THE DIGITAL MUTATION OF WHITE-COLLAR CRIME: LEGAL AND STRATEGIC CHALLENGES IN THE CYBER ERA

Karan Sharma, Bennett University

ABSTRACT

This paper explores the digitization of white-collar crimes due to the dynamic nature of the technology and its rapid advancement. It traces the journey of how innovations like Artificial Intelligence and Blockchain protection have contributed to the rise of economic offences in the cyber space. This study covers all the major financial offences, enabled by cyber technology advancements, and sheds light on how such offences constitute an evolved form of methods used in the manipulation of trust for illegal financial gains. This paper examines the International and domestic legal nets in place, focusing on the Budapest Convention on Cybercrime and the Information Technology Act, 2000. It also discusses key landmark cases such as Enron Scandal, Sony Pictures Hack, and Bernie Madoff Ponzi Scheme. The paper offers a conclusion by suggesting various legal reforms and the need for stronger corporate governance to tackle the ever-changing threat of modern white-collar crime.

Introduction

Definition of Cybercrime

Cybercrime includes a wide range of illegal activities which usually involves a device or a network. It can range from hacking to more orthodox methods of committing computer-based crimes that consists of stalking, theft etc. Due to the dynamic nature of technology, cybercrime continues to be a major concern for security as everyone, ranging from business to governments, are moving towards digitization.[1] The growing technological advancements have enabled businesses and persons to digitize their personal as well as financial data. This in turn has given rise to a new age of highly skilled fraudsters that are challenging for the authorities to identify. These fraudsters take advantage of the technological flaws and weak cyber security to conduct illicit activities. The anonymity of the internet acts as a blanket for illegal activities that can be executed from all around the world. Although white-collar crimes and cybercrimes are different from each other, there are many similarities that connect them; both involve taking advantage of trust, systems and procedures for the purpose of gaining financially and personally. Although cybercrime uses anonymity, its powerful sibling, to extend its reach at a global level. Below are some forms of cybercrimes:

- **Identity Theft** – It is the stealing or illegally obtaining a person's personal information with the intention of committing fraud. This can include bank account details, credit cards, and much more information that is directly linked with a person. The stolen information can prove to be very damaging towards the person as it can be used for unauthorized withdrawals from the victim's bank account, acquiring loans, stealing the identity, etc.

- **Hacking** – Information or data can be stolen by unauthorized and illegal access to computer networks. This is done by hackers with the motive of targeting government networks and large companies for financial gains.

- **Cyber Fraud** – This consists of fraudulent schemes made using digital platforms. Cyber fraud is generally quite difficult to trace, and the perpetrators are usually very

[1] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press, 2007).

difficult to track due to the anonymity of the internet.[2] The number of victims that get affected by cyber fraud ranges to thousands.

- **Cyber Espionage** – It is the process of hacking public or private entities and stealing classified information. This information could include trade secrets and intellectual property.

Evolution Of White-Collar Crime

Historical Background

Edwin Sutherland was a renowned sociologist who coined the term "white-collar crime" during his presidential address to the American Sociological Society in 1939. He described white-collar crime as "a crime committed by a person of respectability and high social status in the course of their occupation"[3]

His thinking was beyond the traditional mindset surrounding the term crimes, which primarily focused on serious or violent offenses. Sutherland's study shifted focus to the wealthy elite and showcased that crime is not only committed by those who live in socially disadvantaged conditions. His study highlighted the fact that white-collar crimes are committed by business executives and professionals behind closed doors. Of course, the concept of cybercrime did not exist in Sutherland's time because the technological instruments to commit cybercrime did not exist.

Traditional Forms of White-Collar Crime

The mentality behind commission of white-collar crimes has always included the manipulation of set procedures to gain profit and avoid financial losses. Following is some of the less common types of white-collar crimes:

- **Embezzlement** – Stealing funds or assets that are entrusted to a particular person is known as embezzlement. The embezzler uses these funds or assets for a different

[2] Michael McGuire and Samantha Dowling, *Cybercrime: A Review of the Evidence* (Home Office Research Report 75, UK Home Office 2013).
[3] Edwin H. Sutherland, *White Collar Crime* (Holt, Rinehart and Winston, 1949).

purpose than for what they were intended. Embezzlement occurs either small or large scale which depends on how much is taken.

- **Corporate Fraud** – Corporate fraud includes illegal and unethical activities that are either conducted by the company or against the company. It has a very complex nature which makes it difficult to identify.

- **Insider Trading** – It involves trading of a company's stocks based on the information obtained, which has not been made public.[4] This gives an unfair advantage to the person involved in insider trading.

- **Tax Evasion** – This is typically done by people who have a high social status. They use some pseudo-complex financial loopholes to hide their true income.

- **Bribery and Corruption** – Any donations, gifts, or money received or given to influence a decision constitutes bribery. This mostly occurs in political or governmental domains.

The Transition to Cybercrime

White-collar crime started to move into the cyberspace from the late 20th and early 21st century.[5] This was majorly due to improvement in technology and innovation. Crimes like fraud and embezzlement have found their way in the internet space, thereby allowing the notorious to commit more ambitious crimes. There has been a drastic growth in digital infrastructure, thereby data stealing and financial fraud has become easier to commit. For instance, cybercriminals take advantage of digital platforms such as cryptocurrency exchanges or wallets like Google Pay, or any other apps used to handle finances to mask stolen money transactions. They exploit the global reach of such financial platforms to move stolen funds across borders. These platforms are safe and secure as the digital transactions are encrypted, thus making it difficult to trace their origins and path. Banks have made it risky to deposit stolen funds as they have strict regulations like Know Your Customer (KYC). Perpetrators use cryptocurrencies and store their stolen money in digital formats to avoid detection by the authorities. Global reach is a distinct feature of cybercrime as a hacker can hack and steal data or funds from the financial

[4] United States Securities and Exchange Commission, *Insider Trading*
[5] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger, 2010).

system while sitting across the world. Like mentioned earlier, internet is all about anonymity, so cybercriminals take advantage to commit financial crimes. The technology of blockchain and virtual private networks (VPNs) has made it more difficult to identify the perpetrators. Technology has enabled persons to commit white-collar crimes on a larger scale. Phishing scams can attack thousands of people in a go, which turns out to be profitable for the perpetrators. Thus, techniques of white-collar crime have evolved over time to overlap cybercrime. There has been a shift in and change in modus operandi, but the manipulation of trust has remained the same.

Technological Advancements Leading to Cybercrime

The changes and improvement in technology has played a major role in expanding the scope of cybercrime. Technological advancements like blockchain and artificial intelligence (AI) has enabled perpetrators to find weaknesses in the system and have allowed them to exploit such areas for their benefits.[6] Development and advancement of internet is taking place every single day. It has revolutionized the way people communicate, interact socially and conduct their business. But a coin has two different sides. Internet's growth has made it easy for cybercriminals to reach millions of people from a single place. With anonymity in their backpack, cybercriminals can make it almost impossible for the law enforcement to find them. Blockchain was created to make sure that the transactions made online over the internet is secure from cybercriminals. Although, thieves are known to exploit the anonymous channels, like Bitcoin and Ethereum, for money laundering and illegal transactions in the black market. Artificial intelligence also has created more threats than opportunities within the domain of cybercrime.[7] AI has the capability of creating complex cybersecurity solutions and detect threats in milliseconds. Cybercriminals use these AI tools and systems for automating attacks or for phishing scams. For instance, identities of personals are stolen through deepfake technology and then used for political or business purposes.[8] Internet of Things (IoT) is another way of penetrating and stealing sensitive data. IoT is a network where a number of devices are connected to each other. This may include wearables, home appliances, phone devices, etc. The use of IoT is to make life and data sharing easier which saves time, but it gives hackers unique

[6] Kim-Kwang Raymond Choo, 'The Cyber Threat Landscape: Challenges and Future Research Directions' (2011) 30(8) *Computers & Security* 719.
[7] Mariarosaria Taddeo and Luciano Floridi, 'How AI Can Be a Force for Good' (2018) 361(6404) *Science* 751.
[8] Nguyen TT et al., 'Deep Learning for Deepfakes Creation and Detection' (2019) arXiv:1909.11573

and new entry points to penetrate the system which could potentially lead to an entry in a larger network.

Comparison with Traditional White-Collar Crimes

Despite the changing times, financial crime still prevails as rich white-collar crimes continue to break new levels in cybercrime. Financial gain is a significant motivator behind most crimes, where the criminals exploit the system for their benefits. Another form of traditional white-collar crime is when a person of authority (politician or business executives), abuses their powers or uses insider information to commit fraud. Cybercrime also tends to exploit the trust of people in digital systems. Complexity and subtle involvement are another two domains where both white-collar crime and cybercrime have similarities in. Crimes like fraud and tax evasion require complex planning and immense legal knowledge. Similarly, cybercriminals use advanced devices and schemes such as multiple levels of encryption that helps in maintaining the anonymity of the hacker. Traditional white-collar crime often affects a single entity or a group of people, whereas one single hack could potentially damage and affect millions of people. There are a lot of similarities between the two types of crimes, but they certain factors that allow them to be different from each other. Some of those factors are as follows:

- **Anonymity –** While considering this factor, traditional white-collar criminals often face difficulty in keeping their identify anonymous as they are usually the people who hold positions of authority or belong to well established organizations. Whereas cybercriminals can mask their identities through various levels of securities or multiple identities.

- **Global Reach –** White-collar crimes are ideally limited to local or regional markets but on the other hand cybercrime can jump borders to attack victims across multiple countries. As a result, the issue of jurisdiction arises when it comes to enforcing laws and regulations.

- **Scale of Impact –** Cybercrime holds the power to damage far more individuals in a shorter period of time as compared to white-collar crime. For example, if a cybercriminal breaches a renowned corporate entity for stealing their data, it could potentially lead to exposing millions of individuals' sensitive information. This may lead to a huge financial loss and could harm the goodwill of the entity.

Types of Cybercrime as White-Collar Crimes

There is a level of sophistication and diversity involved when cybercrime takes goes through a transition to take the form of white-collar crime. It comprises of multiple illegal acts that take the advantage of technologies that are computer based for the purpose of financial gain. Some of the categories of cybercrime come under the umbrella of modern white-collar crime:

Financial Cybercrime

Financial cybercrime refers to a wide array of illegal activities that take the advantage of digital technologies to gain financially or disrupt economies. It includes stealing identity, ransomware attacks, phishing etc. Financial industry is a very profitable target and hence it is an attractive target for the cybercriminals. Some important categories of financial cybercrime include:

- **Phishing –** It is a method of illegally stealing personal information by masking the identity of the perpetrator as a trustworthy organization. This targets sensitive information of individuals like credit card numbers and passwords. Victims of phishing receive several spam emails on their account which seems from a genuine organization. These emails urge the victims to provide their personal information for signing up on a fake website and this is how their information gets stolen. Due to advancements in technology and awareness among people, cybercriminals have started to make realistic duplicates of websites to make to seem legitimate.

- **Trojan –** It is a software which is created for the purpose of tricking the computer system into loading or deleting certain files. After it gets installed, Trojan software could lead to hijacking of the computer system which could delete, modify or steal data and spread viruses. Trojan can also be used to create a backdoor entry for hackers to access the computer. Trojan is integrated in a file which is sent to the victim through an attachment in the email. As soon as the victim opens or downloads the attachment, the software starts to spread viruses in the system. Whenever any sensitive information is entered in the computer, the cybercriminals can get access to it.

- **SIM Swap –** Criminals can obtain sensitive information about the victims through different means like phishing. Post that they approach the network service provider of

the SIM card and get the original SIM card blocked.[9] Then they get a duplicate SIM card issued with a fake ID proof of the victim. This helps the cybercriminals to obtain sensitive passwords like One Time Password (OTP) which leads to stolen banking information or funds from the bank account attached to the phone number of the SIM card.

- **Investment Scams and Ponzi Schemes –** Investment scams involve misleading schemes where criminals attract the victims by showcasing that they can provide high returns while minimizing risk. Such scams mostly use the online platform or advertisements to gain the trust of the people. Due to perfect showcasing of such scams, criminals gain the trust of victims which attracts investment of funds into non-existent ventures, only to realize that the returns that were promised to them are never fulfilled. Ponzi scheme is a specific type of investment scam which enables the criminals to pay the older investors through the funds obtained by the new investors. This creates a cycle of funds. The continuous enlistment of new investors is one of the main factors to Ponzi schemes' success. If a situation arises where the recruitment of new investors come to a stop, then the scheme collapses. The scheme is named after Charles Ponzi who created this scam in 1920s. Both scams lead to high financial losses and are very difficult to trace as the criminals apply sophisticated methods to mask their activities.

Both white-collar crimes and financial cybercrimes have various similarities as both are non-violent in nature with the sole objective of financial benefit. They depend on deceiving and exploiting trust of their victims. White-collar criminals depend on using their professional authority, similarly cybercriminals rely on illegal methods like phishing. Both type of criminals takes advantage of the flaws in the system, helping them in escaping and preventing detection.

Corporate Cybercrime

Cybercrime aims at a global reach through the internet to infiltrate and hijack private systems of people and organizations. It takes a specific form when the attack is directed towards a corporation with a motive of steal data, trade secrets, patented formulas of products, identities and personal information of the employees etc. Then main objective is to disrupt the operations conducted by the company to cause severe financial losses. Although it is much simpler and

[9] RBI Advisory, 'Cyber Security Awareness: SIM Swap Fraud'

easier to conduct through cyber, corporate cybercrime and traditional white-collar crimes are linked to each other. Some types of corporate cybercrimes are as follows:

- **Corporate Espionage –** Corporate Espionage is when an individual acquires sensitive data or information from a corporate entity, through unlawful means, to gain an advantage on its competition. When it comes to the use of internet in terms of this matter, cybercriminals hack the cyber system of a particular company to obtain secretive information or gain access to the intellectual property.

- **Insider Trading using Cyber Tools –** The use of information obtained illegally through hacking the digital platform of a company and using that information to purchase or sell stocks comes under this category. Some confidential information like upcoming mergers of a company and un-published profit reports can be accessed and used to manipulate the stock prices. This is usually done by hacking into the servers of the victim company or through phishing scams.

- **Supply Chain Attacks –** Hackers usually prefer the method of using their supply chain to target the corporate firms. Supply Chain Attack is a type of strategized attack used to bypass the cyber security of a firm by taking advantage of a third-party supplier's business. Cybercriminals use this method to disrupt business related operations of a firm by taking advantage of more lenient security policy of partner firms.

Cyber Extortion and Ransomware

Cybercrime highly depends on the advancements and developments in the technology. Modern cybercriminals penetrate multiple firewalls to steal data from the system. According to the experts, cybercrime is growing at a quick rate and could potentially reach $10.5 million annually by 2025.

Ransomware attacks and cyber extortion contribute to this figure significantly as they involve a ransom demand from the criminals to give back access of the server and system to the original owner. These demands usually include money which is paid in cryptocurrency to avoid detection of the perpetrators. Ransomware is a type of malware which hijacks the data of the targeted victim so it cannot be accessed by anyone else until the demanded ransom is paid. Cyber extortion can take the form of sextortion when the cybercriminal blackmails by threating

to spread private images or videos of the victim.

For instance, Netflix, a well-known movie streaming platform, was hacked by a cybercriminals group called TheDarkOverlord. They managed to penetrate the servers of Larson Studio. The hacking group threatened to post unreleased episodes of the show "Orange is the New Black". Netflix refused to pay the ransom and in return the cybercriminals posted the episode from season five onwards on a site called patebin.com.[10]

The pandemic of Covid-19 also contributed to the growing events of ransomware. Organizations are moving towards remote work rapidly which is leading to more dependence on the internet. Not updating the cyber security of the servers could potentially leave gaps which can be exploited by the cybercriminals. In the year 2023, around 10% of the organizations globally were targeted by ransomware attacks.[11]

Infrastructure such as hospitals and electric grids, that are essential for the growth of the economy is often targeted by cyber attackers. Attackers take advantage of the fear in people to rush payments. As cyber extortion leads to loss in terms of reputation and disrupt operations that leads to loss in the range of millions, the blackmail can greatly impact the lives of individuals. The tactic of "double extortion" is used by criminals to pressurize the victims into compliance. Double extortion is a technique where the data of an individual is stolen and made public if the ransom is not paid. This tactic is used against big companies to ensure their compliance as the company faces a rock and a hard place kind of situation because the ransom demanded is quite high and the risk of data leak is also high and damaging to the firm and its reputation.

The above-mentioned types of cybercrime are all extensions of white-collar crime. They share the core nature and characteristics of being purely for financial gain, non-violent and they rely on the manipulation of trust of the victims. Financial cybercrime involves fraud by focusing on penetration of financial systems digitally for the purpose of stealing funds and transactional manipulation. Corporate cybercrime mainly targets businesses to illegally obtain intellectual property and to gain access through illicit acts. On a similar note, cyber extortion and ransomware attacks focuses on using private information and leverage to gain money. All these

[10] Geeks for Geeks, 'Real-Life Cybercrimes That Shocked the World'
[11] Check Point Research, *2023 Global Ransomware Trends Report*

cybercrimes are a digital representation of white-collar crime as they require the use of advanced technology to use flaws in the digital systems for financial or strategic gains.

Legal Framework and Challenges

International Laws and Treaties on Cybercrime

The 2001 Budapest Convention on Cybercrime was the first agreement signed on an international level that focused on tackling cybercrime and providing a framework for cooperation. This is signed by more than 65 countries which gave it the name the Council of Europe Convention on Cybercrime. Under this convention, the members were obligated to reform their legal frameworks to criminalize illicit acts like hacking, device abuse, and system interference. The convention had certain provisions for enforcement of cross-border rules with the added help of national laws when it came to preservation of data and communications. International cooperation was another important aspect of the agreement in terms of investigation and prosecution of the cybercriminals. Besides the Budapest Convention, there are other organizations too which are working towards countering cybercrime. UN has many programs under its Office of Drugs and Crime (UNODC) by equipping the member states and train them to promote international cooperation. The UN General Assembly in 2021 gave approval to a resolution asking countries to cooperate and contribute towards the fight to prevent cybercrime. Government organizations like Interpol and Europol have also developed certain specific sections to prosecute cybercriminals.[12] The European Cybercrime Centre has the responsibility of overseeing and disrupting cybercrime operations and providing their expertise for EU member states. Recently there has been more talks about the requirement of international norms and structures to manage the threat of cybercrime in the G7 and G20 summits.

National Legal Frameworks

Each country is working towards preventing data theft and cyberterrorism by developing and updating their legislative models to punish the cybercriminals. For instance, the Computer Fraud and Abuse Act (CFAA) was passed in 1986 which possibly is a major piece of the US federal legislation.[13] This act reinforced and prohibited unauthorized access to computers

[12] Interpol, *Cybercrime Directorate*

[13] Computer Fraud and Abuse Act 18 USC § 1030 (1986)

involved in the government and business sector. The CFAA enables the victim parties to claim damages through civil suits and remedies. This Act has been often criticized for the hollow and void phrases that usually exposes it to concerns regarding ethical security research. Other countries have laws like the General Data Protection Regulation of the European Union which emphasizes on protection of data against hacking and imposes strict penalties on corporations concerned with data security and breach notifications.[14] The Cybercrime Act of 2001 is prevalent in Australia which also criminalizes computer related crimes and gives legal power to law enforcement to obtain search warrants for electronic devices.

India has its own legal framework to tackle the problem of cybercrime. The Information Technology (IT) Act, 2000 acts as the main body of law in terms of handling cybercrime in the country.[15] The IT Act facilitates in conducting commerce through the world of cyberspace and the law helps in providing legal protection against cybercrimes like cyberterrorism and data stealing. Section 66 of the IT Act deals with hacking and unauthorized access into computer devices and declares these acts as illegal. Diving deep into this section, sub-clause (f) criminalizes cyberterrorism and makes sure cybercriminals are punished for the illicit acts that they carry out which could pose a threat to national security. After a period of time, amendments were made in the IT Act, especially the IT (Amendment) Act 2008, expanded the scope of the Act by improving the existing the data protection laws and improvements in cybersecurity.

Enforcement Challenges

The legislative frameworks of every nation are ever developing when it comes to protection again cybercriminals, but there is a long list of obstacles that hinders their effective implementation. As cybercrime is executed on a global level, it becomes difficult to determine which country, or state has jurisdiction to investigate and prosecute the case. This complicates the legal process and makes it almost impossible to penalize and punish the culprits with effective legal measures because hackers attacking one country could be residing in another country. Another obstacle is the anonymity of the hackers due to excessive use of Virtual Private Networks (VPNs) which masks the identity and location of the user. Concealing one's identity and location makes it easier for cybercriminals to evade and prevent the authorities to track their activity and operations which can be used as evidence in their prosecution. The

[14] Regulation (EU) 2016/679 (General Data Protection Regulation)
[15] Information Technology Act 2000, ss 43–66.

investigations conducted by law enforcement can be hindered by hiding evidence through encrypting stolen data on encrypted devices. There are recent issues and debates circling around the topic of balancing user privacy through encryption and the allowing the law enforcement to access it. All in all, the authorities are both resource-constrained and at a disadvantage in terms of technology. The prevailing laws and legal frameworks are incapable of keeping up with the rapid technological development which has created bypasses in the ability to prosecute cybercriminals effectively. Furthermore, many organizations made to deal with cybercrime do not possess the tools, know-how and training to tackle it.

Case Studies

The Enron Scandal (2001) –

This scandal marks the key milestone of corporate fraud, where flaws in the accounting system were exploited by the high executives for the purpose of hiding billions of dollars in debt money. Encrypted emails were used by the executives to prevent the authorities from flagging them and digital records were deleted to hinder investigations. This case is a prime example of how technology plays a part in executing and concealing white-collar crimes. Traditional white-collar crimes generally involve a paper trail that could be traced back by thorough investigations. Whereas crimes of the cyber world like Enron's are much more difficult to trace and detect due to effective use of firewalls and deep encryption. In the Enron Scandal, the executives used complex strategies and software for data manipulation creating a mountain of profit. This kind of sophistication is rarely seen in the cases of traditional white-collar crime, which generally involves manipulating records. The Enron case showcases the need for advanced systems to keep an oversight over digital activities to tackle modern white-collar crime. It also underscores how the implementation of technology in operations of corporate companies has opened a window for fraud.

The Sony Pictures Hack (2014) –

A group of North Korean hackers penetrated and leaked sensitive data which included the employee records, sensitive emails and films that were unreleased at that time. This attack was executed because of the film "The Interview" which mocked the North Korean Leader. This hack was different from traditional white-collar crimes as it was not intended for financial gain. However, it somehow comes under white collar crimes as it used techniques like insider

knowledge and sophisticated methods to penetrate the systems. Traditional white-collar crimes usually involve insider trading or theft of intellectual property for financial benefit but in the Sony hack, external players used advanced digital tools. For instance, the hackers used phishing emails to infiltrate the firewalls of Sony's network and deployed malware to steal the sensitive data. This case proved to be a decisive example of how easily cybercriminals can transcend international boundaries and cause financial harm to corporate firms. It also raised the concerns of nation-states' role in tackling the challenges related to defending against such attacks. The need for increased cybersecurity was recognized and companies started investing in advanced threat detection systems.

The Bernie Madoff Ponzi Scheme (2008) –

Bernie Madoff used digital tools and software to create multiple false statements of accounts and manipulated the records which helped in defrauding investors of approximately $65 billion, making it one of the biggest frauds of all time. This case showcases how white-collar criminals execute fraudulent activities thorough exploiting technology. Traditional Ponzi schemes, like the ones that were handling by the creator Charles Ponzi himself, primarily included traditional methods of manual record-keeping and words of mouth was used to attract the investors whereas Bernie Madoff took advantage of modern technology which aided him to scale the fraud at a global level. For instance, his firm produced fake account statements through a certain software which acted as an illusion for the investors to attract large investments. The scale of automation applied in this case is not common in traditional white-collar crimes. This case highlighted the ever-evolving nature of white-collar crime, which is now accelerated by the digital tools available, and the need for a regulatory authority to detect and prevent such fraud schemes. After this case, investment firms were kept under microscopic observation and the reporting requirements became stricter.

Impact Of Cybercrime as A White-Collar Crime

Economic Impact –

There is a great responsibility of financial implications on the organizations, governments and individuals. According to the reports of Cybersecurity Ventures, it is seen that the global yearly cost of losses caused by cybercrime would be approximately $10.5 trillion by end of the year

2025.[16] The direct costs of cybercrime include recovery efforts and ransom pay. In 2021, IBM calculated the general mean cost for a data breach which turned out to be around $4.24 million which is a huge burden for small and medium-sized firms. It also involves various indirect factors which are affected like productivity losses and damaged reputation of the company which leads to loss of customer trust. Even the governments which are focused towards tackling and preventing cybercrime incur large amounts of cost to implement cybersecurity projects and tightening the law enforcements. In such cases, a disruption in the operations of the government affects the delivery of services to the citizens which further leads to the wastage of taxpayers' money. In case of individuals, identity theft leads to significant amount of losses and some damages caused are beyond repair through credit scores. The victims have the remedy of identity restoration, but the process takes several months, and in some cases even years.

Social and Psychological Effects –

Cybercrime has effects on numerous factors other than just the economy; it also affects the mentality and confidence of the consumer. Often confidence of the public is shaken in governments and companies when they are the victims of a cyber-attack. The consumers may become reluctant to do business with a firm that was not able to protect their information from cyberattacks. The lack of trust creates a domino effect which results in reduced sales and provoke a suspicious attitude. The trust of the consumers has been fading away from online purchases because of the danger cybercrime poses. Awareness and warning about fraud and data breach could potentially deter people from using digital services like online banking and e-commerce which affects the chances of acquiring numerous technological and financial innovations. Victims of cybercrimes like financial fraud and identity theft experience psychological trauma. They suffer a fear of getting victimized for a second time which causes shyness to participate in online operations and a lack of trust in technology.[17]

Future Implications for Corporate Governance –

The threat of cybercrime is ever-growing due to technological advancements which calls for reforms in corporate governance procedures that strengthens the cybersecurity. Firms and organizations are required to frame strict and secure practices to improve the storage of

[16] Cybersecurity Ventures, 'Cybercrime to Cost the World $10.5 Trillion Annually by 2025' (2021)
[17] Monica T. Whitty, 'Anatomy of the Online Dating Scam' (2015) 28(4) *Security Journal* 443

sensitive data and restore the confidence of stakeholders as they increasingly rely on digital infrastructure. Therefore, businesses should invest in cybersecurity plans that focuses on post-incident planning and training of employees. Organizations may reduce the consequences of data breaches which includes multi-factor authentication and regular updates in software along with bug fixes. The legal frameworks to tackle cybercrime are evolving to enhance accountability in corporate governance and businesses are kept under strict liability when it comes to protection of personal information due to laws like California Consumer Privacy Act and General Data Protection Regulation (GDPR). Data privacy should be a priority and failure to comply with regulations should attract penalties and legal obligations. Cybersecurity must not leave the top levels of corporate governance. The Board of directors must create committees that oversee and update the firm's cybersecurity strategy.[18]

Conclusion

The evolving nature of cybercrime as a form of modern white-collar crime showcases the major impacts in the case financial sectors due to advancements in technology. Traditional white-collar crimes have always been restricted by international boundaries, but cybercrime has surpassed all the barriers and exploited the anonymity of the digital platforms. This change and advancement introduced new challenges for corporate governance and legal frameworks which are working towards eradicating such crimes and punishing cybercriminals. Cybercrime comes under the blanket of traditional white-collar crime as both have the primary objective of financial gain by exploiting trust. The digital platform has aided in boosting the scale of crimes which has enabled the criminals to target millions of people in a few minutes. The rise in ransomware attacks and corporate espionage showcases that strong cybersecurity systems have to be implemented, and countries need to corporate with each other to counter such threats. The national and international frameworks are also evolving to tackle different types of cybercrimes. But the enforcement of such legislations has been a big problem for the authorities which is mainly because of the anonymity of the internet and complexities in the execution of the crime. Cases mentioned in the article are an example of how technology has been a major tool for committing white-collar crimes. The economic, social and psychological impacts of cybercrime affect not only the financial systems but also disrupt the trust of the public in digital systems. The organizations have started to rely on digital platform for data storage which has increased the need of strong corporate governance. So, the businesses invest in cyber security

[18] World Economic Forum, *Principles for Board Governance of Cyber Risk* (2022)

firms to mitigate the risks posed by cybercrime. In conclusion, as the technology is advancing, the strategies and legal framework made to tackle it should also be updated accordingly. Only by combining innovation in technology, good legal reforms and international cooperation can the problem and challenges of cybercrime be eradicated.

References

1. Edwin H. Sutherland, *White Collar Crime* (Holt, Rinehart and Winston 1949).
2. Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).
3. David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).
4. Christidis K and Devetsikiotis M, 'Blockchains and Smart Contracts for the Internet of Things' (2016) 4 *IEEE Access* 2292.
5. Nguyen TT et al., 'Deep Learning for Deepfakes Creation and Detection' (2019) *arXiv preprint arXiv:1909.11573*.
6. Diana B. Henriques, *The Wizard of Lies: Bernie Madoff and the Death of Trust* (Times Books 2011).
7. Bethany McLean and Peter Elkind, *The Smartest Guys in the Room: The Amazing Rise and Scandalous Fall of Enron* (Portfolio 2003).
8. Cybersecurity Ventures, 'Cybercrime to Cost the World $10.5 Trillion Annually by 2025' (2021).
9. IBM Security, *Cost of a Data Breach Report 202*.
10. Check Point Research, *2023 Global Ransomware Trends Report*.
11. Convention on Cybercrime (Budapest Convention), Council of Europe, ETS No.185 (2001).
12. Information Technology Act 2000 (India), ss 43–66.
13. Information Technology (Amendment) Act 2008, Gazette Notification No. 10 of 2009.
14. *Shreya Singhal v Union of India* (2015) 5 SCC 1.
15. *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
16. Regulation (EU) 2016/679 (General Data Protection Regulation).