INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

IMPACT OF CYBERCRIME ON VICTIMS

AUTHORED BY: HIMANSHU MISHRA
CO AUTHOR: ASST PROF. VAIBHAV SHANKER SHARMA

Abstract

The pervasive nature of cybercrime has escalated in recent years, posing significant threats to individuals across various domains. This research paper delves into the multifaceted impact of cybercrime on victims, highlighting the profound consequences experienced by individuals who fall prey to these digital offenses. Without delving into specific methodological details, this study employs a comprehensive approach to elucidate the far-reaching implications on the psychological, financial, and social well-being of victims. The research explores the psychological toll inflicted upon individuals who become targets of cybercrime, investigating the emotional distress, anxiety, and fear that often accompany such incidents. Financial ramifications are scrutinized, shedding light on the economic losses incurred by victims through fraudulent activities, identity theft, and online scams. Moreover, the social consequences of cybercrime are examined, emphasizing the erosion of trust in digital interactions, strained relationships, and the potential for long-term social isolation. This paper attempts to contribute to a deeper knowledge of the various ways that victims of cybercrime are affected by their experiences by synthesizing the existing literature and utilizing real-world case studies. The results highlight the need for comprehensive strategies to mitigate the growing challenges posed by cyber threats in the modern digital landscape, while also emphasizing the significance of creating efficient support systems and preventative measures.

1. Introduction

In an era dominated by digital interconnectedness, the rise of cybercrime has become an alarming global concern. As technology advances, so do the methods employed by cybercriminals, leading to a myriad of threats that permeate individuals, businesses, and governments alike. This research paper aims to delve into the multifaceted impact of cybercrime on its victims, shedding light on the often overlooked psychological, financial, and societal consequences. Since the cyberspace is so large, it is difficult to find someone who has committed a cybercrime. Currently, the

 ISSN: 2582-6433

government is lagging behind in taking significant action against cybercriminals and cybercrime. The victims of the cybercrime suffer from psychological and financial effects. It should be the goal of the government to take action to enhance cyberspace. The government is still far behind us in terms of development. The first dimension of impact explored in this paper revolves around the financial repercussions experienced by victims of cybercrime. As individuals and organizations increasingly conduct financial transactions online, the vulnerability to theft and fraud escalates. The research will investigate how cybercriminals exploit digital channels to compromise financial security, leading to monetary losses, unauthorized access to accounts, and the overall erosion of financial stability for victims. Beyond the observable financial consequences, the psychological toll victims bear has to be considered as the second factor. Cybercrime frequently causes severe anxiety, deep emotional distress, and a persistent sense of being violated. The infringement of private, the misplacement of confidential data, and the possibility of cyberbullying all lead to an increasing mental health crisis among victims. The psychological aspects of victimhood will be examined in this essay in an effort to comprehend the long-term effects on people's wellbeing as well as the emotional fallout. Furthermore, the research will delve into the societal consequences of cybercrime victimization. As these crimes proliferate, they pose a threat to the fabric of trust within communities. The erosion of trust not only affects individuals but also has broader implications for businesses and institutions. By understanding the societal ramifications, this paper aims to contribute to the development of strategies and policies that address the collective impact of cybercrime on communities. the impact of cybercrime on victims extends far beyond the immediate technological breaches. This research paper seeks to unravel the multifaceted dimensions of victimization, from the tangible financial losses to the intangible psychological and societal repercussions. By shedding light on the hidden costs of cybercrime, it is hoped that this study will inform policymakers, law enforcement agencies, and the public on the imperative need for comprehensive strategies to mitigate the far-reaching consequences of cybercriminal activities.

2. Who are Cyber Victims?

The prevalence of cybercrime has grown to be an ever-present threat in the quickly changing digital age, leaving a trail of victims in its wake. The word "victim" usually evokes images of people who have suffered bodily injury or property loss. Nonetheless, the concept of victimhood has broadened to encompass individuals who become targets of the cunning schemes of cybercriminals in the digital sphere. Traditional crimes usually have clear, immediate effects, but

 ISSN: 2582-6433

cybercrime has more subtle effects that go beyond the physical world and into the intangible areas of security, privacy, and personal wellbeing. As a result of this paradigm change, both people and things are thrown into the intricate web of cybervictimization. Deviating from traditional ideas of victimhood is necessary in order to comprehend the particular difficulties that cyber victims confront. The consequences of cybercrimes can take many different forms, from financial losses and identity theft to the deterioration of one's physical and mental health. This is in contrast to the aftermath of physical crimes. The anonymity afforded to cybercriminals in the digital realm compounds the complexities of victimization, making it imperative to dissect the layers of impact on those ensnared in the web of virtual wrongdoing. The literal definition of cyber victim that is given by scholars are "Individuals or groups who suffer harm or negative consequences resulting from intentional, malicious acts in the virtual realm[1]." But as we know the aspect of cybercrime is going larger day by day due to which the definition of cyber victim's also changing. The recent definition that is given by scholar by Holt and Bossler in 2016 was "Individuals or entities who suffer harm as a result of intentional acts or omissions in cyberspace[2]". This definition provides a concise and encompassing perspective on the concept of cyber victimization. This definition is notable for its clarity and neutrality, capturing the essence of harm resulting from both intentional actions and negligent oversights in the digital realm. The inclusion of "intentional acts or omissions" in the definition is particularly insightful. It acknowledges that harm in cyberspace can arise not only from direct malicious actions but also from failures to secure systems adequately or respond appropriately to emerging threats. This broader scope reflects the dynamic nature of cyber threats and the diverse ways individuals and entities can be adversely affected. Moreover, Holt and Bossler's definition does not limit cyber victimization to individuals alone; it extends to entities, recognizing that organizations, businesses, and even governments can fall prey to cybercrimes. This acknowledgment aligns with the reality that the impact of cyber threats often transcends individual boundaries and can have far-reaching consequences on a larger scale. Holt and Bossler's definition offers a valuable framework for understanding cyber victimization by encompassing intentional actions, oversights, and extending the concept to various entities. It serves as a solid foundation for discussions and research on the multifaceted nature of harm in the digital domain. By the definition given by these scholars gives an understanding about the victims of cybercrime. If we define cyber victim in general terms, we can say that refers to an

[1] Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427.
[2] Holt, T. J., & Bossler, A. M. (2016). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge.

 ISSN: 2582-6433

individual, organization, or entity that has suffered adverse consequences resulting from malicious activities conducted in the digital realm. This broad and evolving term encompasses a wide range of scenarios, including but not limited to individuals experiencing financial fraud, identity theft, online harassment, or unauthorized access to personal information. A cyber victim can also extend to businesses falling prey to sophisticated cyber-attacks that compromise sensitive data, disrupt operations, or lead to financial losses. As cyber threats become more sophisticated, the definition of a cyber victim has changed to reflect the fact that victimization can involve more than just immediate financial loss; it can also involve psychological distress, invasion of privacy, and a decline in trust in the digital world. Comprehending the subtleties of cybervictimization is essential to creating successful preventive strategies, offering assistance, and formulating regulations that tackle the various obstacles encountered by individuals impacted by cybercrime. The definition of a cyber victim is always changing as a result of the advancements in technology. It takes into account the ever-changing nature of cyber threats as well as the growing range of vulnerabilities that face people and organizations in the digital age. The term "cyber victim" has evolved to encapsulate the broad spectrum of challenges arising from the ever-expanding landscape of cyber threats. In order to create effective preventive measures, offer support, and create policies that navigate the intricate web of vulnerabilities in the digital age, it is imperative to acknowledge the heterogeneous nature of cyber victims.

3. Types of impacts on a cyber victim

I. Financial Repercussions

In our digitally connected world, the financial impact that cybercrimes have on people and organizations has become a common and worrisome issue. Cybercriminals use advanced methods to take advantage of holes in online systems, which can have a severe financial impact on their victims. The purpose of this introduction is to shed light on the complex web of financial effects experienced by cyber victims by examining the different ways that financial losses, illegal access, and online fraud can affect the lives of those who are the targets. The financial industry has seen a dramatic shift toward digital transactions, online banking, and electronic commerce as a result of ongoing technological advancements. Although this provides a level of convenience never seen before, it also puts people and companies at greater risk of becoming victims of cybercrimes such as ransomware attacks, identity theft, and phishing schemes. Cyber victims face financial consequences that go beyond their immediate material losses; these include harm to their credit score, legal repercussions, and possible long- term effects on their financial security. Financial

 ISSN: 2582-6433

victims often find themselves at the mercy of cybercriminals who employ tactics such as phishing, identity theft, and online fraud to compromise sensitive financial information. Unauthorized access to bank accounts, credit card details, and personal financial data can lead to direct monetary theft, leaving victims grappling with the aftermath of drained accounts and fraudulent transactions. In cases of ransomware attacks on businesses, organizations may face demands for payment to regain access to critical data and systems, further exacerbating financial strain. Additionally, the costs associated with recovering from a cyber incident, including hiring cybersecurity experts, implementing enhanced security measures, and potential legal fees, contribute to the overall financial burden on victims. The long-term impact extends beyond immediate losses, as damaged credit scores and compromised financial reputations can haunt individuals for years. Consequently, the financial repercussions of cybercrime extend far beyond the digital breach, affecting the economic stability and financial well-being of the victims. Addressing these challenges requires a comprehensive approach that combines cybersecurity measures, financial protections, and support mechanisms for those who have fallen prey to cybercriminal activities. At International level the recent big cybercrime happened in which the cyber victim suffers from huge financial repercussions is the case of "Not Petya Ransomware Attack (2017)[3]" in this cyber-attack case it affected numerous organizations globally, including major shipping and logistics companies. Maersk, a Danish shipping company, reported substantial financial losses due to the disruption of its operations, highlighting the direct financial impact of cyber incidents on businesses. On June 27, 2017, a malware variant that was first believed to be an extension of the Petya ransomware began to spread quickly, sparking the start of the NotPetya attack. It had an impact on computer systems all over the world, but mainly in Ukraine. A few weeks ago, the WannaCry ransomware attack was powered by the same exploit, the "Eternal Blue" vulnerability, which was exploited by the malware. Although at first it was thought that the attack was a ransomware campaign, further research by a number of cybersecurity specialists and intelligence organizations indicated that politics was most likely the driving force. Numerous analysts came to the conclusion that the attack was carried out by the Russian military, possibly as a kind of cyberwarfare meant to destabilize Ukraine. The attack took place during a period of increased hostilities between Russia and Ukraine. If we see in India the latest cyber-attack in happened in the recent year of 2018 the attack is known as Bitcoin Scam Case (2018)[4]. In this case Amit Bhardwaj, an Indian businessman and cryptocurrency

[3] Fayi, S.Y. (2018). What Petya/NotPetya Ransomware Is and What Its Remidiations Are.
[4] https://economictimes.indiatimes.com/tech/technology/indias-biggest-crypto-ponzi-scam-may-grow-to-rs-1-trillion-affecting-1-lakh-people/articleshow/92259698.cms?from=mdr

 ISSN: 2582-6433

entrepreneur, was at the centre of the GainBitcoin case. The case revolved around an alleged Ponzi scheme where Bhardwaj and his associates promised high returns on Bitcoin investments through their company, GainBitcoin. Bhardwaj attracted investors by offering mining contracts and a multi- level marketing structure. However, as the scheme unravelled in 2017, investors realized they were not receiving the promised returns, and suspicions of fraud arose. Bhardwaj was accused of orchestrating a scam that defrauded thousands of investors of their Bitcoin investments worth millions of dollars. He and his brother were arrested in April 2018 by the Pune Police Economic Offences Wing. Subsequently, Bhardwaj was charged with offenses including cheating, criminal conspiracy, and violation of the Maharashtra Protection of Interest of Depositors (MPID) Act. The GainBitcoin case highlighted the challenges associated with cryptocurrency-related frauds and the need for regulatory frameworks to address such issues. It served as a cautionary tale for investors about the risks associated with unregulated investment schemes in the cryptocurrency space. Financial victimization extends beyond simple monetary losses, encompassing damage to credit scores, legal costs incurred in pursuit of justice, and the potential for long-term economic instability. The cases of cyber fraud and scams demonstrate the need for robust cybersecurity measures and greater awareness among users to mitigate the risk of financial exploitation in the digital age. Furthermore, the legal landscape surrounding cybercrimes and financial repercussions is continually evolving as authorities adapt to the dynamic nature of digital threats. The cases serve as a catalyst for the development of more stringent regulations and improved mechanisms for the investigation and prosecution of cybercriminals.

II. Psychological Toll

When discussing cyber victimization, the term "psychological toll" describes the psychological and emotional toll that people who have been the victims of cybercrimes or other digital misconduct have to endure. It includes the detrimental impacts that different types of online victimization—like cyberbullying, identity theft, online harassment, or any other malicious actions conducted in the digital sphere—have on an individual's mental health and emotional state. Psychological toll involves a range of emotional responses, including stress, anxiety, fear, and a pervasive sense of violation. Victims may experience a loss of control over their personal information or privacy, leading to feelings of vulnerability and distress. In cases of cyberbullying or harassment, the constant threat or humiliation inflicted online can contribute to significant emotional strain. The psychological effects are not limited to the immediate event; in severe

 ISSN: 2582-6433

cases, they may result in long-term consequences like low self-esteem, problems with trust, and even symptoms of post-traumatic stress disorder (PTSD). A persistent feeling of discomfort and emotional turmoil can result from someone's digital space and personal boundaries being violated. Understanding the psychological toll on cyber victims is crucial for developing support systems, counselling services, and mental health interventions that address the unique challenges posed by digital victimization. It emphasizes the need for a holistic approach to cybercrime prevention and recovery, taking into account not only the tangible damages but also the often-hidden emotional scars left on individuals affected by online harm. Cybercrimes, with their insidious nature, have been instrumental in inflicting a profound psychological toll on their victims. The violation of personal boundaries, often associated with cybercrimes such as hacking, online harassment, and identity theft, transcends the digital realm and seeps into the emotional well-being of individuals. The loss of privacy and control over personal information can trigger feelings of vulnerability and anxiety, as victims grapple with the unsettling reality that their digital presence has been compromised. Instances of cyberbullying, wherein individuals face persistent online harassment or threats, contribute to heightened stress, fear, and, in extreme cases, may lead to depression or other mental health issues. The psychological impact intensifies when victims are confronted with the aftermath of financial cybercrimes, such as fraudulent activities resulting in monetary losses. The betrayal of trust and the intrusion into one's financial security can evoke feelings of powerlessness and distress, magnifying the emotional toll on victims. Additionally, the arduous process of reclaiming stolen assets or rectifying the damage caused by financial cybercrimes can exacerbate the emotional burden, leading to frustration and a sense of helplessness. The anonymity provided by the digital landscape often emboldens cybercriminals, creating an environment where the consequences of their actions extend beyond the tangible realm to inflict lasting emotional scars on their victims. As society becomes increasingly dependent on digital interactions, addressing the psychological toll of cybercrimes is imperative. Supporting victims through counselling, raising awareness about online safety, and implementing stringent measures against cyber offenders are crucial steps in mitigating the psychological impact and fostering a resilient and secure digital environment. Recovery from the psychological toll inflicted by cyber victimization is a nuanced and gradual process, necessitating a combination of self-care, social support, and professional assistance. Firstly, acknowledging and accepting the emotional impact is crucial; victims should allow themselves to process the feelings of distress, violation, and anxiety without judgment. Seeking support from trusted friends, family members, or support groups can provide a crucial outlet for expression and understanding.

 ISSN: 2582-6433

Engaging in open conversations about the experience may alleviate the sense of isolation and validate the emotional response. In addition, navigating the psychological fallout requires professional mental health support. Counsellors or therapists with experience in trauma and cybervictimization can provide victims with a safe space to express their feelings, as well as coping mechanisms and validation. Cognitive-behavioural therapy (CBT) is one technique that can help with reframing negative thought patterns and reestablishing a sense of security. The development of new digital habits is another essential component in psychological healing. Regaining control over one's digital presence, learning about cybersecurity procedures, and improving online privacy measures could all be part of this. Rebuilding a victim's sense of security can be greatly aided by providing them with the information and resources they need to protect themselves online. Ultimately, it is critical to concentrate on holistic well-being. Maintaining a healthy lifestyle, practicing mindfulness, and partaking in joyful activities can all have a positive effect on mental health. Making self-care a priority in your routine can help with the slow process of psychological healing. In light of the psychological toll, there is a pressing need for awareness campaigns, educational initiatives, and counselling services to empower individuals in navigating the emotional aftermath of cybercrimes. By recognizing and addressing the psychological impact, society can work towards fostering a resilient digital environment that prioritizes the well-being of individuals and communities affected by the ever-growing spectre of cyber threats.

III. Societal Consequences

In an era dominated by digital connectivity, the societal consequences of cyber victimization cast a wide and profound shadow, impacting not only individual victims but also communities and the broader fabric of trust within society. As cybercrimes proliferate, their ripple effects extend far beyond the immediate victims, creating a collective vulnerability that challenges the very foundations of social cohesion. Comprehensive strategies for mitigation are necessary due to the complex web of challenges presented by the deterioration of trust within communities, the consequences for businesses and institutions, and the overall societal ramifications. As individuals face cyber victimization, whether through financial fraud, online harassment, or identity theft, the collateral damage is felt at a communal level. The breach of trust within communities becomes palpable, as the fear of cyber threats permeates social interactions and engenders a sense of vulnerability. This paper delves into the ways in which the societal consequences of cyber victimization contribute to a broader narrative of distrust, examining the

 ISSN: 2582-6433

implications for social relationships, community well-being, and the functioning of institutions within the digital age. Among the various types of cybercrimes, those that generate a significant societal impact often involve large-scale data breaches and cyberattacks targeting critical infrastructure. Data breaches, where vast amounts of sensitive information are compromised, have profound societal consequences. When personal details, financial records, or medical information are exposed, individuals become susceptible to identity theft, fraud, and other forms of exploitation, leading to a loss of trust in digital systems. Cyberattacks on vital infrastructure, like transportation networks, power grids, or healthcare facilities, can also have a significant negative impact on society. Not only can essential service disruptions jeopardize public safety, but they also undermine trust in the stability of social structures. These assaults have the potential to cause widespread fear, financial losses, and a collapse in confidence in institutions' capacity to protect essential facets of everyday existence. Cybercrimes encompassing online manipulation, social engineering, and fake news have the potential to sow distrust and division among communities. The spread of misleading information and the planning of internet campaigns aimed at swaying public opinion can have a polarizing effect on society and undermine mutual respect and collaboration. Recovering cyber victims from the societal consequences of cybercrimes requires a multifaceted approach that addresses both the immediate impact and the broader implications on communities. Firstly, fostering a supportive and empathetic environment is crucial. Initiatives should be launched to raise awareness and reduce the stigma associated with cyber victimization. Educational programs, community workshops, and awareness campaigns can play a pivotal role in not only informing the public about the prevalence of cybercrimes but also in promoting empathy and understanding towards the victims. It is necessary to strengthen legal frameworks and law enforcement initiatives to guarantee that cybercrime offenders receive just punishment. The public and private sectors working together can improve cybersecurity measures' efficacy and help avert similar incidents in the future. The establishment of support groups and counselling programs designed especially for cyber victims can also help in their recuperation. By providing a safe space for people to share their experiences and seek guidance, mental health professionals can help individuals cope with the emotional distress caused by cybercrimes. Moreover, it is imperative to establish a resilient culture in communities. This entails fostering responsible digital citizenship, educating people about online safety, and advancing digital literacy. Communities can actively help to lessen the negative effects of cybercrimes on society by fostering a sense of shared responsibility for online safety. Public-private partnerships are essential to the creation and execution of all-encompassing strategies. In order to address the

 ISSN: 2582-6433

societal impact of cyber victimization, government agencies, non-profit organizations, and the private sector can work together to create support networks, resources, and policies. In the end, healing cyber victims and building a safe and encouraging digital community require an all-encompassing and cooperative strategy.

IV. Conclusion

The impacts of cybercrime on victims are both extensive and intricate, touching on financial, psychological, and societal dimensions. The pervasive nature of cyber threats underscores the urgent need for comprehensive preventive measures to curtail the far-reaching consequences. Financially, victims face not only immediate monetary losses but also enduring damage to credit scores, legal complications, and potential long-term economic instability. Psychologically, the toll involves heightened stress, anxiety, and a profound sense of violation, particularly in cases of identity theft and online harassment. Societal repercussions include the erosion of trust and the potential for broad community-level consequences. To combat these challenges, preventive measures must encompass enhanced cybersecurity education, robust digital security frameworks, and the integration of advanced technologies such as artificial intelligence and blockchain. Public awareness campaigns and the promotion of responsible online behaviour are crucial elements in the fight against cyber victimization. Additionally, collaborative efforts between governments, law enforcement agencies, technology companies, and the public are essential to create a resilient and secure digital landscape. By combining technological advancements with proactive education and legislative initiatives, it is possible to mitigate the impact of cybercrime on victims and foster a safer online environment for individuals and communities alike.