# A study on financial cyber-crimes, trends, patterns, and its effects in the economy.

**Abhijith Sunny***

Department of Criminology, Nirmala College, Muvattupuzha, Kerala, India

## Abstract

**This study focuses on financial cybercrimes, examining their trends, patterns, and impact on the economy. Financial cybercrimes pose significant threats to individuals, businesses, and governments, necessitating a comprehensive understanding of their nature and consequences. By analyzing the evolving tactics and techniques employed by cybercriminals targeting financial systems, institutions, and individuals, policymakers, cybersecurity professionals, and law enforcement agencies can develop effective strategies to prevent and mitigate such attacks. Financial cyber crimes have far-reaching consequences for the economy, resulting in substantial financial losses, decreased trust in online transactions, and disrupted critical infrastructure and services. These impacts extend beyond immediate financial losses, affecting productivity, investment decisions, and consumer confidence. To address the economic impact of financial cybercrimes, stakeholders must prioritize cybersecurity investments, implement robust authentication protocols, and foster cybersecurity awareness. Additionally, comprehensive regulations and international cooperation are necessary to deter cyber criminals and facilitate coordinated responses to cross-border cybercrimes. Through in-depth studies, this research aims to enhance our understanding of financial cybercrimes, identify emerging trends, and develop proactive strategies to mitigate their impact, ultimately safeguarding the economy and building a resilient digital ecosystem.**

**Keywords:** Cyber crimes, Economic models of cyber crimes, Cyberspace crime prevention models.

## Introduction

Cybercrime has become a major concern in the modern era, as technology has become an essential part of our daily lives. The internet and other digital technologies have made our lives easier and more efficient, but they have also created new avenues for criminal activity. Cybercrime refers to any illegal activity that involves the use of computer networks or digital technologies. This can include activities such as hacking, online fraud, identity theft, and cyberbullying [1]. The growth of the internet and digital technologies has created new opportunities for criminals to engage in illegal activities. Cybercriminals can operate from anywhere worldwide and target individuals, businesses, and governments. They can steal personal information, financial data, and sensitive business information, causing significant financial losses and reputational damage. Cybercrime has evolved over the years, becoming more sophisticated and complex. Hackers and cybercriminals have developed new methods and tools to evade detection and carry out their illegal activities. They can use malware, phishing scams, and other tactics to gain access to computer systems and networks, steal data, and disrupt operations. The impact of cybercrime is significant, and it affects individuals and organizations of all sizes. Individuals can suffer financial losses, identity theft, and emotional distress, while businesses can lose sensitive information, suffer reputational damage, and face legal action. Governments and other organizations may also suffer from cyber attacks, leading to the compromise of critical infrastructure and national security. In response to the growing threat of cybercrime, governments, and law enforcement agencies have implemented new laws and regulations to combat these activities. Cyber security measures such as firewalls, anti-virus software, and encryption are now widely used to protect against cyber attacks. However, cybercriminals continue to develop new methods and tools to evade these measures. As the world becomes increasingly connected and reliant on technology, the threat of cybercrime will continue to grow. It is essential that individuals, businesses, and governments remain vigilant and take steps to protect themselves against these threats. This may involve investing in cybersecurity measures, training employees on best practices, and raising awareness about the risks of cybercrime. The growth of the internet and digital technologies has created new opportunities for criminals to engage in illegal activities. The evolution of cybercrime means that new threats will continue to emerge [2].

***Correspondence to:** Abhijith Sunny, Department of Criminology, Nirmala College, Muvattupuzha, Kerala, India. E-mail: sunnyabhijith2018@gmail.com

***Received:** 07-Jan-2023, Manuscript No. AARA-23-114148; **Editor assigned:** 09-Jan-2023, PreQC No. AARA-23-114148 (PQ); **Reviewed:** 23-Jan-2023, QC No. AARA-23-114148; **Revised:** 27-Jan-2023, Manuscript No. AARA-114148 (R); **Published:** 07-Feb-2023, DOI: 10.35841/aara-7.1.186*

***Citation:** Sunny A, A study on financial cyber-crimes, trends, patterns, and its effects in the economy. Addict Criminol. 2024;7(1):186*

## *Economic Models of Financial Cyber Crimes*

Financial cyber crimes are a growing concern in the modern digital age. As such, various economic models have been developed to explain the behavior of cybercriminals, their motivations, and the impact of their activities on the economy. Here are a few economic models that are commonly used to study financial cyber crimes.

## *Rational Choice Theory Model*

Rational choice theory can be applied to financial cyber crimes by assuming that cybercriminals are rational actors who weigh the costs and benefits of engaging in criminal activities. The theory suggests that cybercriminals will continue to engage in cybercrime as long as the perceived benefits outweigh the costs. In the context of financial cyber crimes, the benefits may include financial gain, access to sensitive information, or damage to a competitor. The costs may include the risk of being caught, legal penalties, and damage to reputation. Cybercriminals will weigh these costs and benefits before deciding whether to engage in a particular criminal activity. For example, a cybercriminal may choose to engage in phishing scams because they perceive the benefits of stealing personal or financial information to be greater than the costs of being caught. On the other hand, they may choose not to engage in more sophisticated cyberattacks that require a higher level of technical expertise and carry a greater risk of detection [1].

The application of rational choice theory to financial cyber crimes can inform the development of prevention and mitigation strategies. For instance, increasing the cost of cybercrime through stronger legal penalties, improved cybersecurity measures, and increased law enforcement can make engaging in cybercrime less attractive to rational actors. Furthermore, educating individuals and organizations about the risks and consequences of cybercrime can increase the perceived costs of engaging in such activities, reducing the likelihood of such crimes being committed. In summary, the rational choice theory provides a useful framework for understanding the behavior of cybercriminals and developing effective prevention and mitigation strategies to reduce financial cyber crimes [2].

## *Game Theory Model*

Game theory is a mathematical framework used to analyze strategic interactions between two or more decision-makers. In the context of financial cybercrime, game theory can be used to model the strategic interactions between cybercriminals and their potential victims, as well as between cybercriminals and law enforcement agencies. One common game theory model used in the study of financial cybercrime is the prisoner's dilemma. In this model, two cybercriminals are arrested for cybercrime and are interrogated separately. [1] Each criminal has the option to cooperate with the authorities and confess to the crime, or to remain silent and risk a lesser charge if the other criminal confesses. The optimal strategy for each criminal depends on the strategy chosen by the other criminal. If both criminals remain silent, they both face lesser charges. However, if one confesses and the other remains silent, the confessing criminal will receive a reduced sentence while the silent criminal will face a more severe sentence. If both criminals confess, they will both receive a moderate sentence [2].

Another game theory model used in the study of financial cybercrime is the stag hunt game. In this model, two cybercriminals have the option to cooperate and engage in a profitable cybercrime or to defect and engage in a less profitable cybercrime. However, if one criminal defects and the other cooperates, the defector will receive a greater reward while the cooperator will receive no reward. If both criminals defect, they will both receive a lesser reward. In the context of financial cybercrime, these game theory models can be used to inform strategies for law enforcement agencies and organizations to prevent and deter cybercrime. For example, by increasing the potential rewards for cooperating with law enforcement agencies and by increasing the penalties for cybercrime, the incentive for cybercriminals to cooperate may be increased. Additionally, by implementing strong cybersecurity measures and conducting regular vulnerability assessments, organizations can reduce the potential rewards for cybercriminals and increase the costs associated with engaging in financial cybercrime. Another game theory model used in the study of cybercrime is the public goods game. In this model, multiple players have the option to contribute to a public good, such as a cybersecurity system, or to defect and not contribute. The optimal strategy for each player depends on the strategies chosen by the other players and the benefits and costs associated with contributing to the public good [1].

## *Risk Analysis Model*

This model involves assessing the potential risks and costs associated with different cybercrime scenarios. This could involve analyzing the potential financial losses for victims of cybercrime, as well as the potential costs of implementing various cybersecurity measures. Risk analysis can be useful for understanding the broader economic impacts of cybercrime and the ways in which society can mitigate these risks [4]. A risk analysis model for financial cybercrime should consider the following factors:

**Threats:** Identify the types of threats that are prevalent in financial cybercrime, such as hacking, phishing, malware, insider threats, etc.

**Vulnerabilities:** Analyze the potential weaknesses in the financial systems that may be exploited by cybercriminals. This can include weak passwords, unsecured networks, outdated software, and more.

**Consequences:** Consider the potential consequences of a successful cyber attack, such as financial loss, reputational damage, legal and regulatory consequences, and more.

**Likelihood:** Assess the likelihood of a successful cyber attack occurring based on factors such as the volume of transactions, the level of security in place, and the sophistication of potential attackers.

**Risk assessment:** Combine the above factors to calculate the overall risk of financial cybercrime, and prioritize the highest risk areas for mitigation and prevention.

**Mitigation:** Develop and implement strategies to mitigate the identified risks, such as improving security measures, training employees on cybersecurity best practices, and implementing incident response plans.

**Continuous monitoring:** Regularly monitor and update the risk analysis model to ensure it remains up to date with changing threats and vulnerabilities, and adjust mitigation strategies as necessary.

Overall, a comprehensive risk analysis model for financial cybercrime should take a holistic approach that considers all aspects of the organization's financial systems and operations and involves ongoing monitoring and adaptation to evolving threats and risks [1].

### *Behavioural Economic Model*

Behavioral economics provides a useful framework for understanding financial cybercrime, as it acknowledges that human decision-making is not always rational, and can be influenced by various biases and heuristics. Some of the key concepts from behavioral economics that can be applied to financial cybercrime are the following:

**Prospect Theory**: Prospect theory, developed by psychologists Daniel Kahneman and Amos Tversky, explains how individuals make decisions under uncertainty. The theory suggests that people tend to be risk-averse when it comes to gains, but risk-seeking when it comes to losses. This has implications for financial cybercrime, as cybercriminals can exploit this tendency to steal money and sensitive information from victims. In the context of financial cybercrime, prospect theory can help us understand why individuals might fall victim to phishing attacks or other scams [5]. For example, a phishing email might offer a gain, such as a prize or discount, but in reality, is designed to steal personal or financial information. Because people are risk-averse when it comes to gains, they may be more likely to click on a link or enter their information in order to secure the supposed gain. On the other hand, cybercriminals can also exploit the risk-seeking behavior of individuals when it comes to losses. For example, they may create a sense of urgency or fear, such as threatening to delete a victim's data or exposing sensitive information, in order to prompt them to make a hasty decision without considering the potential risks. Overall, a prospect theory approach to financial cybercrime suggests that cybercriminals may exploit people's decision-making biases to their advantage [6]. To mitigate this risk, it is important to provide education and awareness to individuals about the risks of financial cybercrime and how to recognize and avoid scams. Additionally, implementing strong security measures and protocols can reduce the likelihood of successful attacks, and implementing systems for reporting and responding to incidents can help mitigate the harm caused by financial cybercrime [2].

**Anchoring**: Anchoring is a psychological manipulation technique that is commonly used by cybercriminals to facilitate financial fraud. Anchoring involves setting a reference point or benchmark in a person's mind, which can influence their subsequent decisions and actions. In the context of financial cybercrime, anchoring can be used in a variety of ways. For example, a cybercriminal might send a phishing email to a potential victim that includes a fake invoice for a small amount of money. This invoice serves as an anchor point, which makes subsequent requests for larger sums of money seem more reasonable and legitimate. Another example of anchoring in financial cybercrime is when a cybercriminal gains access to a victim's online banking account and sets up a small, recurring transfer to a fake account [4]. This creates an anchor point for the victim, who may not notice the small transfer and will be less likely to suspect larger transfers to the same account. Overall, anchoring is a powerful psychological manipulation tool that can be used to facilitate financial cybercrime. To protect themselves, individuals and businesses should be wary of any requests for money or sensitive information, particularly if they involve small amounts that could be used as an anchor point for larger requests. Additionally, strong security measures such as two-factor authentication and regular monitoring of financial accounts can help to prevent cybercriminals from gaining access to sensitive information or funds [2].

**Social proof:** Social proof refers to the tendency for people to rely on the actions or opinions of others in order to make decisions. Cybercriminals can use social proof by creating fake reviews or testimonials that promote their products or services, or by impersonating someone trusted in order to gain access to sensitive information.

**Scarcity**: Scarcity refers to the perception that a resource is limited or scarce, which can increase its perceived value. Cybercriminals can create a sense of scarcity by using fake countdown timers or limited-time offers, which can increase the likelihood of victims making impulsive decisions without fully considering the risks [10].

The behavioral economic model of financial cybercrime should consider how human biases and heuristics can be exploited by cybercriminals in order to influence victims' decisions and actions. It should also focus on developing interventions that address these biases and promote more rational decision-making in the face of cyber threats. This may involve strategies such as education and awareness campaigns, improved user interfaces and decision-making tools, and stronger legal and regulatory frameworks to protect consumers from financial cybercrime [1].

### *The Demand and Supply Model*

The demand and supply model of financial cybercrime refers to the economic factors that drive the market for cybercriminal activities, including the demand for stolen financial data and the supply of the tools and services needed to carry out cyber attacks. On the demand side, there is a growing market for stolen financial data, such as credit card numbers, bank account details, and personal identification information (PII). This demand comes from a range of criminal groups and individuals, including identity thieves, fraudsters, and money

launderers. These actors seek to use stolen financial data to make fraudulent purchases, open fraudulent accounts, or launder money through the banking system [7].

On the supply side, cybercriminals are constantly developing and improving their tools and services for carrying out cyber attacks. This includes the development and sale of malware, such as keyloggers and ransomware, as well as the creation of online marketplaces and forums where stolen financial data can be bought and sold. The supply of cybercrime tools and services is driven by the profit motive, as cybercriminals seek to maximize their profits by creating and selling effective tools and services to other criminals. At the same time, the demand for stolen financial data is also driven by the potential profits that can be made from fraudulent activities. The interaction between supply and demand in the market for financial cybercrime can create a vicious cycle, as the profits generated by successful cyber attacks can fuel further demand for stolen financial data and encourage more cybercriminals to enter the market. Overall, the demand and supply model of financial cybercrime highlights the economic incentives that underlie this type of criminal activity and the challenges faced by law enforcement and the financial industry in combatting it [1].

### *Theory of Information Asymmetry Model*

Anderson's Theory of Information Asymmetry is a theory in economics that explains how information asymmetry can lead to market failure. The theory was developed by James E. Anderson, an American economist, in 1979. According to Anderson's theory, information asymmetry occurs when one party in a transaction has more information than the other party. This information asymmetry can create a situation where the party with less information is at a disadvantage, as they are unable to make informed decisions. This can lead to market failure, as the party with less information may not be willing to participate in the transaction, or may be willing to participate only at a price that is unfavorable to the other party [3]. Anderson's Theory of Information Asymmetry can also be applied to financial cybercrime. In this context, the theory suggests that cybercriminals may have more information about vulnerabilities in a system or network than the defenders who are responsible for protecting it. This information asymmetry can allow cybercriminals to exploit the system or network in ways that defenders are unable to anticipate or prevent. For example, a cybercriminal may have information about a particular software vulnerability that has not yet been discovered by the software developer. The cybercriminal can then exploit this vulnerability to gain unauthorized access to the system or network, steal sensitive data, or carry out other malicious activities [8].

To address this information asymmetry, financial institutions can take several measures, such as improving their cybersecurity defenses, investing in threat intelligence and sharing information with other institutions, and working with law enforcement agencies to identify and prosecute cybercriminals. Overall, Anderson's Theory of Information Asymmetry provides a useful framework for understanding the challenges associated with financial cybercrime and for developing effective strategies to address these challenges [1].

## Review of Literature

Cybercrime has become a significant threat to the global economy, affecting individuals, businesses, and governments worldwide. Cybercriminals are exploiting vulnerabilities in the digital infrastructure to steal sensitive information, commit fraud, and disrupt essential services. This literature review examines the impact of cybercrime on the economy and highlights recent research on this topic [5]. Several studies have examined the impact of cybercrime on the economy, and they have found that the costs of cybercrime are significant and increasing. According to a report by the Center for Strategic and International Studies (CSIS), cybercrime costs the global economy up to $600 billion annually. The report estimated that the costs of cybercrime would increase to $10.5 trillion annually by 2025. Another study by the World Economic Forum (WEF) identified cybercrime as one of the top five risks to the global economy in terms of likelihood and impact. The study estimated that cybercrime would cost the global economy $3 trillion by 2020 [9].

Furthermore, cybercrime has a significant impact on businesses, particularly small and medium-sized enterprises (SMEs). A study by the National Cyber Security Alliance (NCSA) found that 60% of small businesses that experience a cyberattack go out of business within six months. The study also estimated that the cost of a single cyberattack could range from $84,000 to $148,000 for an SME. Several recent studies have focused on the impact of cybercrime on the economy and identified the challenges facing businesses and governments in mitigating cyber risks [10]. A study by the Organization for Economic Cooperation and Development (OECD) examined the economic impact of cybercrime and identified the need for a comprehensive approach to addressing cyber risks. The study highlighted that businesses and governments need to work together to develop effective policies and strategies to prevent cybercrime. Another study by the International Monetary Fund (IMF) examined the impact of cybercrime on the financial sector and identified the risks posed by cyberattacks to financial stability [6]. The study called for financial institutions to improve their cybersecurity measures and be prepared to respond to cyberattacks. One of the trends identified in financial cybercrime is the use of malware to steal financial information. Malware can be used to gain access to financial institutions' systems or to extract data from victims' devices. According to a study by the Ponemon Institute, 69% of financial institutions experienced malware attacks in 2018 [11].

## Methodology of the Study

### *Objectives of the Study*

- To analyze the trends and patterns of cybercrime in India and the USA
- To analyze the trends and patterns of financial cybercrime in India and the USA
- To study the impact of financial cybercrime in both economies

- To study the crime prevention models and strategies to prevent cyber crimes and financial cyber crimes

### *Study Sample and Data Collection Methods*

In research studies, sampling refers to the process of selecting a subset of individuals, cases, or elements from a larger population to represent that population and draw meaningful inferences. Sampling plays a critical role in ensuring the validity and generalizability of research findings, as it is often impractical or impossible to collect data from the entire population of interest. By selecting a representative sample, researchers can obtain insights and make inferences about the larger population. The process of sampling involves careful consideration of various factors, including the research objectives, the characteristics of the population, the desired level of accuracy, and the available resources. The goal is to select a sample that accurately reflects the characteristics and diversity of the population, allowing for meaningful analysis and drawing valid conclusions. For studying the financial cybercrimes we have collected various secondary data published by various governments and cyber security policies and strategies developed by prestigious institutions like Interpol. For analyzing the trends patterns and growth of cybercrime and its financial aspect we have collected data from the Crime in India report published by NCRB [7] and the Internet Crime Report published by the FBI [4]. The sampling method used to collect data is convenient sampling.

### *Statistical Analysis of the Study*

Statistical analysis is a fundamental component of research that involves the systematic collection, organization, and interpretation of data. It provides a powerful toolkit for researchers to uncover patterns, relationships, and insights from their data, enabling them to draw meaningful conclusions and make informed decisions. In the context of a study, statistical analysis plays a crucial role in examining research questions, testing hypotheses, and deriving evidence-based conclusions. The primary goal of statistical analysis is to analyze data in a rigorous and systematic manner, transforming raw data into meaningful information. It involves applying a range of statistical techniques and methods to summarize, describe, visualize, and infer from the data. All statistical analyses were done with software like SPSS, Gretl, and STATA. In order to analyze the rate of growth of cybercrimes and various financial cyber crimes in India and the USA, a Linear regression test was conducted using SPSS software. The dependent variable in this analysis is the cybercrimes reported in India and USA in the last twenty years and the independent variable is the time or the year. During the analysis, a notable finding was the structural break in the two nations in different years. So the structural break was analyzed with the software named STATA. Wald test was conducted to analyze the structural break and found the results with the help of this software [3].

## Analysis of the Study

### *Rate of Growth of Cyber Crime in India*

This section deals with the rate of growth of cybercrime in India. In order to analyze the rate of cybercrime in India, we used regression analysis and the results of the test are the following (Table 1) (Figure 1)

***Table 1.*** *Model Summary and Parameter Estimates (India).*

| Dependent Variable: India | | | | | | | |
|---|---|---|---|---|---|---|---|
| Model Summary | | | | | | Parameter Estimates | |
| Equation | square | F | df1 | df2 | Sig. | constant | b1 |
| Exponential | .981 | 907.913 | 1 | 18 | <.001 | 11.778 | .407 |

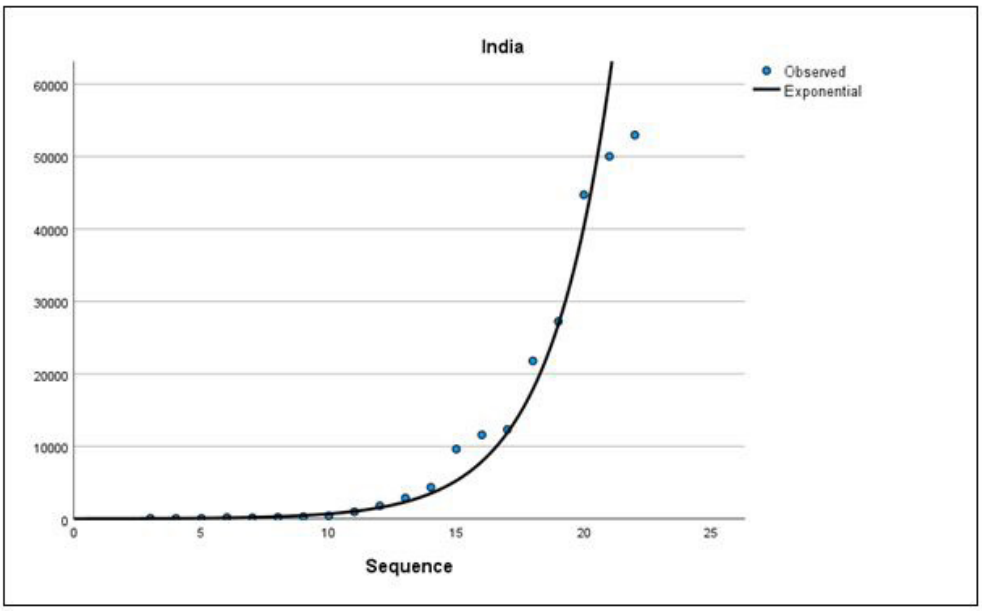


***Figure 1.*** *Rate of Growth of Cyber Crime in India.*

***Citation:*** *Sunny A, A study on financial cyber-crimes, trends, patterns, and its effects in the economy. Addict Criminol. 2024;7(1):186*

The output provided is from a statistical regression analysis of the dependent variable against a single independent variable in the Exponential model. Here is an analysis of the results:

**R Square:** This value represents the proportion of variance in the dependent variable that can be explained by the independent variable in the model. The R Square value for the Exponential model is 0.981, indicating a strong relationship between the independent and dependent variables.

**F:** This value is the result of an F-test that tests the overall significance of the model. The F value for the Exponential model is 907.913, which is statistically significant, indicating that the model is significant and can provide useful information.

**df1 and df2:** These values represent the degrees of freedom for the model. df1 is the number of independent variables, and df2 is the number of observations minus the number of independent variables. In the Exponential model, df1 is 1 and df2 is 18.

**Sig:** This value represents the significance level of the F-test. The Sig value for the Exponential model is less than 0.05, indicating that the model is significant at the 95% confidence level.

**Constant and b1:** These values are the parameter estimates for the intercept and coefficient for the independent variable in the model. The values for the Exponential model are 11.778 and 0.407, respectively. These values provide information about the relationship between the independent and dependent variables.

## *Rate of Growth of Cybercrime in the USA*

This section deals with the rate of growth of cybercrime in the USA. In order to analyze the rate of cybercrime in India, we used regression analysis and the results of the test are the following (Table 2) (Figure 2)

The model summary shows that the R-squared value is 0.913, which indicates that the model explains a high proportion (91.3%) of the variance in the dependent variable. The F-statistic has a value of 62.951 with a p-value of 0.000, which suggests that the overall model is statistically significant. Moving on to the parameter estimates, the constant (intercept) term is -181361.676. This means that when all the independent variables in the model are zero, the expected value of the dependent variable is approximately -181,362. The coefficients for the independent variables are b1 = 137539.444, b2 = -13643.699, and b3 = 429.460. It's not clear from the information provided what the independent variables represent, but the coefficients indicate the expected change in the dependent variable for a one-unit increase in each independent variable, holding all other variables constant. For example, for every one-unit increase in b1, we expect the dependent variable to increase by 137,539.44 units (assuming b2 and b3 remain constant).

## *Trends of Cyber Crime in India and the USA*

This section deals with the trend of cybercrime in India and the USA. The data to analyze the trend is from the Crime in India report and Internet Crime Report. Following are the findings of the trends of cybercrime (Figure 3)

From the graph, the result shows that there is a structural break at a certain point in time. In order to know more about the details of a structural break Wald test for a structural break was performed. Structural break refers to a significant

***Table 2.*** *Model Summary and Parameter Estimates (US).*

| Dependent Variable: US | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Model Summary | | | | | | Parameter Estimates | | | |
| Equation | square | f | df1 | df2 | Sig. | constant | b1 | b2 | b3 |
| Cubic | .913 | 62.951 | 3 | 18 | <.001 | -181361.676 | 137539.444 | -13643.699 | 429.460 |

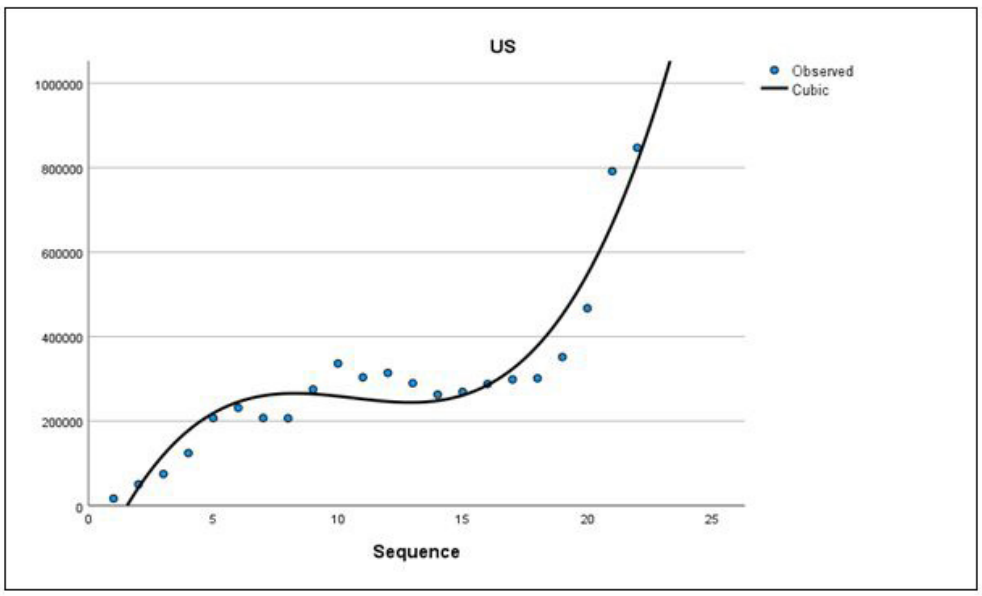


***Figure 2.*** *Rate of Growth of Cyber Crime in US.*

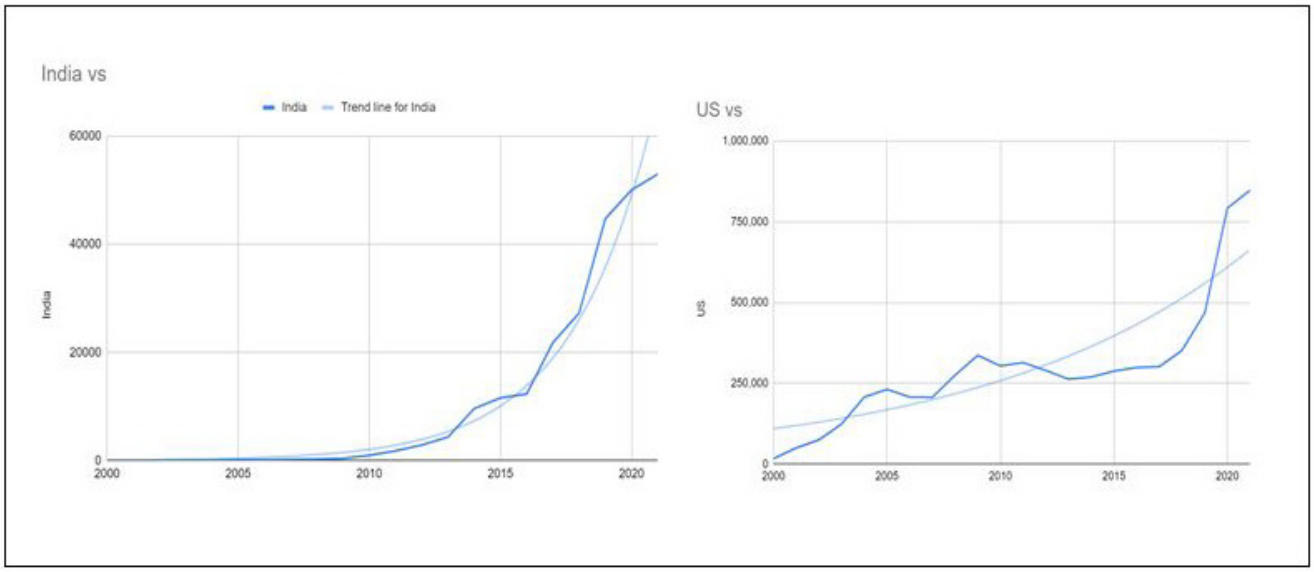


***Figure 3.*** *Rate of Growth of Cyber Crime in India and the USA.*

change in the underlying structure of a time series data. This change can be sudden or gradual and can be caused by various factors such as economic policy changes, natural disasters, or technological advancements. Structural breaks can significantly impact the analysis and forecasting of time series data as they can lead to changes in the relationships between variables, and can affect the accuracy of statistical models. Therefore, it is important to identify and account for structural breaks when analyzing time series data. The Wald test is a statistical test used to determine whether a structural break has occurred in time series data. It compares the estimates of the model parameters before and after a certain point in time to see if they are statistically different. If the test indicates that there is a significant difference in the estimates, a structural break is said to have occurred. The Wald test is commonly used in econometric analysis to detect changes in economic relationships over time. It is important to identify structural breaks because they can have a significant impact on analysis and forecasting. The Wald test is a statistical test used to determine whether a particular parameter in a model is significantly different from a hypothesized value. In the context of detecting a structural break in a time series model, the Wald test can be used to test whether the coefficients before and after the break are significantly different from each other. The formula for the Wald test statistic is

$$W = [(\theta\_hat - \theta\_0) / SE(\theta\_hat)]^2$$

where θ_hat is the estimated value of the parameter, θ_0 is the hypothesized value of the parameter, and SE(θ_hat) is the standard error of the estimated parameter. The test statistic follows a chi-squared distribution with one degree of freedom under the null hypothesis that there is no structural break. If the calculated value of W is greater than the critical value of the chi-squared distribution, then the null hypothesis is rejected and a structural break is detected. (Table 3) (Table 4)

H0: There is no structural break in the cybercrime pattern of India

H1: There is a structural break in the cybercrime pattern of India

(Table 5)

H0: There is no structural break in the cybercrime pattern of the USA

H1: There is a structural break in the cybercrime pattern of the USA

The test result is that in India there is a structural break in the pattern of cybercrime in 2015 and there is a structural break in the USA in the year 2015. There are many reasons for this pattern changes which will be discussed in the findings.

### *The Pattern of Financial Cybercrime in India and the USA*

This section deals with the pattern of financial cybercrime in India and the USA. There are certain types of financial cybercrime that are analyzed to find the pattern of financial cybercrime. The most prominent five financial cybercrimes in both nations are malware attacks, identity theft, online banking frauds, lottery frauds, etc. following are the data regarding financial cybercrime:- (Table 6) (Figure 4) (Table 7) (Figure 5).

## Crime Prevention Model for Financial Cybercrime

The crime Prevention Model deals with the various aspects that help to prevent cybercrimes in a more comprehensive manner. Various conventions and conferences have identified various mechanisms to prevent cybercrime in a more comprehensive manner like the Budapest convention etc. This cybercrime prevention model has adopted certain elements from the international and national conventions and created a unique and feasible crime prevention model for cybercrime. The five main elements of this model are Legal, Technical, Organizational, Capacity Building, and Psychological. (Figure 6)

***Table 3.*** *Trends of Cyber Crime in India and the US.*

| Regress India Year | | | | | | |
|---|---|---|---|---|---|---|
| Source | SS | df | MS | Number of Observation | 20 | |
| Model | 4.2446e+09 | 1 | 4.2446e+09 | F(1,18) | 43.11 | |
| Residual | 1.7721e+09 | 18 | 98452450.1 | Prob>F | 0.0000 | |
| Total | 6.167_09 | 19 | 316668859 | R-squared | 0.7055 | |
| | | | | Adj R- squared | 0.6891 | |
| | | | | Root MSE | 9922.3 | |
| **India** | **Coefficient** | **Std. err.** | **t** | **P >\|t\|** | **[95% conf. interval]** | |
| | 2526.421 | 384.7711 | **6.57** | 0.000 | 1718.047 | 3334.795 |
| Year-conc | -5069808 | 773970.2 | -655 | 0.000 | -6695859 | -3443757 |

***Table 4.*** *No structural break in India and US.*

| Test | Statistic | p-value |
|---|---|---|
| Supremum wald | 207.5475 | 0.000 |

***Table 5.*** *Trends of Cyber Crime in USA.*

| Regress US Year | | | | | | |
|---|---|---|---|---|---|---|
| Source | SS | df | MS | Number of Observation | 22 | |
| Model | 5.6014e+11 | 1 | 5.6014e+11 | F(1,20) | 41.36 | |
| Residual | 2.7086e+11 | 20 | 1.3543e+10 | Prob>F | 0.0000 | |
| Total | 8.3100e+11 | 21 | 3.9572e+10 | R-squared | 0.6741 | |
| | | | | Adj R- squared | 0.6578 | |
| | | | | Root MSE | 1.2e+05 | |
| **US** | **Coefficient** | **Std. err.** | **t** | **P >\|t\|** | **[95% conf. interval]** | |
| | 25150.94 | 3910.796 | 6.43 | 0.000 | 16993.17 | 33308.72 |
| Year-conc | -5.03e+07 | 7862694 | -6.39 | 0.000 | -6.67e+07 | -3.39e+07 |

***Table 6.*** *The Pattern of Financial Cybercrime in India and the USA.*

| | **Ransomware attacks** | **Identity theft** | **Credit & debit fraud** | **ATM Frauds** | **Online banking frauds** | **OTP frauds** |
|---|---|---|---|---|---|---|
| 2021 | 648 | 4071 | 1624 | 1899 | 4823 | 2028 |
| 2020 | 727 | 5148 | 1194 | 2160 | 4047 | 1093 |
| 2019 | 1023 | 12255 | 367 | 2067 | 2093 | 549 |
| 2018 | 1218 | 6688 | 309 | 1284 | 968 | 319 |
| 2017 | 300 | 3724 | 395 | 1543 | 804 | 334 |
| **Slope** | **20.5** | **-84.6** | **334.3** | **158.8** | **1111.7** | **416.2** |

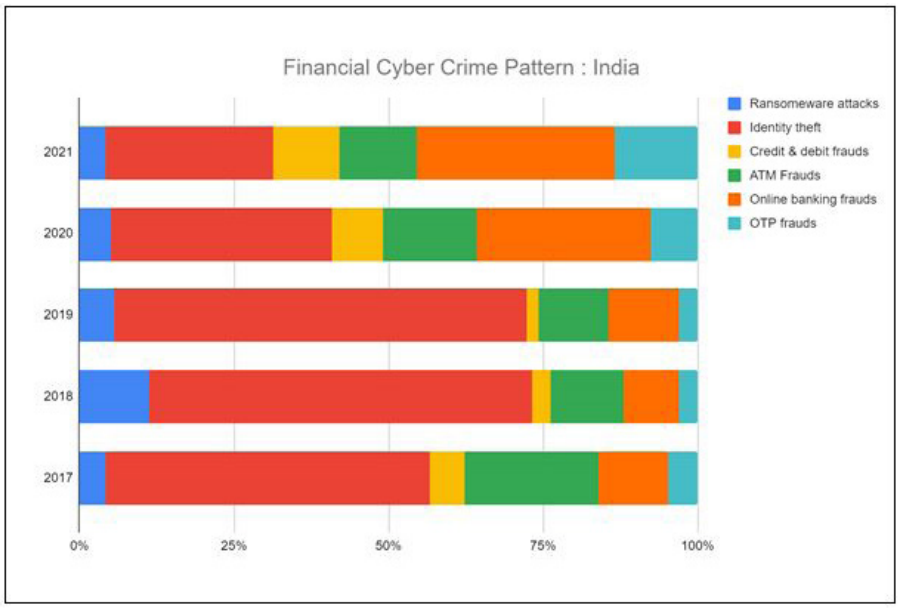


***Figure 4.*** *The Pattern of Financial Cybercrime in India.*

***Table 7.*** *The pattern of Financial Cybercrime in the USA.*

| | Ransomware attacks | Identity theft | Credit & debit fraud | Online banking frauds | OTP frauds | Lottery fraud |
|---|---|---|---|---|---|---|
| 2021 | 3,729 | 51,629 | 16,750 | 120456 | 24,299 | 5,991 |
| 2020 | 2,385 | 43,330 | 17,614 | 93037 | 23,751 | 8,501 |
| 2019 | 2,474 | 16,053 | 14,378 | 80786 | 19,473 | 7,767 |
| 2018 | 1,783 | 16,128 | 15,210 | 68987 | 18,493 | 7,146 |
| 2017 | 1,493 | 17,636 | 15,220 | 64894 | 15,372 | 3,012 |
| 2016 | 2,673 | 16,878 | 15,895 | | | 4,231 |
| **Slope** | **247.0571429** | **7164.628571** | **303.5714286** | **13517.4** | **2311.2** | **739.6571429** |

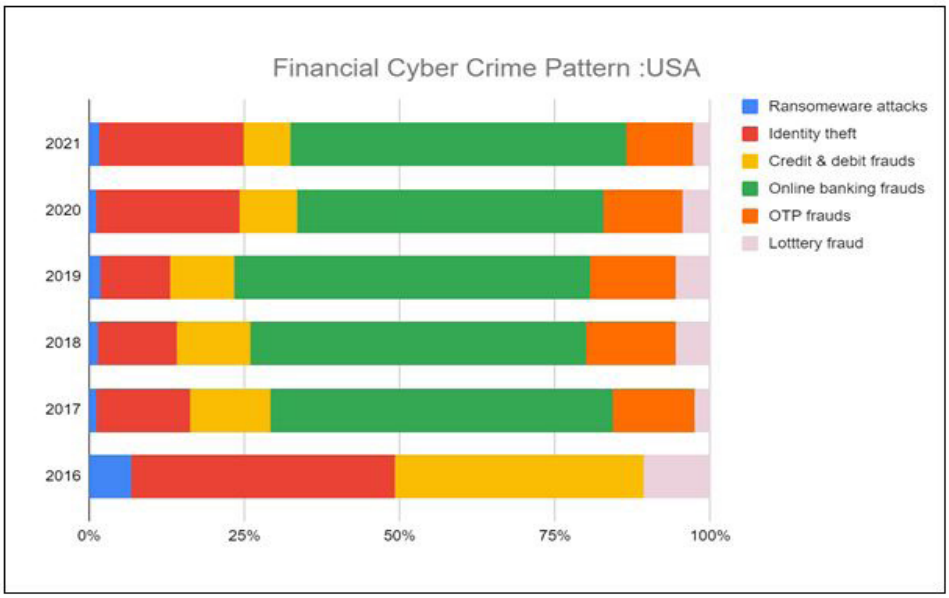


***Figure 5.*** *The pattern of Financial Cybercrime in the USA.*

Cyber Crime has a transnational effect, so with close collaboration with all the nations, proper solutions can be enacted. The global agencies should be in leadership for implementing the framework that helps in reducing cybercrime and proactively responding to cybercrime. These five elements will help to prevent cybercrimes to a certain limit. Each of these elements can be further divided into certain perspectives to prevent offenses. There should be proper legal mechanisms to prevent these types of crimes. Because of its transnational nature, there should be a close collaboration with other nations to make a unique code or law that explains and criminalizes each crime. Each law or code should be equipped with the proper technology and capabilities that ensure the safety and security of all citizens. There should be proper organization. (Figure 7)

The first main aspect of the crime prevention model is the legal framework. There are four factors in the legal framework in which cybercrimes can be effectively prevented. With proper legislation, we can effectively and comprehensively prevent a crime. Implementing an International Penal Code for Cyber Crimes, International Criminal Procedure Code, and International Evidence Act for effective penalization, evidence collection, and investigation of cybercrimes in an effective manner. Cyber crimes have a transnational nature so there should be an international law that needs to be enacted for the protection and surveillance of cyberspace. There are many hurdles to enacting and implementing these types of international codes. One of the main drawbacks is who will enact and implement it. Will the UNO be capable of that in this present economic and political scenario which failed to normalize situations in Ukraine and take strong actions against Russia? In many nations some cybercrimes are legal and some are not. There are various fluctuations in enacting and implementing laws. It is the national interest of each and every nation to enact and penalize any crimes. So to enact and implement these types of laws or codes, each nation should sacrifice its national interest over collective well-being, which is the need of the hour. So the nations under UNO should consider enacting an international code that penalizes these crimes. (Figure 8)

The next stage of the crime prevention model comprises the technical framework. It includes the development of advanced surveillance mechanisms for cyberspace. It is time to develop some software for crime prevention that prevents cybercrime attacks of an unknown person. There should be a proactive mechanism to give alerts of cybercrime to citizens which will help to bring down cybercrime to a certain extent. Defense-in-depth model is a cyber-security model that provides multiple layers of security services [9]. It involves implementing various security measures at different levels to create overlapping layers of defense. These types of security services should be provided for enhancement of the security. There


***Figure 6.*** *Crime Prevention Model for Financial Cybercrime.*

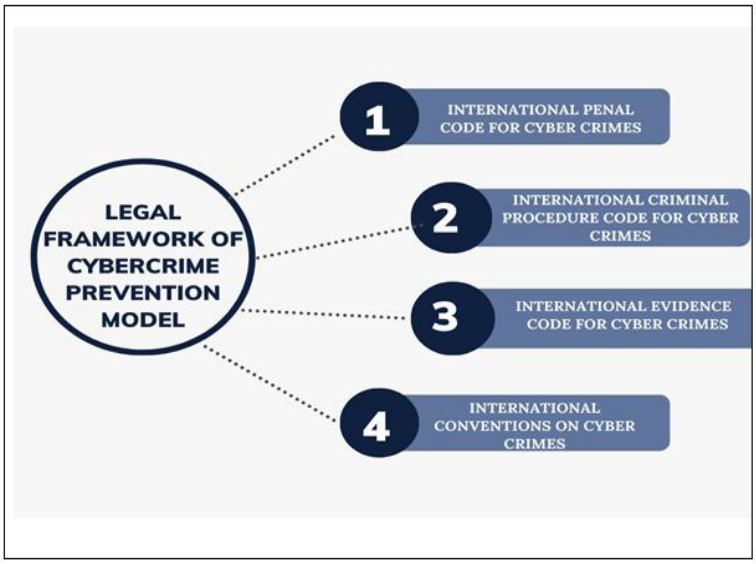


***Figure 7.*** *Legal Framework of Cybercrime Prevention Model.*

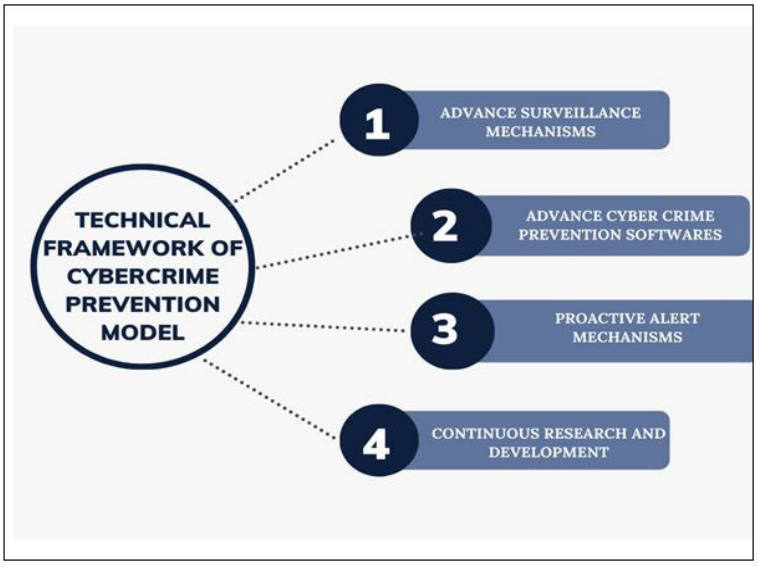


***Figure 8.*** *Technical Framework of Cybercrime Prevention Model*

should be continuous research and development in these fields which will adopt the upcoming threats and also provide all preventive mechanisms for advanced threats. So these types of research and development should be enhanced. (Figure 9)

The third aspect of the crime prevention model is the organizational framework. There should be a proper organizational structure for the implementation of various crime prevention programs and their penalization and legislation. The three main proposed organizational structures are the International Court of Justice for Cybercrime, the International Investigative Agency for Cybercrime, and the International Council of Cybercrime Prevention. It is the need of the hour to initiate a unique judicial framework that focuses only on cyber-related crimes. It will also help to increase the conviction rate of cybercriminals. Each and every nation can also implement a tribunal or other judicial framework that focuses only on the judicial aspect of cybercrime. The unique investigative agency will help to investigate these types of crimes with advanced technologies and will also enhance risk assessment and prevention mechanisms. The third aspect of this is an apex council of experts from all the member nations which will foster collaboration and participation. It will also foster research and development in these areas. This organization framework will create a proper structure and enhance crime prevention strategies. (Figure 10)

Capacity building is the next major dimension of the proposed crime prevention model. The state of art infrastructure should be developed in order to provide technical and scientific methods of cybercrime prevention. The state-of-the-art infrastructure includes the international cyber forensic division which focuses on the forensic aspects and analysis of cybercrimes. In the present scenario, there are many institutions like Interpol, Europol, etc which have advanced cyber forensic divisions. It should be enhanced with experts from each and every nation and a proper code of action needs to be legislated. The next state-of-the-art infrastructure is the cybercrime prevention forum. It includes cyber forensic experts who can design and develop prevention techniques throughout the world. The next institution is a research and development forum that includes criminologists who specialize in cyber criminology and other experts related to this field. Cyber Psychological Investigation Division includes a team of forensic psychologists who assess the behavioral deviance and other psychological parameters of cyber criminals. It will also equip the cyber investigation with forensic psychological tools which will help to assess the behavioral pattern of cybercriminals. (Figure 11)

The last dimension of the cybercrime prevention model is the psychological framework of crime prevention. It includes the creation of a unique cyber criminal profiling registry that includes the information of cybercriminals throughout the world which will help in the investigation of crime as well as act as a reference database. It should be an international cyber criminal profiling registry. There should be a proper framework to assess the deviance of cyber criminals like another psychological questionnaire. The cybercrime deviance assessing framework should enhance the creation of a new psychological tool to assess the deviance of cyber criminals. In the present scenario, there are various institutions that provide proper and advanced counseling to the victims of cybercrimes. There should be continuous research and development in this field which will help to predict and adapt the coming changes in this field. Proper research should be there to assess the behavioral patterns of cybercriminals. There will be some correlation between the behavioral patterns of cyber criminals and ethnicity. It should be included in order to create a comprehensive assessing framework of cyber deviance.

## Recommendations

Following are the recommendations made to prevent cybercrime globally based on the crime prevention model of the study:-

- The study strongly recommends creating a uniform law internationally to prevent cybercrimes through legal reforms by enacting and implementing the International

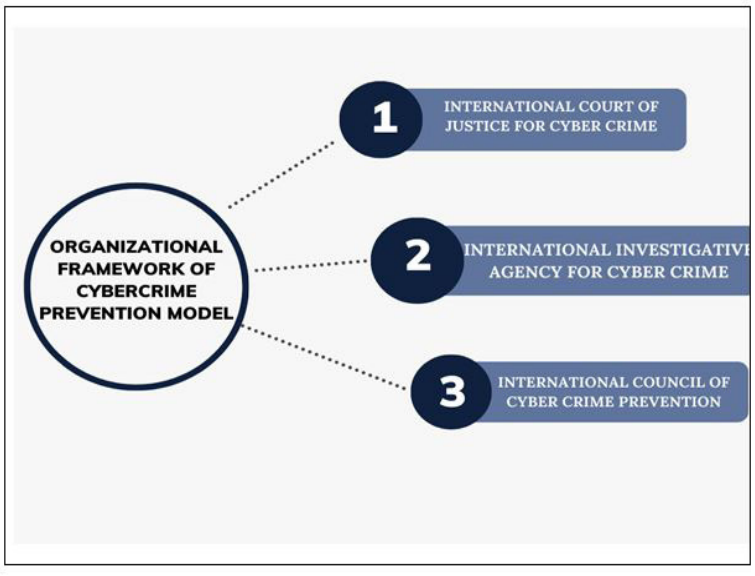


***Figure 9.*** *Organizational Framework of Cybercrime Prevention Model.*

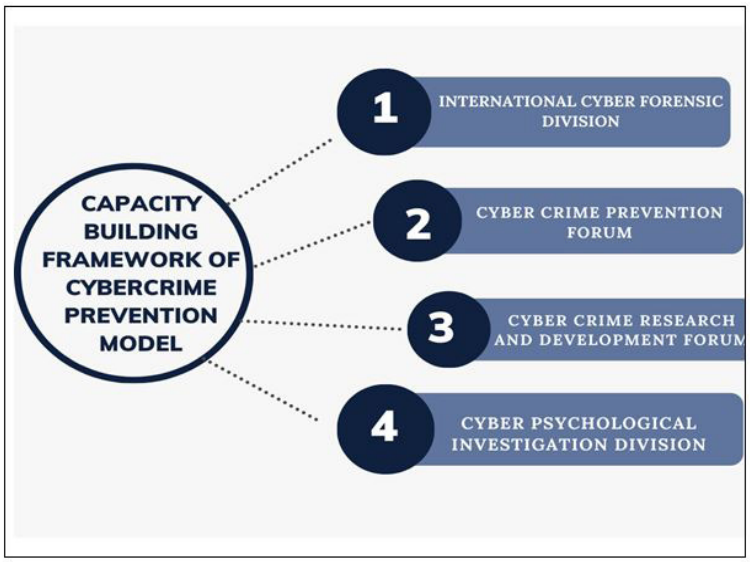


***Figure 10.*** *Capacity Building Framework of Cybercrime Prevention Model.*

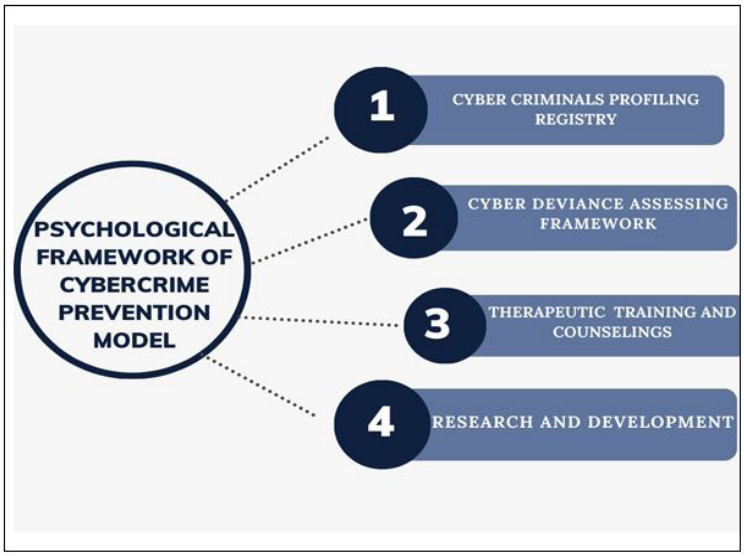


***Figure 11.*** *Physiological Framework of Cybercrime Prevention Model.*

Penal Code for Cybercrimes which mentions the details of cybercrimes and its punishment.

- The study strongly recommends creating a uniform law internationally to prevent cyber crimes through legal reforms by enacting and implementing the International Criminal Procedure Code for Cybercrimes which mentions the procedure which should be followed in the investigation and other procedures of arrest and pieces of evidence.
- The study strongly recommends creating a uniform law internationally to prevent cyber crimes through legal reforms by enacting and implementing the International Evidence Code which mentions the relevance, admissibility, and forms of evidence.
- The study strongly recommends creating a uniform law internationally to prevent cyber crimes through legal reforms by enacting and implementing the International Conventions of Cybercrime which provides more awareness and knowledge about cybercrimes and how they can be prevented in a comprehensive manner.
- The study strongly recommends creating suvellience alert mechanisms through the development of advanced technology to proactively prevent cybercrime.
- The study strongly recommends creating a uniform law internationally to prevent cyber crimes through legal reforms by enacting and implementing the International Court of Justice for Cybercrime which helps to improve the efficiency of conviction of cybercrimes.
- The study strongly recommends creating a uniform law internationally to prevent cyber crimes through legal reforms by enacting and implementing the International Investigative Agency for Cybercrimes which provides a

uniform and technical investigation of cybercrime as it has a transnational nature.

- The study strongly recommends creating a uniform law internationally to prevent cyber crimes through legal reforms by enacting and implementing the International Council of Cybercrimes which is an expert panel consisting of cyber experts, criminologists, lawyers, and Psychologists.

## Conclusion

In conclusion, a study on financial cybercrimes, including their trends, patterns, and impact on the economy, highlights the urgent need for comprehensive cybersecurity measures and robust countermeasures. Financial cybercrimes pose significant threats to individuals, businesses, and governments, with far-reaching consequences for the economy. The study of financial cybercrimes provides valuable insights into the evolving tactics and techniques employed by cybercriminals targeting financial systems, institutions, and individuals. By understanding these trends and patterns, policymakers, cybersecurity professionals, and law enforcement agencies can develop effective strategies to prevent and mitigate such attacks. Financial cybercrimes have a profound impact on the economy. They result in substantial financial losses, both for individuals who fall victim to scams and for businesses and financial institutions targeted by sophisticated attacks. These losses ripple through the economy, impacting productivity, investment decisions, and consumer confidence. The effects of financial cybercrimes extend beyond immediate financial losses. They erode trust in online transactions, leading to decreased adoption of digital services and hindering economic growth. The reputational damage suffered by affected organizations can result in long-term consequences, including a loss of customers and diminished investor confidence. Furthermore, financial cybercrimes can disrupt critical infrastructure and services, such as banking systems and payment networks. Such disruptions have the potential to cause significant economic instability and systemic risks, affecting not only individual entities but also the broader financial ecosystem. To address the impact of financial cybercrimes on the economy, stakeholders must prioritize cybersecurity investments and collaborative efforts. Strengthening cybersecurity measures, implementing robust authentication protocols, and promoting cybersecurity awareness among individuals and organizations are essential steps toward mitigating these risks. Moreover, policymakers should develop and enforce comprehensive regulations that deter cybercriminals and facilitate international cooperation to combat cross-border cybercrimes. Collaborative information sharing and coordination among governments, law enforcement agencies, and financial institutions can enhance the ability to detect, respond to, and prosecute cybercriminals effectively. By conducting in-depth studies on financial cybercrimes, we can better understand the evolving nature of these threats, identify emerging trends, and devise proactive strategies to mitigate their impact on the economy. Such research is crucial for developing effective countermeasures, fostering innovation in cybersecurity technologies, and building a resilient digital ecosystem. In conclusion, a comprehensive study on financial cybercrimes sheds light on the critical importance of protecting financial systems, institutions, and individuals from cyber threats. By addressing these challenges head-on, we can safeguard the economy, protect individuals' financial well-being, and foster a secure and thriving digital environment for all.

## References


1. Buhalis D, Law R. Progress in information technology and tourism management: 20 years on and 10 years after the Internet—The state of eTourism research. Tour Manag. 29(4), 609–623.
2. Broadhurst R. Developments in the global law enforcement of cybercrime. Policing: Int j police sci manag. 2006;29(3):408-33.
3. Dilek S, Çakır H, Aydın M. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. Int J Artif Intell App. 2015; 6(1), 21–39.
4. FBI: Internet Crime Report 2020. Computer Fraud & Security, 2021(4), 4. (2001– 2020)
5. Jaishankar K, editor. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press; 2011.
6. Jaishankar K. The Future of Cyber Criminology: Challenges and Opportunities1. Int J Cyber Criminol. 2010;4(1/2):26.
7. NCRB: Crime in India Report. (2002 to 2021)
8. Nagurney A. A multiproduct network economic model of cybercrime in financial services. Serv Sci. 2015;7(1):70-81.
9. Rid T, Buchanan B. Attributing cyber attacks. J Strateg Stud. 2015;38(1-2):4-37.
10. Sharma, S., & Sharma, V. (2020). Cyber Crime Analysis on Social Media. Bsss J Comput.
11. Wolff, R. D., & Resnick, S. A. (2012). *Contending economic theories: Neoclassical, Keynesian, and Marxian*. MIT Press.


***Citation:*** *Sunny A, A study on financial cyber-crimes, trends, patterns, and its effects in the economy. Addict Criminol. 2024;7(1):186*