portions, in particular.

1. Trespass to the person, and
2. Trespass to assets.

Trespassing is generally understood to be an unwanted entry into another person's property without that person's consent. Trespassing is wrong under both civil law and criminal law, or both branches of the law. In contrast to criminal law, civil law disregards the importance of the

[10] Kritika Jain, "Ethical Hacking and its Legality", (Oct. 10, 2017) *available at:* https://legaldesire.com/ethical-hacking-legality/.

goal. The sole crime that is frequently associated with moral hacking is the wrong of trespass, but it is more accurately related to hacking than ethical hacking.

B. Civil Law

Trespassing is the legal term for invading someone else's property without that person's consent. It is founded on the case laws and is a part of the Law of Torts, which is an unaltered law. However, as the law of torts only applies to tangible possessions, neither hacking nor ethical hacking are covered by it. In support of this, moral hacking no longer entails any legal obligation because it is done with the owner's permission, hence the argument that it is a civil wrong will never be raised.

C. Criminal Law

Trespass is a criminal offence in India and is covered in great detail under section 441 of the Indian Penal Code (IPC), 1860. Trespassing is defined as intentionally entering someone else's property with the intent to cause harm or to intimidate the property owner. In this case, it is not clear exactly what types of assets would constitute trespassing. Trespassing is a transgression that affects both tangible and intangible property. Hacking is entering a computer device that is an intangible asset. The presence of physical incursion and physical harm is not always necessary to establish legal liability for trespass. These days, computers, software, and websites are all considered to be property. Phrases like "homepage," "tour of a website," "area," "viewing a website," and many others. are utilised throughout the global internet; this demonstrates that the websites are owned. Therefore, any uninvited intrusion that has bad intentions might be viewed as a type of criminal trespass. The act of ethical hacking lacks all the necessary components, such as a motive to commit an offence or to frighten, offend, or annoy someone; as a result, it is not criminal and carries no legal ramifications.

D. Information Technology Act, 2000

The Information Generation (IT) Act, 2000 is a landmark in the field of cyber law and a turning point in Indian legal history. If we carefully examine the provisions of the IT Act, we can infer that it includes almost all of the wrongs that result from hacking because hacking is a very broad offence that can include many other offences, such as. When someone hacks into another person's computer, their personal information may be exposed, they may be forced to pay money, a black hat hacker may use the knowledge to further his or her own interests, and so forth.

The act of hacking is specifically addressed in Chapter XI Section 66 of the IT Act, 2000. Any person who commits any of the unlawful or fraudulent acts listed in Section 66(1) is referred to as a hack, and Section 66(2) lays out the associated penalties. In India, hacking is a crime that carries a sentence of up to three years in prison, a fine of up to 2 lakh rupees, or both.

A punishment is outlined in Chapter IX Section 43 of the IT Act of 2000 for damage to a computer or computer device. It is a typical event that occurs whenever a computer device gets compromised. Black hats damage the system they hack and steal the data. There are numerous activities included in this enumerative provision.

The specified act's Chapter XI Section 65 defines tampering with laptop source files as a crime. The invasion of confidence and privacy is a crime under Section 72 of the Equal Chapter. The most frequent result of hacking is this.

Since ethical hacking lacks the mala fide, or intended, harm that is required by the aforementioned regulations, moral hacking isn't always illegal in India. According to safety software company Symantec, India is placed third among nations that are facing the widest variety of cyber dangers. The same research also came in second place for focused attacks. Considering these facts, it is far from justified to downplay the necessity and significance of ethical hacking in the current legal climate. It is illegal to hack a networking device in this way, and you have to abide by certain rules. In a sense, the act is justified because the relevant regulations were followed. Furthermore, moral hacking requires the consent of the device's owner and is carried out in accordance with the law, which further enhances the case against moral hackers.[11]

The technology of the internet and internet of things characterise the era we currently live in. A laptop computer serves as a home to an infinite number of data and accounts, making chance omnipresent. Due to this massive data storage, our computer system needs to be updated on a regular basis, and necessary steps must be made to prevent black hats from obtaining such information.

Conclusion

As internet usage advances, everyone becomes reliant on it and stores their most vital and

[11] Dr. B. Mahammad Rafee & Prof. Shuaib Ahmed Shariff, "Good and Bad about Ethical Hacking in Indian Perspective" 5(2) *International Journal of Technical Research & Science* 12-18 (2020).

crucial data online. Essentially, this is an invitation to "crackers" to acquire access to information. Security is therefore the organization's main issue. This demonstrates how crucial ethical hackers are. The company recruits knowledgeable, skilled ethical hackers for this reason. There is no legal definition of ethical hacking in India. Only after having a conceptual grasp of the laws that regulate hacking can its legality be determined. It can be said that ethical hacking is legal in India after being put to the test using criteria from both civil law and criminal law. crimes such as phishing, credit card fraud, bank robbery, illegal downloading, industrial espionage, child porn, kidnapping children through chat rooms, scams, cyber terrorism, production and/or distribution of viruses, spam, and so forth. As a result, instances involving cybercrimes, the theft of millions of rupees from banking servers, and reported online money frauds are still pending in the courts. The government must act immediately to protect the resources by upholding moral principles. Hacking is without a doubt a big challenge to the online world. In the nation, not many people are aware of this theft. More people in the nation need to be aware of hacking and cracking. Although the government creates strict regulations, they are not always enforced or known by the general public. Due to a lack of equipment and the fact that few individuals report small offences despite the severity of the punishment, the majority of hacking incidents go unreported. It is also highly challenging to find a virtual hacker. It becomes challenging for the police to track him down and prosecute him in another country because hacking can occur anywhere in the world. To deter others from engaging in such behaviours, the punishment can also be a little harsher.

Bibliography

Articles:

1. Kumar Utkarsh, "System Security and Ethical Hacking", 1 *International Journal of Research in Engineering & Advanced Technology* 1, (2013).

2. Aman Gupta & Abhineet Anand, "Ethical Hacking and Hacking Attacks" 6 *International Journal of Engineering And Computer Science* 21042-21050 (2017).

3. K Bala Chowdappa, S.Subba Lakshmi & P.N.V.S.Pavan Kumar "Ethical Hacking Techniques with Penetration" 5 (3) *International Journal of Computer Science and Information Technologies* 3389-3393 (2014).

4. Deepak Kumar, Ankit Agarwal & Abhishek Bhardwaj, "Ethical Hacking" 4(04) *International Journal of Engineering and Computer Science* 11466-11468 (2018).

5. Shivanshi Sinha & Dr. Yojna Arora, "Ethical Hacking:The Story of a White Hat Hacker" 8 *International Journal of Innovative Research in Computer Science & Technology* 131-136 (2020).

6. Lokesh Vyas, "Legality of ethical hacking in India", (May 31, 2018) https://blog.ipleaders.in/legality-of-ethical-hacking-in-india/

7. Dr. B. Mahammad Rafee & Prof. Shuaib Ahmed Shariff, "Good and Bad about Ethical Hacking in Indian Perspective" 5(2) *International Journal of Technical Research & Science* 12-18 (2020).

8. Jas Singh, "Hacking Legal or Illegal? (Ethical Hackers Hactvists)", (Sept. 15, 2021) https://cybersecuritykings.com/2021/05/27/hacking-legal-or-illegal-ethical-hackers-hacktivists/.

9. Kritika Jain, "Ethical Hacking and its Legality", (Oct. 10, 2017) https://legaldesire.com/ethical-hacking-legality/.

Statutes:

1. Constitution of India

2. Indian Penal Code, 1960

3. Information Technology Act, 2000