Journal of Inventive and Scientific Research Studies (JISRS)
www.jisrs.com Vol: II, Issue: 1 June 2024 ISSN: 2584-0630 (Online)

CYBERCRIME AND CYBERSECURITY: RETHINKING THE ROLE OF ETHICS

Ugwunnadi Charles Chukwudi[1*], Chukwuma Joseph Nnaemeka[2]

[1]Department of Philosophy, University of Nigeria, Nsuka.
E-mail: Charles.ugwunnadi.189808@unn.edu.ng
[2]Department of Philosophy University of Nigeria, Nsuka.
E-mail: Nnaemeka.chukwuma@unn.edu.ng

Received: May 04, 2024, **Accepted**: May 30, 2024, **Online Published**: June 15, 2024

ABSTRACT

Due to the increased dependence on the internet, cybercrime and cybersecurity have become a crucial issue for individuals, business organizations, and governments all over the world. As technology continues to evolve, so do the threats posed by cybercriminals who are always on the lookout to exploit vulnerabilities in networks and systems. Since no network or system is 100% secured and all technical and technological solutions developed to tackle cybercrime are not sufficient, there is a growing recognition that ethical considerations must play a vital role in addressing cybercrime and enhancing cybersecurity. This paper examines the evolving landscape of cybercrime and cybersecurity and the role of ethics in mitigating the risks and consequences of cybercrime and enhancing comprehensive and robust cybersecurity. This paper argues that while technical and technological solutions are vital, they must be accompanied by ethical principles that guide individuals, business organizations, and government in making responsible decisions about their use of technology and what form of cybersecurity approach is best for them to adopt in responding to cyber-attack from cyber criminals. The paper adopts the qualitative method.

Keywords: Cybercrime, Cybersecurity, Ethics, Network, and Technology.

Introduction

In the contemporary digital era, marked by an enormous dependence on the internet and information technology, cybercrime and cybersecurity have become a herculean challenge for individuals, business organizations, and governments all over the world. As the world is getting highly interconnected due to technological advancement, the increase in cybercrime poses a formidable threat, exploiting the weaknesses and vulnerabilities in networks and computer systems. While technological and technical measures have been developed to fight these threats, they are not sufficient. This gives rise to the importance or indispensability of ethics and ethical principles in developing and implementing robust and comprehensive cybersecurity measures. The role of ethics and ethical principles in helping individuals, businesses, and government in decision-making relating to cybersecurity cannot be overemphasized.

Lillie (1984:1) defined "ethics as the normative science of conduct of human beings living in societies-a science which judges human conduct to be right or wrong, to be good or bad, or in some similar way." Ethics can be seen as a systematic study of human action. It is the study of what *ought to be* and not what is. This means that ethics is a prescriptive science and not a descriptive science. Ethics does not study human action to describe it; rather, it studies human action with the intention of passing a moral judgment, according to http://dcencompass.com.

Ethics refers to well-founded standards of what is right and wrong that prescribe what we ought to do when confronted with specific situations. The goal of ethics is not to dictate what professionals must do when faced with every ethical dilemma but to instill a strong sense of principle that govern behaviour or conduct.

The dynamic and ever-evolving nature of cybercrime makes the ethics and ethical frameworks indispensable in cybersecurity. This paper explores the role of ethics and ethical theories and principles in fighting cybercrime and equipping cybersecurity personnel with comprehensive ethical knowledge beyond mere technical solutions. Ethical principles are important guide-moral compass-that should guide cybersecurity personnel, individuals, business organizations, and government in making decisions on the appropriate way to react to cyber threats or attacks.

From the earliest recorded history, humanity has always sought guiding principles that would direct their actions and guide their relationship with one another in society. Different schools of thought aim to understand what makes human actions ethical and how people can make morally good choices. Deontologists, for example, emphasize the importance of duty in determining the morality or otherwise of an action.

Deontological ethics or deontology (Greek: δέον (deon) meaning 'obligation' or 'duty') is an approach to ethics that focuses on the rightness or wrongness of actions themselves, as opposed to the rightness or wrongness of the consequences of those actions (Olson, 1967:343)

The deontological school maintains that the intention of an action is what matters and not the consequences of the action. Anthony (1979:73) notes that deontological ethics is often distinguished from consequentialist or teleological ethical theories, which hold that action is determined by its outcome or consequences. In contrast, deontological ethics focuses on the inherent rightness or wrongness of action itself, regardless of its consequences.

One of the major proponents of the deontological ethical theory is Immanuel Kant. Kant (1780), in the preface to *The Metaphysical Elements of Ethics*, argues that moral rightness is achieved when individuals act in accordance with their duty, driven by a sense of moral obligation rather than a desire for specific outcomes. Kant believed that the moral value of an action is determined by the intention or motive behind it rather than its consequences. He maintained that for an action to be considered morally good, it must be motivated by a genuine willingness to do good, which he termed ‘goodwill.’ In Kant’s philosophy, goodwill is the only unconditional good, and it is the foundation of moral behaviour. Kant (1997:8) maintains that:

> Goodwill is the only thing to which we attribute unconditional value. Goodwill is not good because of what it affects or accomplishes, because of its fitness to attain some proposed end, but only because of its volition; that is, it is good in itself and, regarded for itself, is to be valued incomparably higher than all that could merely be brought about by it in favour of some inclination and indeed, if you will, of the sum of all inclinations.

Kant is of the view that “the consequences of an act of willingness cannot be used to determine that the person has goodwill; good consequences could arise by accident from an action that was motivated by a desire to cause harm to an innocent person, and bad consequences could arise from an action that was well-motivated."

Kant's deontological ethical theory can guide cybersecurity personnel in responding to cybercrime and cyberattacks. It emphasizes principles such as treating individuals with respect, upholding privacy, and acting according to universal moral law. This approach would encourage cyber defenders to act with goodwill in protecting individual's digital rights, maintaining the confidentiality of sensitive data, and acting in ways that can be generalized as ethical standards.

Nature and Scope of Cybercrime

Before we discuss the nature and scope of cybercrime, it is pertinent to define crime in its traditional sense. "Crime is a public wrong. It is an act of offense which violates the law of the state and is strongly disapproved by the society. Crime is defined as acts or omissions forbidden by law that can be punished by imprisonment or fine. Murder, robbery, burglary, rape, drunken driving, child neglect, and failure to pay taxes are examples of crimes. The term crime is derived from the Latin word "crimen," meaning offence and also a wrong-doer. Crime is considered as an anti-social behavior" Thotakura, (2011). Crime, according to Hagan (2014), is a socially harmful act or behavior that violates the norms, rules, and laws of a society and leads to legal sanction. Crime can be seen as any action or omission that contravenes the law of a given society, and it is punishable by the law.

From the above definitions of crime, it is obvious that the law ultimately determines what is and what is not a crime. Since nothing constitutes a crime unless the law prescribes it, then there is a challenge in defining cybercrime because most of the categories of cybercrime are still beyond the reach of the law. There is no consensus over what constitutes cybercrime. ? It is quite an arduous task to define cybercrime because of many reasons, including the rapidly evolving nature of technology, the global and interconnected nature of the internet, the various legal jurisdictional complexities involved, and the dynamic nature of cybercrime. Cybercrime is quite more dynamic and complex than traditional crime. It is quite difficult to track cybercriminals because they can easily adopt fake identities, and cybercrime is transnational.

In support of the above position, Chowbe (2011) posits that It is easy to detect and track criminal activity in traditional society, but it is quite difficult to do such in cyberspace because it is difficult to identify the perpetrator/s in cyberspace as it is very simple to mask a fake identity.

Chowbe (2011) notes that nothing is a crime unless prescribed by the law. However, most cybercrime categories are beyond the reach of law. He further notes that there is no unanimous consensus over what constitutes cybercrime.

Aghatise (2006) defines cybercrime as a crime performed on the internet using the computer as either a tool or a targeted victim. "Cybercrimes are offenses that are committed against a group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as the internet (chat rooms, emails, notice boards, and groups) and mobile phones" Halder and Jaishanker (2011). Such crime can harm individuals, groups, business organizations, properties, and even the government of a country. Cybercrime can easily be defined as any crime activity orchestrated in cyberspace that harms individuals, business organizations, or the government. Ekeji (….) defines cybercrime as "those criminal acts either committed entirely on cyberspace, such as various forms of identity theft and bank frauds or acts that have a physical component and are facilitated through the use of the internet-based tools. Such acts commonly include the distribution of fraudulent emails and child pornography on the internet, unauthorized access to computer files and theft of proprietary information, distribution of information housed with viruses and selling illegal objects and substances over the internet, and theft and forgery of identity". Pande (2017) defines cybercrime as "any unlawful activity in which computer or computing device such as smartphones, tablets, Personal Digital Assistants (PDAs) e.t.c which are stand-alone or part of a network are used as a tool or/and target of criminal activity. It is often committed by people of destructive and criminal mindset either for revenge, greed or adventure".

Classification of Cybercrime

There is no consensus among scholars on the classification of cybercrime. Scholars classify cybercrime differently and for different reasons. Observing the difficulty in the classification and identification of cybercrime, www.wefinder24.com (2023) observes that:

Cybercrime has spread to such a proportion that a formal categorization of this crime is no longer possible. Every single day gives birth to a new kind of cybercrime, making every single effort to stop it an almost futile exercise.

Pandee (2017) states that cybercrime “could be internal or external to the organization facing the cyber-attack; hence, cybercrime could be categorized into two: internal and external attack. An internal attack on a computer system or network by some persons with authorized system access is known as an internal attack. It can also be seen as an insider attack. Dissatisfied or unhappy employees or contractors often carry it out”. The intention of an insider attack may include revenge or greed. It is relatively easier for “an insider to carry cyberattack as he/she is aware of the policies, process, IT architecture and weakness of the security system.”

An external attack occurs when the attacker is hired either by an insider or an external entity in the organization. Any organization that faces cyberattacks often faces financial loss and also loss of reputation.

Pandee (2017) further notes that cyberattacks can be categorized into structured and unstructured attacks, depending on the attacker’s level of sophistication. Some researchers classify these attacks as external attacks, but there are cases where an internal employee carries out a structured attack.

Unstructured attacks are typically carried out by inexperienced individuals who lack clear motivations to perform the cyberattack. Usually, these inexperienced individuals try to test a tool that is available on the internet on a random company’s network. Skilled and experienced professionals with defined objectives execute structured attacks. They utilize sophisticated tools and technologies to gain access to other networks without being detected by their Intrusion Detection Systems (IDSs). These attackers also have the requisite knowledge to develop and enhance the existing tools to meet their purpose.

According to www.wefinder24.com, cyber-crime can be basically classified into three parts:

i. Cybercrimes against persons.
ii. Cybercrimes against property.
iii. Cybercrimes against the government.

Cybercrimes against persons: these are cybercrimes committed against individuals. It includes various crimes like transmission of child pornography and harassment of someone with the use of a computer such as email. This type of cybercrime involves an individual distributing malicious or illegal information online. Cybercrime via e against individuals includes harassment via Email, cyberstalking, identity theft, cyberbullying, phishing, etc.

Harassment via Email involves harassing people by sending them letters, attachment files, and folders through Email. It is common in social media such as Twitter, Facebook, TikTok, WhatsApp, and many more.

Cyberstalking involves the use of the internet, phone, and other electronic communication devices to stalk another person. Kharat (2017) notes that cyberstalking is an expressed or implied physical threat that creates fear through the use of computer technology such as the internet, email, phones, text messages, webcam websites, or videos.

Identity theft is when an individual or a group of individuals uses another person's personal data or financial data for monetary or other personal gain.

Identity theft is a crime in which an imposter obtains key pieces of personal identifying information (PII), such as social security numbers and driver's license numbers, and uses them for their gains. Younes.

Identity theft also involves a fraudster or an imposter using someone's picture and name on the internet to defraud unsuspecting people. People can easily create an account with the picture of a known politician, celebrity, or religious leader and also use such an account to scam and defraud people. An imposter can also use the identity of a company, an institution, or a group for fraudulent activities.

Cyberbullying is a form of cybercrime that involves bullying or harassing people using electronic means. Cyberbullying is often called online bullying. It involves sharing private or personal information about someone to embarrass or humiliate them. Cyberbullying aims to make victims feel less of themselves.

Phishing involves tricking people into giving out their identity, bank account numbers, passwords, etc, over the internet or by email with the intention of using this information to steal their money.

Cybercrime against property

Cybercrime against property refers to criminal activities that are committed online and target property such as digital assets or physical computers, networks, or other digital technologies with the intention of causing damage. Cybercrimes against property include the following:

Hacking: hacking is having unauthorized access to a computer system or network with the motive of stealing sensitive information, causing damage or disruption, or taking control of the system.

Malware attacks: malware attacks involve the use of damaging software such as viruses, worms, or Trojan horses to infect a computer system or network and steal data or cause serious damage.

DDOS attacks Distributed Denial of Service (DDOS) attack is a kind of cyberattack where a multiple number of compromised systems known as botnets are used to invade a targeted website or network with traffic, making it unavailable to users. The objective of a DDOS attack is often to overwhelm the target server, network, or website with traffic, making it crash or become unavailable.

Cybercrime against government

Cybercrime against government refers to illegal activities carried out on the internet with the intention to compromise or disrupt the operations, systems, or data of government entities.

Cyberterrorism refers to the use of cyber attacks and digital tools to instill fear, cause panic, disrupt critical infrastructure, or promote ideological, political, or religious agendas. It involves leveraging technology to carry out acts of terrorism on the internet, with potential real-world consequences. It involves individuals threatening the government through the Internet. It also involves terrorizing citizens of a country over the internet. It also involves hacking into a government or military-maintained site.

What is cybersecurity?

Cybersecurity is the act of protecting computer systems, networks, software, and data from cyber threats, including cyberattacks and cybercrime. It involves a multifaceted range of “technologies, processes, and practices designed to safeguard digital information and prevent unauthorized access, data breaches, and other malicious activities.”

Approaches adopted by cybersecurity personnel to tackle cyberattacks and cybercrime:

Risk Assessment and Management: Cybersecurity professionals often start by identifying potential vulnerabilities and threats through risk assessments. They evaluate the possible impact of different cyberattacks and concentrate resources based on the level of risk.

Firewalls and Intrusion Detection/Prevention Systems: Firewalls serve as a block between a trusted internal network and untrusted external networks, dictating incoming and outgoing network traffic. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) track network traffic for suspicious activities and can automatically stop or notify about possible threats.

Secure Network Architecture: Designing a secure network architecture involves segmenting networks, implementing strong access controls, and using techniques like VLANs (Virtual LANs) to isolate sensitive data from potential attackers.

Encryption: Data encryption ensures that even if attackers gain access to sensitive data, it remains unreadable without the proper decryption key. This includes both data in transit (communication between devices) and data at rest (stored data).

User Authentication and Access Control: Implementing strong authentication methods such as multi-factor authentication (MFA) ensures that only authorized users can access systems and data. Access control mechanisms limit what users can do based on their roles and privileges.

Patch Management: Keeping software and systems up to date with the latest security patches is important. Cybersecurity professionals constantly update software to tackle known vulnerabilities that attackers could exploit.

Security Awareness Training: Cybersecurity personnel educate employees and users about best practices, such as recognizing phishing emails, using strong passwords, and not sharing sensitive information.

Incident Response Planning: creating a detailed incident response plan aids organization in effectively responding to security breaches. It shows steps to be taken when a breach occurs, including detecting the breach, containing it, recovering affected systems, and learning from the incident to block similar occurrences in the future.

Threat Intelligence: Being informed about recent threats and attack techniques is vital. Cybersecurity personnel use threat intelligence services to understand emerging threats and adapt their defenses accordingly.

Vulnerability Management: Regularly scanning systems for vulnerabilities and weaknesses is vital. Cybersecurity professionals detect and remediate loopholes before attackers exploit them.

Advanced Security Tools: These can include intrusion detection systems, anti-malware software, security information and event management (SIEM) tools, sandboxing, and more. These tools help in real-time monitoring and response to threats.

Penetration Testing: Organizations often hire ethical hackers to perform penetration tests. These tests simulate real-world attacks to detect loopholes and weaknesses in systems and processes.

Regulatory Compliance: Adhering to industry-specific regulations and standards helps organizations maintain a baseline of security. This may include GDPR, HIPAA, PCI DSS, and more.

Collaboration and Information Sharing: Cybersecurity professionals often collaborate within and across organizations, sharing information about threats and best practices to improve defenses collectively.

Why is Ethics Important in Cybersecurity?

There is an increasing agreement among scholars that ethics is of enormous importance to cybersecurity and cybersecurity personnel in technical fields and that it must be included in the language that cybersecurity personnel are conversant with.

What is the factor motivating this growing focus on the role of ethics in cybersecurity? What is the logic behind it? The reason behind this is that cyberspace and cybersecurity, to a great extent, influence how human beings seek to live a good life, and their success or otherwise significantly depends on the failure or success of cybersecurity personnel. According to https://www.sennovate.com

Ethics is of utmost importance when applied to cybersecurity, as seemingly unimportant actions can lead to consequences for the professionals and the organizations they work for. Thus, cyber security experts can figure out what is expected of them professionally by understanding the rules of ethical behaviour.

According to Vallor and Rewak, Cybersecurity practices "have as their aim the securing—that is, the keeping safe—of data, computer systems and networks (software and hardware). While those data, systems, and networks might have some economic or other value in and of themselves, what cybersecurity practices primarily protect are the integrity, functionality, and reliability of human institutions/practices that rely upon such data, systems, and networks. In protecting those institutions and practices, cybersecurity professionals, in turn, protect the lives and happiness of the human beings who depend upon them. This means that ethical issues are at the core of cybersecurity practices because these practices are increasingly required to secure and shield the ability of human individuals and groups to live well".

It is the moral responsibility of cybersecurity personnel to protect others who depend on cyberspace by being conscious of the choices they make in carrying out their job.

Kant's Deontological Ethical Theory and Contemporary Ethical Issues in Cybersecurity.

Harms to Privacy: Due to the enormous amount of personal and confidential data that individuals and institutions give out and generate, there is an ethical concern about how individuals and organizations use and generate this data.

The rapid growth of digital data generation and sharing has indeed led to increased vulnerabilities and risks to personal and organizational privacy. Most of us may know how open our lives and property are, or can be, by adopting a poor cybersecurity approach.

Cybercriminals, terrorists, governments, and other entities can exploit poor cybersecurity to monitor individuals' online activities without their consent, potentially violating privacy rights. An unethical cybersecurity approach creates an environment that is enabling harm to privacy.

In the context of the harm to privacy caused by poor and unethical cybersecurity practices, deontological ethics can guide how individuals and organizations should behave to uphold ethical standards and mitigate these issues.

Kantian deontological ethics emphasizes treating “individuals as ends in themselves, rather than a means to an end.” This principle can guide individuals and organizations to respect the privacy of others and refrain from exploiting their sensitive data for personal gain.

Kant's principle of universalizability encourages individuals to act according to maxims (principles) that could be consistently applied as a universal law. In the context of cybersecurity, this would mean adopting practices that everyone can follow without compromising their privacy or security. For example, individuals and organizations should use strong security measures and protect data as they would want others to do the same.

Kantian ethics shows the importance of fulfilling one's duties and obligations. In the context of cybersecurity, individuals and organizations have to protect the personal information entrusted to them by implementing rigorous security measures, regularly enhancing software, and being informed about potential threats.

Kantian ethics advocates for honesty and transparency in interactions. Applying this principle to privacy and cybersecurity involves being open about data collection practices, informing users about how their data will be used, and obtaining informed consent. Kantian ethics values individual autonomy and rationality. In the context of privacy, this means that individuals should have power over their data and the ability to make informed choices about its use. Organizations should respect users' choices regarding data sharing and provide mechanisms for opt-in and opt-out.

Hacking Back: Hacking back refers to the act of retaliating against cyber attackers by actively targeting and potentially compromising their systems or networks. This practice raises significant ethical and practical concerns within the field of cybersecurity.

Hacking back can be seen as a form of “digital vigilantism, where individuals or organizations take the law into their own hands.” This can lead to a chaotic and unregulated environment where conflicts escalate rapidly and without oversight.

Accurately attributing a cyber-attack to a specific entity is a complex task. It is quite difficult to determine the individual or organization behind any cyber-attack accurately, and hacking back without certainty about the attacker's identity can lead to innocent parties being targeted, causing harm and potential legal consequences. Hacking back can inadvertently affect innocent bystanders or unrelated systems and networks. This can result in significant disruptions and unintended negative consequences.

Hacking back can easily escalate cyber conflicts, leading to a tit-for-tat cycle of attacks. This escalation can cause greater damage to all parties involved, and it may be challenging to determine when to stop.

Kant’s deontological ethics provides a moral framework that can help analyze and address the ethical issues involved in hacking back.

According to Kant, one should act according to principles that could be universally applied without contradiction. When considering hacking back, one should ask whether hacking back could be consistently applied as a universal rule without leading to contradictions or chaos. If hacking back were universally practiced, would it lead to a sustainable and ethical digital environment, or would it result in increased harm, escalation, and ethical dilemmas?

Kantian ethics emphasizes treating “individuals as ends in themselves and not merely as a means to an end.” Applying this to hacking back, one should consider whether hacking back respects the autonomy, rights, and dignity of all parties involved. This includes considering potential collateral damage, the impact on innocent bystanders, and the potential violation of the privacy and autonomy of hackers themselves.

Recommendations

Cybersecurity professionals should carry out their duties and obligations to individuals, organizations, and governments ethically.

Cybersecurity professionals should be trained to converse with the ethical issues involved in their profession.

Ethical experts or ethicists should be involved in the process of developing technical approaches to cybersecurity issues.

There is a need to develop comprehensive ethical codes of conduct for cybersecurity experts.

Each emerging risk and cyberattack must be properly assessed in order to determine the appropriate approach for tackling it.

Conclusion

The role of ethics in cybersecurity cannot be over-emphasized. Ethical issues in cybersecurity are complex and dynamic. The discourse surrounding cybercrime and cybersecurity has gone beyond mere technical and legal considerations, delving into the intricate realm of ethics. This paper has explored the dynamic landscape of digital threats, the significance of robust and comprehensive security measures, and the imperative need to reevaluate the role of ethics within the domain of cybersecurity.

References

Antony, F. (1979). 'Consequentialism'. In A Dictionary of Philosophy, (2nd Ed.). New York: St Martins.

Chowbe, R.S. (2011). The Concept of Cybercrime: Nature and Scope in *Electronic Journal*. https://www.researchgate.net/publication/256008668_The_Concept_of_Cyber-Crime_Nature_Scope

DC Encompass. (2021). Cybersecurity ethics. Retrieved from https://dcencompass.com.au/blog/cybersecurity_ethics/

Ekeji, C. (n.d.). Cybercrime in Nigeria. Retrieved from https://www.academia.edu/4818858/Cyber_Crime_in_Nigeria

Hagan, F. E. (2014). Introduction to criminology: Theories, methods, and criminal behaviors. Sage Publications.

Halder, D., & Jaishankar, K. (2011). Cybercrime and the victimization of women: Laws, rights, and regulations. Information Science Reference.

Kant, I (1997) *Groundwork of the Metaphysics of Morals*. Cambridge University Press.

Kant, I. (1780). *The Metaphysical Elements of Ethics*. Kingsmill Abbot

Kharat, S. (2017). Cybercrime-A Threat to Persons, Property, Government and Societies https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2913438

Lillie, W. (1984). *An Introduction to Ethics*. Methuen and Co Ltd.

Olson, G. (1967), 'Deontological Ethics'. In Paul Edwards (ed) *The Encyclopedia of Philosophy*. Collier Macmillan:

ResearchGate. (n.d.). Cybercrime definition. Retrieved from https://researchgate.net/publication/265350281_Cybercrime_definitionhttps://www.academia.edu/916868/Debarati_Halder_and_K_Jaishankar_June_2011_Cyber_crime_and_the_Victimization_of_Women_Laws_Rights_and_Regulations_Hershey_PA_USA_IGI_Global_ISBN_978_1_60960_830_9

Thotakura, s. (2011). Crime: A conceptual Understanding in *Indian Journal of Applied Research*, 4(3) 196-198. https://www.researchgate.net/publication/270238380_Crime_A_Conceptual_Understanding

Wefinder24. (2023). Cybercrimes, classification and types of cybercrime. Retrieved from https://www.wefinder24.com/2023/01/nature-and-scope-of-cyber-crime.html?m=1

Wefinder24. (2023). Nature and scope of cybercrime. Retrieved from https://www.wefinder24.com/2023/01/cyber-crimes-classification-and-types.html?m=1Aghatise, J. (2006), Cybercrime Definition: cybercrime

Younes, W. (….). Identity Theft.https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.cmu.edu/iso/aware/presentation/id_theft.pdf.