ISSN: 2634-9221
European Journal of Applied Sciences; Vol. 14 No. 01 (2026) (478-492)
https://doi.org/10.14738/aivp.1401.19906

Rise of Computer-Related Crimes: Loss of Data, Infrastructures, and Monetary Assets

Arianna E. Ortiz & Rohitha Goonatilake

1. Department of Mathematics and Physics, Texas A&M International University, Laredo, Texas 78041, USA

Abstract: In recent years, there has been a significant rise in computer-related crimes that have caused loss of data, damage to infrastructure, and monetary loss. This paper intends to analyze the extent of the losses and other damage using the data extracted from the FBI's Internet Crime Complaint Center (IC3) reports, ranging from the years 2020 to 2024, and to analyze trends in financial losses, mostly because of a wide range of internet crimes. Additionally, this paper recognizes the pattern of reported losses and calculates the expected values for the future years of 2025 and 2026. Losses reported on the IC3 increased significantly from $4.2 billion in 2020 to a staggering amount of $16.6 billion in 2024 and are predicted to keep increasing in future years. To ascertain the potential losses, time series forecasting is conducted on the data mostly provided in the IC3. Due to the rise of Artificial Intelligence (AI) related applications, AI-driven attacks are on the horizon, the proliferation of dark web tools, and increased global interconnectedness mean that the scale, speed, and cost of cybercrime continue to accelerate, necessitating significant investment in cybersecurity measures and resilience. Computer-related crimes are escalating rapidly, resulting in massive losses of data, severe damage to infrastructures, and staggering monetary assets. The global cost of cybercrime is projected to reach $10.5 trillion annually by 2025, growing by 15% each year, according to some estimates. These findings alert the public to be aware of severity of this dire situation they could face and to harden their software and take possible preventative measures to minimize the losses.

Keywords: Cybercrime trends and financial losses, Internet Crime Complaint Center (IC3) data analysis, Time series forecasting in SAS, Exponential growth modeling of cybercrime, Cybersecurity risk and economic impact.

INTRODUCTION

Cybercrime has grown significantly to become one of the largest financial threats in the expanding technology era, affecting individuals, businesses, and government agencies worldwide (Dashora, 2011; Choo, 2011; Sussmann, 2017; Goodman 2015). As the internet and technology advance, cybercriminal tactics evolve rapidly and closely following these developments (Cordesman, 2001). The Federal Bureau of Investigation (FBI) established the Internet Crime Complaint Center (IC3) in 2000 to monitor cybercrime trends (US Federal Bureau of Investigation, 2024). This platform is essential for collecting and analyzing data on annual complaints and financial losses reported by the public. These reports offer insights into crime types, affected age groups and regions, and victim-reported losses. Incidents reported have increased exponentially over the past four years, from 2000 to 2024, particularly during and after the COVID-19 pandemic (Hawdon et al., 2020; Hawdon, 2021). During its first year, the IC3 would record about two thousand complaints each month; just last year, the IC3 would record about two thousand complaints per day (US Federal Bureau

of Investigation, 2024). Since its start, IC3 has recorded 9 million complaints of fraud. Science of technology and the World Wide Web has increased significantly since then, therefore providing an easier way to access the internet for more cybercrime in recent years (Cordesman, 2001).

The IC3 plays a crucial role in helping the FBI and others develop preventive strategies against cybercrime. Its core functions include collection, analysis, public awareness, and referrals. Financial losses reported to the IC3 reflect the rapidly increasing number of incidents where cybercriminals attack, and the financial burden they place on the public. Analyzing these trends helps us understand how cybercrimes evolve with new technologies (Anderson et al., 2019; Romanosky, 2016). This information offers valuable insights for cybersecurity professionals and researchers aiming to reduce cybercrime rates. While some data points were taken from other files, most of the complaints and losses reported originated from the IC3 records on the FBI website. The data was well labeled and categorized to show differences over years, ages, types of complaints, financial losses, and regions affected by cybercrime. With today's technology, it is much easier for criminals to access private information with mere taps on a keyboard.

This study aims to **analyze cybercrime-related financial losses from 2000 to 2024** and **project potential losses for 2025 and 2026**. The study uses **SAS-based trend analysis and forecasting models** to estimate future crime reports and monetary damages. The code applies to an exponential growth model to accurately predict the losses and complaints for 2025 and 2026. If a linear regression model were used, the results would reflect the earliest years of the dataset. The findings from this research help deepen understanding of cybercrime trends and the likely future financial impacts. Since the internet was not as advanced in 2000 as it is now, cybercriminal activity was also not as advanced (Bagchi & Udo, 2003). There were about 17 thousand complaints and about $20 million reported losses in the year 2000. Since then, the number of complaints reported in 2024 has increased to around 860 thousand (up about 4,959%), and the financial losses racked up to $16.6 billion (an increase of 82,900%).

Figure 1: Annual amount of monetary damage caused by reported cybercrime in the United States from 2000 to 2024 (in billion US dollars)

Figure 1 reveals a strong upward growth in losses as the years increase from 2000 to 2024. However, from 2000 to 2017, the increase appears to be linear, but a dramatic shift has been observed since 2017. It is assumed that if the trend is continued, then the future years will also continue to grow drastically. Given this exponential growth in recent years, the predicted years, 2025 to 2028, will follow the steep increase. As is seen in Figure 1 for an easy crude estimate, the plot is consisted of two linear trends, one from 2000 to 2017 and another from 2017 to 2024 with a slope of 0.079 billion/year (r = 0.931) and 2.125 billion/year (r = 0.967) respectively. If this trend continues throughout the forecasted period, the forecasted losses are estimated to be 18.40 billion for 2025, 20.53 billion for 2026, 22.65 billion for 2027, and 24.78 billion for 2028, using the year 2017 as a point of reference. These are much lower than the estimates obtained from the polynomial regression model forthcoming later in the paper.

PRELIMINARIES AND CURRENT STATUS

Existing impact of cybercrimes in the UK and internationally have been examined the extent of their magnitude and nature of crimes, the characteristics of the victims and offenders, and the associated financial losses (McGuire & Dowling, 2013; Levi, 2017; Lavorgna & Holt, 2025). Several internet users report negative online experiences, e.g., approximately 31-37% of adult internet users in the UK experienced computer viruses in the previous year, hacking is reported less, yet it is increasing over the years. At least 8% of businesses have experienced viruses in the past 12 months; viruses make up a big part of these incidents. Young people, men, and frequent internet users are more likely to experience computer viruses or unauthorized access. Many claim to use security measures (antivirus, firewalls, etc.) and keep them up to date. However, survey data suggests several gaps in practices. The evidence is much more limited. The Offending, Crime and Justice Survey (Home Office (UK), 2009) provides some self-report data: e.g., small proportions of young people admitting sending viruses or hacking without permission; males more than females. Skill levels of offenders can be organized in a pyramid: a small exclusive group with high skills, a middle group with semi-skilled offenders, and a large group of low-skilled criminals (script kiddies) (Leukfeldt et al., 2017; Lavorgna & Holt, 2025). Losses are claimed to be “several billion pounds per year” for the UK across cybercrime broadly. Additionally, losses of personal data, emotional impacts, privacy, etc., are noted but not well measured.

A study has been done to analyze if the COVID-19 pandemic and its restrictions in the US changed peoples’ internet routines and in return affected rates of cybervictimization. Hawdon, Parti, & Dearden, 2020 used routine activity theory (Cohen & Felson, 1979) as their framework which explains that crime depends on the movement of time and space of offenders, targets, and lack of guardians. The pandemic is seen as a natural experiment that could affect these components. Thereof, two surveys using Dynata, with one survey in November 2019 (pre-COVID) and another in April 2020 (post-COVID) for a sample of size about 1,109 in the pre-COVID sample, 1,021 in the post-COVID sample. The samples are balanced on key demographics (sex, race/ethnicity) with some differences in age, education, and unemployment between the pre- and post-COVID time points. Self-reported victimization across seven types of cybercrime (e.g., online scams, identity theft, malware/viruses, online sexual harassment/bullying). Self-reported online routines / computer-related behaviors (social media use, reading news, online shopping, working on the computer etc.). Self-protection behaviors (antivirus/firewalls, etc.) A negative binomial

regression for count-data (number of different victimization experiences), χ^2 tests and t-tests for comparing pre vs post, and models incorporating routine activity theory variables. Among specific victimization types, one difference is that reports from companies about data losses decreased (21% in pre COVID to 16% in post COVID) in the post COVID sample showed a slight increase in usage of virus software and firewalls in the post COVID sample (up to 4% increase), though the difference is modest and close to the significance threshold. In their regression model, many routine activity theory predictors behaved as expected: darker web usage, time on social media, time reading news predicted higher victimization; protective behaviors associated with lower risk. The COVID indicator variable itself was not significant.

DATA DESCRIPTION AND REPORTING

The data used in this study were obtained from the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) Annual Report (US Federal Bureau of Investigation, 2009, 2015, 2019, 2024). The dataset is made up of reports made from 2000 to 2024. Three key variables are included:

1. Year, representing the reporting period.
2. Complaints indicate the total number of cybercrime complaints reported to the IC3 by the public.
3. Total Reported Losses, measured in billions of US dollars (USD), reflect the financial impact of the crimes.

Crime types were not included in this dataset because the cleanliness of the outputs of the code would have been compromised (Parn & Edwards, 2019; Omolara et al., 2018). Instead, only the three main variables were needed to keep the report as sleek as possible.

The data was structured as a time series dataset for a clear view to run an analysis in the SAS Studio code. The variables were organized with Year as the temporal identifier, Complaints as the count variable, and Losses in billion as the continuous financial variable. This series format aided the use of SAS forecasting techniques (e.g., PROC FORECAST and PROC REG) to model and project cybercrime losses through 2025 and 2026.

The dataset represents the long-term trend of the rise in cybercrime, both in complaints and monetary losses reported from early email fraud to ransomware and cryptocurrency related crime (Choo, 2010; Roche, 2006; Ombu, 2023). Table 1 represents the data used in the analysis to show the exponential progression of each variable from 2000 to 2024. The number of cybercrime incidents reported to the FBI's Internet Crime Complaint Center (IC3) has more than doubled over the past decade, and 2020 marked a nearly 70 percent increase in reports, likely related to the pandemic. In addition to becoming more common, cybercrimes have become more costly, with total losses surging by 765 percent since 2011. The shape of cybercrime has also changed as consumers and security providers have caught onto tactics, forcing criminals to change their methods.

Cybercrime complaints have increased significantly in recent years, with the FBI's Internet Crime Complaint Center (IC3) reporting an increase in complaints from 791,790 in 2020 to 859,532 in 2024. In the same period, losses have also grown dramatically from $4.2 billion in 2020 to over $16 billion in 2024. The shape of cybercrime has also changed as

consumers and security providers have caught onto tactics, forcing criminals to change their methods. Cybercrime complaints have increased significantly in recent years, with the FBI's Internet Crime Complaint Center (IC3) reporting an increase in complaints from 791,790 in 2020 to 859,532 in 2024. In the same period, losses also grew dramatically from $4.2 billion.

Table 1: IC3 Reported Cybercrime Complaints and Financial Losses, 2000–2024

Year	Complaints	Losses (Billions in USD)
2000	16,838	0.02
2001	50,412	0.02
2002	75,064	0.05
2003	124,515	0.13
2004	207,449	0.07
2005	231,439	0.18
2006	207,492	0.20
2007	206,884	0.24
2008	275,284	0.26
2009	336,655	0.56
2010	303,809	0.47
2011	314,246	0.49
2012	289,874	0.53
2013	262,813	0.78
2014	269,422	0.80
2015	288,012	1.07
2016	298,728	1.45
2017	301,580	1.40
2018	351,937	2.70
2019	467,361	3.50
2020	791,790	4.20
2021	847,376	6.90
2022	800,944	10.30
2023	880,418	12.50
2024	859,532	16.60

Source: FBI Internet Crime Complaint Center (IC3) Annual Report (Federal Bureau of Investigation, 2024).

In addition to offering quantitative insights into cybercrime, the IC3 dataset shows how digital criminal behavior has changed over time. From simple identity theft and email fraud in the early 2000s to widespread ransomware, business email compromise, and cryptocurrency-related crimes in recent years, the types of incidents reported have changed as technology has advanced. This change in cybercrime typologies highlights how sophisticated and complex criminals are becoming. The dataset also reveals important correlations between technological advancements and losses, such as the sharp rise in digital dependency during and after the COVID-19 pandemic (Hawdon et al., 2020). In addition to providing a solid basis for time-series forecasting, these longitudinal records are a crucial instrument for developing policies, raising public awareness, and allocating

cybersecurity resources. By using this data, the study quantifies both monetary losses and contextualizes them within technological and societal changes.

METHODOLOGIES AND OVERVIEW

In this section, an overview of methodologies is provided in terms of model selection and justification, and further, forecasting for estimated monetary losses and expected number of complaints for the years 2025 to 2028. However, it should be noted that once the public is so informed of the complaints, the public seeks solutions rather than continuing to file additional complaints one after another. Explanatory analysis and associated forecasting mechanisms follow thereafter.

Table 2: Summary Statistics of Quantitative Overview from 2000 to 2024

Variable	N	Mean	Std. Dev.	Minimum	Lower Quantile	Median	Upper Quantile	Maximum
Year	25	2,012.00	7.36	2,000.00	2,006.00	2,012.00	2,018.00	2,024.00
Complaints	25	362,394.96	260,996.78	16,838.00	207,492.00	289,874.00	351,937.00	880,418.00
Losses (in Billion)	25	2.62	4.37	0.02	0.2	0.56	2.7	16.6

The summary statistics provided in Table 2 give insight into the quantitative overview of the IC3 dataset from the years 2000 to 2024. The average reported financial loss due to cybercrime over the 25 years was $2.62 billion (USD) per year, with a median of $0.56 billion, which indicates a strong right skewness driven by larger losses in the most recent years. This is further supported by the large standard deviation of $4.37 billion, presenting high variability and values toward the upper end of the dataset. Losses ranged from a minimum of $0.02 billion in 2000 to a maximum of $16.60 billion in 2024. Similarly, the complaints follow the same trends with a mean of 362,395 complaints and a standard deviation of 260,997, supporting the increasing volatility of cybercrime activities. The quartile values of both complaints and losses show that most observations in earlier years were shown in the lower quartiles, while the most recent observations in the upper quartiles show that there is a sharp rise in observed reporting periods. Table 2 highlights substantial growth, increasing variability, and strong right skewness in both complaints and losses over the period of 25 years.

The Shapiro–Wilk test was applied to the reported complaints and losses throughout the years. The results reveal a strong rejection of normality for both variables. Complaints resulted in a Shapiro–Wilk statistic of $W = 0.822$ with $p = 0.000538$, while financial losses revealed an even more pronounced deviation from normality of $W = 0.639$ with $p = 1.22 \times 10^{-6}$. This supports the indication of strong right skewness in both variables. The findings align with the large dispersion observed in the summary statistics and the long right tails displayed in the distributional histograms. These results justify the use of exponential modeling approaches to forecast future years.

Model Selection and Justification

This data is used to produce a trend analysis from year to year. In earlier years of the data, it could be said that as the years increased, the data would also increase linearly. The linear trend model was used to examine whether the relationships between the years, complaints,

and losses followed a consistent trend over time. The visual and residual analysis proved this to fail around 2018 due to both complaints and loss variables significant and intense increase (Khiralla, 2020). The exponential growth of the trend in the data is most accurately represented by using a forecasting model that follows the same path as the dataset increases over recent years (Sharif & Mohammed, 2022).

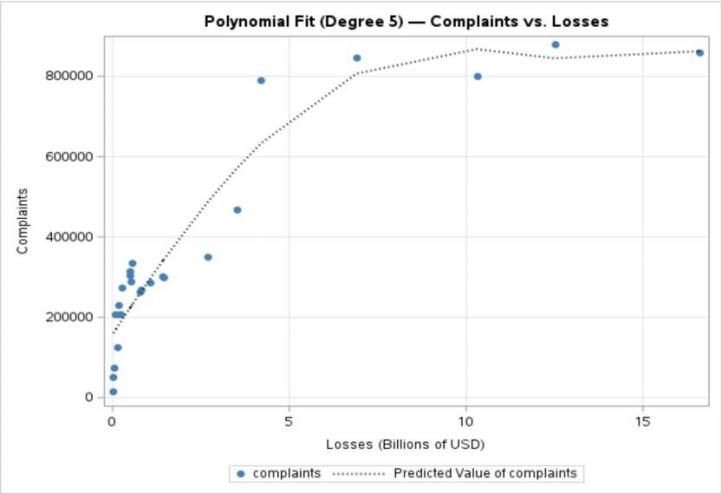

Figure 2: Correlation between Complaints Vs. Losses using Polynomial Regression

Figure 2 works for forecasting and other estimation purposes. However, the main downsides of polynomial regression are overfitting, where the model fits the noise in the training data and performs poorly on new data, and extrapolation issues, causing the model to behave erratically outside the data range (Lagazio et al., 2014). Other disadvantages include difficulty in interpreting the coefficients as the polynomial degree increases and increased computational cost. Additionally, the model can be sensitive to outliers, thus distorting the fitted curve. It was made to find the optimal degree that captures the underlying trend without overfitting noise, often choosing the one with the lowest RMSE (Root Mean Squared Error). Lower degree, 5 seems to be working, so aim for a balance where the curve fits the data well but does not wiggle excessively through individual points. Computational complexity is that the higher-degree polynomials require more computational resources, and that in turn can slow down the training process, especially with large datasets. Output statistics for this model are provided in Table 3.

Table 3: Output Statistics Used in the Polynomial Regression Model

Observation	Dependent Variable	Predicted Value	Residual
1	16,838	160556	-143718
2	50,412	160556	-110144
3	75,064	164589	-89525
4	124,515	175316	-50801
5	207,449	167275	40174
6	231,439	181997	49442
7	207,492	184664	22828
8	206,884	189990	16894

9	275,284	192648	82636
10	336,655	232153	104502
11	303,809	220377	83432
12	314,246	223000	91246
13	289,874	228235	61639
14	262,813	260653	2160
15	269,422	263223	6199
16	288,012	297560	-9548
17	298,728	344687	-45959
18	301,580	338570	-36990
19	351,937	488324	-136387
20	467,361	569735	-102374
21	791,790	633430	158360
22	847,376	807008	40368
23	800,944	867781	-66837
24	880,418	844977	35441
25	859,532	862572	-3040

Sum of Residuals	0
Sum of Squared Residuals	1.502189E11
Predicted Residual SS (PRESS)	7.920252E13

For two time series variables, we can use correlation tests like Pearson's coefficient, r to check for a linear relationship, regression models like Vector Autoregression (VAR) to model the relationship to understand the underlying properties of the series. Statistical tests for exponential random variables include goodness-of-fit tests like the Kolmogorov-Smirnov and Anderson-Darling tests to check if data fits the exponential distribution, and hypothesis tests such as the likelihood ratio test to compare two exponential distributions or test a single distribution's parameters (Romanosky, 2016; Anderson et al., 2019).

The IC3 figures reflect reported losses via complaints and not the full societal cost. The actual losses may be much higher, therefore making the IC3 a source to track complaints and losses due to cyber activity in the US.

The following notes and caveats are worth noting:

1. Definitions vary (what counts as “cybercrime” or “computer crime”), so comparability across years is limited and various interpretations, at times.
2. Use this as a trend-indicator rather than a precise cost history.

Exploratory Analysis

The exploratory analysis provides a clear understanding of the dataset before conducting the forecast analysis. Investigation of growth rates, descriptive statistical tests, and visual graphs and patterns were shown to aid in visual representation.

Summary statistics were key to showing the trend and spread of reported losses from 2000 to 2024. With SAS procedures, the descriptive analysis revealed an approximate $2.96 billion of mean annual losses, with $0.80 billion in median value (Kshetri, 2010). The

dramatic increase in financial losses due to cybercrime reflects the growing use and dependence on technology between 2000 and 2024. The high standard deviation and positive skewness reveal an exponential increase that accurately represents the recent years' influence on the overall average (Saini et al., 2012). A quick upward trajectory in the last couple of years' worth of data aligns with the expectation of nonlinear growth in future projections.

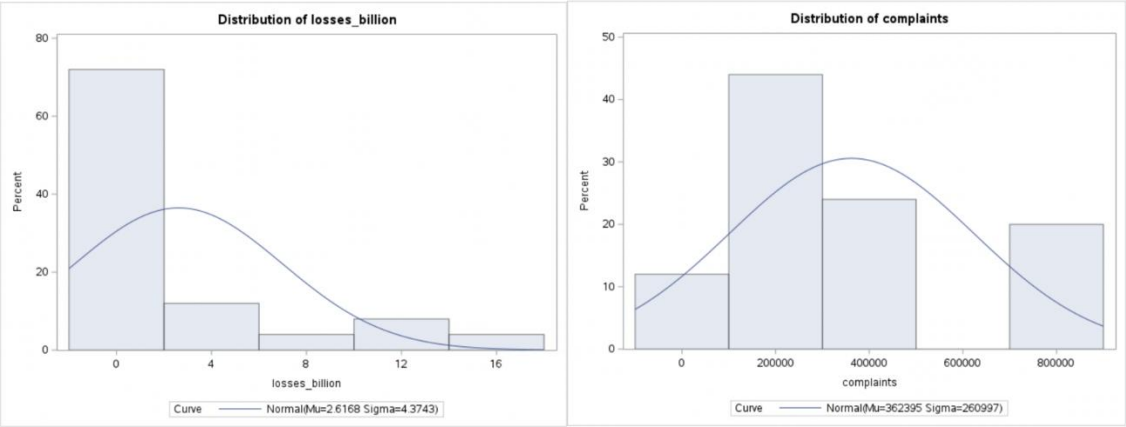

Figure 3: Histograms of Distributions of Complaints and Losses

Both images in Figure 3 reveal strong right skewness, which aids in determining that the increase in complaints and losses throughout the years is exponential rather than nonlinear. The prediction of future years should follow the same exponential growth as shown between the years 2020 and 2024. To verify this, SAS is used to calculate the number of complaints and losses in the following years.

Forecasting Methods

Statistical software, such as SAS programming, is used to analyze and forecast data. Time series data are prepared to be examined using line plots and summary tables. Forecasting is then performed by using PROC FORECAST. The forecast results provide both point estimates and confidence intervals, determining the most dependable and accurate magnitude of financial losses in the years 2025, 2026, 2027, and 2028. From these projections, it is determined that cybercrime is increasing, and statistical modeling is important for evaluating the cybersecurity risks and taking preventive measures to mitigate the losses.

In statistical modeling terms, an exponential growth trend in SAS depicts occurrences where the dependent values increase at a proportional rate. By using the PROC FORECAST procedure in SAS, the exponential method (METHOD=EXPO) addresses the trend and portrays an exponential curve that follows the more recent data (Sharif & Mohammed, 2022). In this case, each year's growth is based on the previous year, therefore producing a curve that makes each year an accumulation of data that curves upward over time. When this information is applied to the dataset, the model yields a low residual variance and a higher coefficient determination, whereas compared to linear alternatives, the prediction would be much higher and accurate.

The model was configured with a smoothing weight of 0.3 (WEIGHT=0.3), which balances the more recent data by 30% while giving the rest of the 70% to the model's previous data when predicting the next values for 2025, 2026, 2027, and 2028 (Lagazio et al., 2014). This is significantly important because if the smoothing weight is any lower, then the model will react slowly to new changes. After all, it would give too much importance to older data. If the weight is too high, then the model will become overly sensitive to the newer data, which can cause an unpredictable forecast. Furthermore, a weight of 0.3 will balance out the cybercrime trends in the data, considering the surge of activity after the COVID-19 pandemic. This trend pattern best aligns with the real-world situation of a rapid growth in IC3 reports of cybercrime. The spread of the digital world and connectivity has magnified opportunities for criminals to have easier and profound access to contribute to these crimes.

RESULTS AND FINDINGS

This section confines to all exploratory findings, the possible forecasting results, and regression analysis using both exponential and polynomial regressions.

Exploratory Findings

Exploration of the analysis provides important information regarding the quick progression of cybercrime activity in the United States from 2020 through 2024. During these five years, financial losses increased immensely from 4.2 billion in 2020 to 16.6 billion in 2024. The losses increased by approximately 295%, highlighting the rapid growth in economic harm from cyber incidents. Inspecting the visual of the loss trajectory endorses a steep, increasing pattern which infers the intensified cybercrime over time.

The pattern of the overall trend is not uniform. Year-to-year changes reveal increasing growth rates, indicating areas of particularly intensified cybercrime activity. From the years 2020 to 2024, the most pronounced growth happened between 2021 and 2022, when losses reported to the IC3 jumped from $6.9 billion to $10.3 billion, an increase of approximately 49% (Parn & Edwards, 2019; Anderson et al., 2019). The significant spike represents the steepest increase in losses in the dataset. It may also correspond to more systemic vulnerabilities such as an increase in reliance on technologies after the COVID-19 pandemic or the growth of high-impact attack methods like ransomware and business email compromise.

Moreover, the interquartile range (width of the middle 50% section of the data) and distributional summaries of losses in the dataset validate the conclusion that damage became more skewed towards higher-valued incidents in recent years. As the median increased from $560 million to much larger values by 2023 and 2024, the distribution reflects growing amounts of loss events. The increased volatility makes a significant contribution to the use of forecasting in later sections. Agencies and policymakers may use this information to anticipate the economic burden posed by future cybercrime threats.

The exploratory findings provide a clearly escalating threat slope with extensive financial consequences that compound annually. Observing these factors justifies deeper trend modeling and correlation analysis to better understand factors that contribute to the growth and projection of potential losses in future years.

Forecasting Results

Exponential smoothing was applied to the IC3 time series data to produce a table of short-term forecasts of cybercrime losses from 2025 to 2028. The model portrayed the strong upward slope noted in the previous data for the last couple reported years and projected that losses will continue to rise significantly in the next couple of years. This is if there are no other drastic economic impacts that affect the exponential increase over the next three years. The trend indicates that damage due to cybercrime accelerates exponentially rather than steadily, which aligns with the nonlinear growth that had been observed in earlier reported years. Based on the fitted model, the forecasted losses and complaints are provided in Table 4.

Table 4: Forecasted Losses and Complaints for Every Year from 2025to 2028

Years	Forecasted Losses	Forecasted Complaints
2025	$19.21 billion	981,234
2026	$22.73 billion	1,051,653
2027	$26.52 billion	1,123,692
2028	$30.59 billion	1,197,351

These predictions reflect a continued steep increase in both financial losses and complaints, with an expected growth to be nearly 84.3% in losses and about 39.3% in complaints from 2024 to 2028. The IC3 data is approached by using exponential smoothing to give greater weight to more recent observations to better predict the years to come. This approach is well-suited for datasets like this to analyze the rapid, recent acceleration of losses and complaints. As a result of this method, the model strongly responds to the dramatic increase in losses and complaints during 2021 through 2024 and projects that the surge will continue to heighten.

Results in the exponential smoothing process highlight an escalating projection of reported losses and complaints. This reinforces the need for continued monitoring, planning, and cybersecurity investment in the next few years as cybercrime continues to impact the economy.

Correlation Analysis

To examine the strength and direction of the relationships each year, reported complaints and total monetary losses, correlation analysis was conducted. Several notable patterns were revealed that reinforce the trends that have been discussed in earlier sections.

A strong positive correlation was observed between year and complaints with r = 0.879, indicating that the number of reported crimes consistently increases as the years increased. Similarly, the relationship between the year and losses also showed a strong positive correlation with r = 0.756, reflecting the growth of monetary damage to the public throughout the observed years. Also, the correlation between complaints and losses was strongly positive with r = 0.877, confirming that higher complaint counts mean higher financial losses reported. This information suggests that the overall volume of reported cases, losses, and years correspond with each other throughout the years. Therefore,

increases in incident frequency are closely related to the severity of economic impact that may have been occurring due to the escalation of attacks.

Overall, the correlation analysis accurately reveals that cybercrime activity has intensified in frequency and financial severity of the years, especially over 2020-2024. These strong statements validate the need for forecasting and trend modeling to understand the critical anticipation for future risks and create better opportunities for protective resources and inform the general public.

Polynomial Regression

A fifth-degree polynomial regression model is used to further investigate the exponential relationship between reported cybercrime complaints and financial losses. The model fives a flexible form capable of achieving complex curvature and growing trends that a simple linear regression model may not accurately display. The high exponential power of the model, reflected by an $R^2 = 0.91$ ($r = 0.954$), shows that the polynomial structure reports a substantial portion of the variability in complaints based on the values of the losses.

Despite the model's strong fit, the individual polynomial coefficients were not significant to the statistical analysis that was done at conventional levels. This occurred because higher-order polynomial terms usually show strong multicollinearity, inflating standard errors and reducing the statistical significance of each individual variable even when the combined polynomial function fits the data well. This means that while the curve successfully traces the nonlinear pattern between complaints and losses, the interpretation of certain coefficient values is not as meaningful as the overall capability of the model's prediction.

The fitted curve, as a result, portrays a clear upward trend, with complaints and financial losses increasing rapidly- particularly in the more recent years of 2020-2024. The shape of the polynomial curve contributes to the conclusion that the relationship between cybercrime frequency and reported damage is not proportional but accelerates, showing the presence of compounding effects such as recurring attacks, high-impact incidents, or broader widespread vulnerabilities.

The polynomial regression model strengthens that conclusion the financial losses and complaints rise together in an exponential fashion. This fortifies earlier evidence of escalation in cybercrime, where frequency and severity intensify concurrently. The model further supports its use to better describe the complex dynamics of cybercriminal activity over time.

DISCUSSION AND LIMITATIONS

The provided findings align with the current data, which shows an accelerating growth in cybercrime losses driven by increasing global digital reliance and sophisticated attack methods used for these attacks. Overall, forecasts emphasize the growing economic burden and financial losses, projected to reach approximately $10.5 trillion annually by 2025. Among the alignment with current trends and their accelerating growth of the incidents are noteworthy. The FBI's Internet Crime Complaint Center (IC3) reported over $16 billion in losses in 2024, a 33% increase from 2023, confirming a rapid rise in financial damage. Increasing digital reliance and its sophistication add much to the burden for those

concerned. Some sparing forecasts emphasize the growing economic burden, not knowing the uncertainties.

The world's increasing reliance on digital infrastructure creates an expanding "attack surface," which criminals exploit using advanced attack techniques like AI-driven attacks and complex investment frauds, particularly involving cryptocurrency. This will cause an added economic burden for all involved in innovation and increasing market shares. Cybercrime is now considered a top global business risk and, if measured as a country, would be the world's third-largest economy after the US and China. Reasonably validated limitations are essential. The limitations identified in our findings are widely acknowledged challenges in cybercrime reporting and analysis. The prevailing data only spans over shorter time series spectrum determines the severity marginally. While data exists over a longer period, recent rapid changes mean a 5-year series is a common, and sometimes the most relevant, timeframe for trend analysis, given the pace of technological evolution and advancement. In some instances, underreporting would create a lot of chaos. The official reports, like those from the FBI's Internet Crime Complaint Center (IC3), consistently state that reported losses are only a fraction of the actual total. Many victims, particularly businesses, do not report incidents due to shame, lack of awareness, or the exclusion of indirect costs (e.g., business downtime, reputational damage).

Aggressive interventions, policy changes, and recommendations are vital and need to be revisited as the emerging unpredictable nature of incidents. This does not amount to interventions or policy changes. Most analyses focus on the impact of cybercrime rather than the effects of specific interventions. However, reports highlight that measures such as employee training, use of security AI-automation, and international policy collaborations can significantly reduce losses, suggesting interventions do have an impact even if not perfectly quantified in top-line loss reported, thereafter.

CONCLUSIONS AND FUTURE WORK

It is certain that IC3 losses have risen sharply over the years, reaching over $16.6 billion in 2024. These forecasts show a startling scenario yet to come. The global cybercrime damages are projected to reach approximately $19.2 billion in 2025, $22.7 billion in 2026, $26.5 billion in 2027, and an estimated $30.6 billion in 2028. Naturally, much needed future work is necessary to be carried out to prevent this economic calamity

IC3 losses rose sharply during the years 2020 to 2024. Reported losses to the FBI's Internet Crime Complaint Center (IC3) have increased significantly, totaling over $50 billion since 2020 alone. The reported losses for 2024 were $16.6 billion, a 33% increase from 2023. Cybercrime damages are projected to reach approximately $19.2 billion (USD) annually by the end of 2025. Estimated losses for 2028 suggest global costs will increase to around $30.6 billion. Results stress the fact that proactive cybersecurity measures and hardening of software infrastructure are needed. The exponential rise in costs highlights the urgent need for robust, proactive cybersecurity strategies, increased investment, and enhanced public-private collaboration to mitigate risks and combat evolving threats like AI-driven attacks and advanced ransomware. Furthermore, individuals and organizations can report incidents to the IC3 website to aid law enforcement tracking efforts to curb the losses and prevent future attacks.

REFERENCES

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2019). Measuring the changing cost of cybercrime. Journal of Cybersecurity, 5(1), tyy006. https://doi.org/10.1093/cybsec/tyy006

Bagchi, K. & Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. Communications of the Association for Information Systems, 12(46), 684–700.

Choo, K. K. R. (2010). High tech criminal threats to the national information infrastructure. Information Security Technical Report, 15(3), 84–91. https://doi.org/10.1016/j.istr.2010.11.001

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

Cordesman, A. H. (2001). Cyber-threats, information warfare, and critical infrastructure protection. Center for Strategic and International Studies.

Dashora, K. (2011). Cyber-crime in the society: Problems and preventions. Journal of Alternative Perspectives in the Social Sciences, 3(1), 240–259.

Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable, and what we can do about it. Doubleday.

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice, 46(6), 837–842. https://doi.org/10.1007/s12103-021-09652-7

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. American Journal of Criminal Justice, 45(4), 546–562. https://doi.org/10.1007/s12103-020-09524-4

Home Office (UK). (2009). The Offending, Crime and Justice Survey: Longitudinal analysis, 2003–2006 (Home Office Research Report 19). UK Home Office. https://www.gov.uk/government/publications/the-offending-crime-and-justice-survey-longitudinal-analysis-2003-to-06

Khiralla, F. A. M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. International Journal of Computer Science and Network (IJCSN), 9(5), 112–120.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. Third World Quarterly, 31(7), 1057–1079. https://doi.org/10.1080/01436597.2010.518752

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security, 45, 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Lavorgna, A. & Holt, T. J. (2025). Cybercrime in criminology: Re-examining core themes and concepts. Journal of Criminology and Criminal Justice, 3(1), 100012. https://doi.org/10.1016/j.crimcj.2025.100012

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Organisations and cybercrime: The victimisation of Dutch organisations through cybercrime. Crime, Law and Social Change, 67(3), 239–259. https://doi.org/10.1007/s10611-016-9648-4

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. In Cybercrimes, cybercriminals and their policing in crime, law and social change (pp. 1–20). Springer.

McGuire, M. & Dowling, S. (2013). Cybercrime: A review of the evidence – Chapter 1: Cyber-dependent crimes. Home Office Research Report 75. Home Office Science.

Ombu, A. (2023). Role of digital forensics in combating financial crimes in the computer era. Journal of Forensic Accounting Profession, 1(2), 45–59. https://doi.org/10.2478/jfap-2023-0007

Omolara, A. E., Jantan, A., Abiodun, O. I., et al. (2018). State-of-the-art in big data application techniques to financial crime: A survey. International Journal of Computer Applications, 181(7), 1–14.

Parn, E. A. & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and blockchain deterrence. Engineering, Construction and Architectural Management, 26(2), 245–266. https://doi.org/10.1108/ECAM-03-2018-0106

Roche, E. M. (2006). Internet and computer related crime: Economic and other harms to organizational entities. Mississippi Law Journal, 75(3), 115–145.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202–209.

Sharif, M. H. U. & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trends. World Journal of Advanced Research and Reviews, 15(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.045

Sussmann, M. A. (2017). The critical challenges from international high tech and computer related crime at the millennium. In Computer Crime (pp. 233–255). Taylor & Francis.

US Federal Bureau of Investigation. (2024). Internet Crime Report 2024. Internet Crime Complaint Center (IC3). https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf