ABSTRACT

Title of Thesis:	UNDERSTANDING CYBERCRIME IN THE COVID-19 PANDEMIC
	Natalie Marie Jillson, Bachelor of Science, 2024
Thesis Directed By:	Associate Professor, Bianca Bersani, Criminology and Criminal Justice

The COVID-19 pandemic, beginning in March of 2020, shifted daily life from an in-person to a virtual environment. This shift motivated an array of criminal justice research focusing on the pandemic's effect on property and street crime. Overlooked, however, is the impact that this shift had on cybercrime victimization, and there currently exists a lack of research on any long-term effects that the pandemic may have had on cybervictimization. This study employs an Interrupted Time Series Analysis (ITSA) to compare cybercrime trends before and after the pandemic's inception. The analysis reveals an upward trend in the number and severity of cybercrime attempts after 2020. The results highlight a need for the implementation of stronger cybersecurity measures in an increasingly virtual world and serve as a starting point for future research, which should continue to explore these trends more in-depth. The work also emphasizes the importance of developing an official

documentation process and measurement tool for cyberattacks to better inform future work.

UNDERSTANDING CYBERCRIME IN THE COVID-19 PANDEMIC

by

Natalie Jillson

Thesis submitted to the Department of Criminology and Criminal Justice at the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Bachelor of Science
2024

© Copyright by
Natalie Marie Jillson
2024

Acknowledgements

I can’t start this paper any other way than thanking my advisor, Dr. Bianca Bersani, for her constant support throughout this learning process. You’re the type of educator that every student wants to have and hates to leave at the end of the year, and I am so grateful for the two years I got to spend under your guidance. Casey, thank you for the close reads of our drafts and for helping me understand all of the R output that seemed like nonsense at the time, but were actually my major results. To my cohort, congratulations on your theses and thank you for the constant stream of feedback and support. To my family and friends, I am who I am because of you, and I am so incredibly thankful to have your unwavering encouragement in every project I take on.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

On March 11, 2020, the World Health Organization (WHO) announced the official start of the COVID-19 pandemic, signaling to many that a large lifestyle change was soon to occur (AJMC Staff 2021). As expected, the United States government began to implement strategies in an attempt to curb the spread of the disease. By mid-to-late March, school closure recommendations were made in all 50 states, domestic and international travel advisories were put in place, and a majority of employers were promoting a work-from-home environment for their employees (Hawdon, Parti, and Dearden 2020; AJMC Staff 2021; CDC 2023). Even now, after 3 years of ebbs and flows of the disease, this transformation to virtual work has become permanent for many individuals. As recent as June 2023, 40.9% of U.S. employees were still working in a fully-remote or hybrid format (Haan 2023). This change in daily habits, which can be referred to as routine activities, as result of this global pandemic has provided a variety of new opportunities for criminological research.

Prior research has examined the application of the routine activities theory (RAT) to crime during the COVID-19 pandemic in several facets. Routine activities theory posits that for a crime to occur, there must be a convergence of a motivated offender, suitable target(s), and the absence of a capable guardian (Cohen and Felson 1979). In the context of the COVID-19 shift to a virtual environment, there were less suitable targets on the street to be victimized and more capable guardians present to disrupt or discourage property crime. According to the ideas of RAT, this would suggest a decrease in property crime – a suggestion supported by several recent

papers (Ashby 2020; Koppel, Capellan, and Sharp 2023; Rosenfeld, Boxerman, and Lopez 2023). Routine activities theory has more recently been applied in the cyberspace, which is another venue that saw a large change in activity during the COVID-19 pandemic.

In the case of the Internet, unlike with the in-person environment, the COVID-related shift was toward the venue rather than away from it. This shift would be characterized, then, by an increase in suitable targets in the cyberspace, where there is already little opportunity for the presence of a capable guardian to exist (Maimon and Louderback 2019; Hawdon et al. 2020; Johnson and Nikolovska 2022). Recent research reviewing cybercrime during the COVID-19 pandemic has found short-term significant increases for certain types of cybercrime in the UK (Buil-Gil et al. 2021; Kemp et al. 2021).

However, there still remain many unanswered questions about cybercrime in the United States during the pandemic, stemming from a lack of research about any long-term effects that COVID-19 may have had on cybervictimization. Since the major pieces of prior literature in the space only utilize data measuring 2-3 months beyond the onset of the pandemic, any long-term effects on cybercrime trends have yet to be discovered. Identifying these longer, large-scale trends can help determine if the threat of cybercrime is increasing and, if it is, help to guide cybersecurity resources to prevent victimization.

The current research examines a U.S.-based data source with the opportunity to obtain more long-term findings – through 2023 – about cybercrime during and following the pandemic. The dataset for this project was created using the FBI

Internet Crime Complaint Center's annual reports and contains a wide scope of cyber-enabled and cyber-dependent crime types. Cyber-enabled crimes are offenses that utilize technology as a tool for committing a crime, like fraud, while cyber-dependent crimes represent cases in which technology was both the tool used to commit the crime as well as the target of the crime itself, like hacking (Anon n.d.). This study analyzes the dataset to determine if opportunities for cybercrime in the United States have changed since the declaration of COVID-19 as a global pandemic.

This work serves a significant purpose in filling existing gaps in literature surrounding current cybercrime trends. By determining what, if any, changes in cyber victimization have occurred since the onset of the pandemic, better cybersecurity measures and crime prevention efforts can be put in place to help curb victimization.

Chapter 2: Literature Review

The COVID-19 Pandemic

In the early days of 2020, the World Health Organization (WHO) announced the discovery of a novel coronavirus that had originated in Wuhan, China. Within the span of a few weeks, the issue grew to be a Global Health Emergency and on March 11, 2020, the WHO officially declared the start of the COVID-19 Pandemic (AJMC Staff 2021). As cases in the country grew, the United States searched for ways to mitigate the spread of the virus. Schools began conducting classes virtually. Sports, concerts, and almost all public events were canceled. Nightlife and leisure activities ceased to exist, non-essential stores and services closed, and many employees began to work from home (Ashby 2020; AJMC Staff 2021; Regalado, Timmer, and Jawaid 2022). As of May 2020, 88% of people were being encouraged or required by their employer to work from home (Hawdon et al. 2020). This 2020 shift from in-person to online work was not short-lived, either. A 2022 study found that 60% of individuals whose jobs could be performed from the home were doing so on a part or full-time basis, and this number remained above 40% into 2023 (Parker, Horowitz, and Minkin 2022; Haan 2023). This massive shift of in-person activities to a virtual setting, caused by the COVID-19 pandemic, had major implications on what many criminologists would refer to as the "routine activities" of individuals across the country.

Routine activities are any recurrent and prevalent responsibilities that account for much of everyday life including work, school, child-care duties, social

interactions, and standard acts of necessity – such as grocery shopping (Cohen and Felson 1979; Cullen, Agnew, and Wilcox 2021). With the rise of this idea of "routine activities" in the late 1900s came the suggestion that a change in these activities – or a change in the way people live – may change crime trends as well, leading to the development of the routine activities theory.

Routine Activities Theory

Routine activities theory (RAT) was developed in 1979 by Cohen and Felson as a means of explaining situational factors in which crime is most likely to occur. The theory suggests that for a crime event to occur, there must be a convergence in space and time of three elements: motivated offenders, suitable targets, and the absence of a capable guardian (Cohen and Felson 1979; Perera 2024). Motivated offenders are individuals who are willing and able to commit a crime, suitable targets can be a person or property that an offender can identify and is willing to engage with, and capable guardians are any person or object whose presence can prevent the commission of a crime. Cohen and Felson make a key assumption that the first element, the presence of a motivated offender, is a given, and that there will always be individuals present who are willing and ready to engage in criminal activity. Given this assumption, RAT considers the last two features – presence of suitable targets and a lack of guardianship – as being the core dimensions of criminal opportunity (Cohen and Felson 1979; Cullen et al. 2021). Cohen and Felson posit that the absence of any one of these three elements may be enough to prevent the successful completion of a crime.

Routine activities theory was created shortly after World War II and grew in popularity for its ability to explain crime rates given the changing economic context in the United States. During this time there existed a contradiction in which crime rates were rising but factors that had historically been considered causes of violent crime – such as lack of education, unemployment, and poverty – were decreasing (Miró 2014). Women were joining the workforce, there was a growing urban population, and more people had access to vacations – ultimately reducing the number of people available to provide guardianship over individuals and property (Cohen and Felson 1979; Buil-Gil et al. 2021). Also at this time, automobiles acted as a new tool for criminals and goods became more durable and more valuable – increasing offender mobility and making property crime physically easier and more monetarily beneficial. Violent and property crime increased dramatically during this time period, when the FBI Uniform Crime Report measured more than 150% increases in robberies, burglaries, aggravated assaults, rapes, and homicides in the 30 years following WWII (Cohen and Felson 1979). According to Cohen and Felson's new theory, the post-war shift in the workforce affected the structure of everyday life for many people, which in turn opened up new opportunities for motivated offenders through increased targets and less present guardians.

Ultimately, routine activities theory proposes an interdependence of illegal activities on legal ones and suggests that the structure of normal activities plays a large role in determining the quantities, types, and locations of crime at any given time (Cohen and Felson 1979; Cullen et al. 2021). While RAT was developed in the

context of post-war America and designed to review crime in physical spaces, the elements can be reflected across the modern cyberspace as well.

Routine Activities in the Cyberspace

RAT focuses on the convergence – or lack thereof – of three actors to predict the likelihood of crime: motivated offenders, suitable targets, and capable guardians. These actors exist across the Internet as well, making the cyberspace another venue for crime to occur (Stickle and Felson 2020; Dearden and Gottschalk 2023). While these same actors exist in both physical and technological spaces, the way they interact online versus in person is very different. Actors are much more transient in nature across the cyberspace than they are on the street (Hawdon et al. 2020). They come and go regularly and for short periods of time, and often have the ability to remain anonymous to other actors. In this venue, the convergence between the offender and their target that is needed for crime to occur can happen asynchronously – while one or more actors isn't currently present in the space. Also unlike traditional crime, cyberattacks can be launched from anywhere in the world, eliminating an offender's geographical barriers to suitable targets and greatly increasing their pool for victim selection (Hawdon et al. 2020; Lallie et al. 2021). The ways in which interactions between offenders and victims occur on the Internet make it a very versatile space for cyber-enabled and cyber-dependent crimes to occur.

The third actor of RAT, the guardian, also functions differently online than in real life. Guardianship is essentially nonexistent online, as most platforms do not have space for the role of a guardian in situations of convergence between an offender and a target (Hawdon et al. 2020; Johnson and Nikolovska 2022). Individuals may

employ security measures such as firewalls and antivirus programs that aim to protect network security from certain cybercrimes such as malware (malicious software) and computer viruses, but these measures do not hold up against communication-based cybercrime (Holt and Bossler 2008). Many cyber-dependent crimes occur via one-on-one communication channels such as email, phone call, and direct message, essentially eliminating the possible presence of a capable guardian who would likely, according to routine activities theory, be able to prevent the crime from occurring. Although slightly different from its application to offline crime, previous research has found support for the application of RAT to both individual and group-level cyber victimization (Maimon and Louderback 2019). Routine activities theory stands as the most frequently-applied theory to victim-based studies of cybercrime and may be similarly successful in explaining cybercrime trends as it historically has been with offline crime.

While contemporary criminologists have applied RAT to a variety of offline and online criminal contexts, there may not have existed a societal shift as significant as that of post-WWII in the four decades following the theory's inception. However, that may have changed with the onset of the COVID-19 pandemic, which had similar, if not larger-scale implications on daily life. Given the notion by Cohen and Felson (1979) that routine activities determine the presence of people and property across space and time and thus influence their risk of victimization, it is probable that the changes in daily life that occurred as a result of the COVID-19 pandemic affected various U.S. crime trends.

Crime in the COVID-19 Pandemic

The routine activities theory was developed in context of a wide-spread change in daily life after WWII. Whereas the mid-to-late 1900s saw an increase in property crime after a shift away from the home, the COVID-19 pandemic shifted masses into their homes – affecting crime trends in an inherently "opposite" way. Recent research has supported this idea, finding decreases in property crime after the introduction of stay-at-home orders (Koppel et al. 2023; Rosenfeld et al. 2023). RAT may explain this change in property crime that occurred after a shift in daily life as a result of the COVID-19 pandemic and may further be applied to cybercrime trends during the same time period.

Property Crime in the COVID-19 Pandemic

Many criminologists have used the shift to virtual life caused by the COVID-19 pandemic to test the routine activities theory, as criminal opportunity as defined by RAT changed greatly during this time. Historically, people and their property were often separated for several hours a day as a result of routine work activities (Cohen and Felson 1979). As previously discussed, however, this time away from the home was nearly nonexistent for many Americans during the COVID-19 lockdown. Widespread social isolation resulted in fewer targets in public spaces and more guardians in households, which minimized the opportunity for violent and property crime. Recent studies have found post-lockdown decreases in robberies, residential burglaries, and larcenies in the early months of the pandemic (Ashby 2020; Regalado et al. 2022; Koppel et al. 2023; Rosenfeld et al. 2023). Ashby (2020) found a short-term decrease in residential burglaries from January to May 2020 in 8 of 11 examined

cities. Rosenfeld and colleagues (2023) found similar evidence in support of a longer-term trend, reporting a 26% decrease in residential burglaries from 2019 to 2022. When examining non-residential burglaries, however, it was found that 90% of examined cities saw an increase, to which the author credits a lack of guardianship as a result of many of these locations being closed to the public during lockdown (Ashby 2020). These findings support the routine activities approach that suggests a likely change in property crime given a shift of everyday life away from public areas and toward the home.

Contrast to most other COVID-related crime research, Rosenfeld and colleagues (2023) completed a more long-term analysis, looking beyond just the start of lockdown and utilizing data through December 2022. Outside of their results of a continued decrease in residential burglaries, they found that larcenies – which decreased 14% from 2019 to 2021 – rose 8% between 2021 and 2022, and they found a similar pattern for motor vehicle thefts. They attributed this trend to a slow return to "normalcy" in 2022 which, similarly to the post-WWII context in which RAT was developed, is categorized by an increasing number of people leaving the home. 2021 and later is when communities started to see an increased return of a pre-pandemic lifestyle, such as the re-opening of stores and increased people in public, resulting in more opportunity for theft of property and vehicles.

Property crime trends seen after the rise of the COVID-19 pandemic may be attributed to the changes in routine activities that occurred during that time, which resulted in more guardianship and less suitable targets. Since routine activities theory has been applied to cybercrime in similar ways to its historical application to violent

and property crime, it may be the case that a change in routine activities that affects property crime trends would also be associated with changing cybercrime trends.

Cybercrime in the COVID-19 Pandemic

The COVID-19 pandemic created a displacement of legitimate activities from a physical to an online environment. Buil-Gil and colleagues (2021) suggest that crime opportunities were displaced in a similar manner. In a time where socialization moved primarily online, there would have been more opportunities for the elements of routine activities theory – motivated offender, suitable target, and absence of a capable guardian – to converge via the internet (Miró-Llinares and Moneva 2019; Buil-Gil et al. 2021).

As noted earlier in the paper, Cohen and Felson made the assertion in their original development of RAT that there is always a presence of motivated offenders. The current research assumes that the authors' original assumption of an ever-present motivated offender remains true in the cyberspace and thus focuses primarily on the two remaining actors: the target and the guardian.

Guardianship on the internet, as previously mentioned, is often very limited. This is likely due to the one-on-one communication channels frequently used by cyber criminals, such as text, phone call, e-mail, or direct messaging. These communication types are often utilized during the commitment of cybercrimes as they often ultimately prevent the opportunity for a capable guardian to be present in the space.

The pandemic also afforded cybercriminals an especially unique group of vulnerable targets to exploit. During this time of crisis, many individuals faced

heightened stress as a result of the pandemic, essentially making them an even more suitable target (Lallie et al. 2021). This could likely be attributed to a variety of factors, including health anxieties, unemployment, or the simultaneous balancing of work, family, and childcare duties. There were also individuals with low technological literacy essentially being forced into this virtual environment with little-to-no knowledge of how to keep themselves safe online. Since it is known that RAT can be legitimately applied to cybercrime in the ways it can be to property crime, it is likely that this shift in routine activities to the online environment would be associated with increasing cybercrime trends.

In the United Kingdom, Buil-Gil and colleagues (2021) found significant short-term increases in the fraud and hacking of personal computers, social media accounts, and email accounts through May 2020. A similar study was conducted in the United States by Hawdon and colleagues (2020). While it is known that there are reporting discrepancies for cyber-related crimes across jurisdictions, the data utilized in this study came from police agencies in 11 major cities (Cain and Goodwin 2023). Similar to Buil-Gil's work, this research also utilized data through May 2020 but comparatively found no significant changes in cybercrime victimization after the start of the pandemic. In both of these studies, the analysis was extremely short-term, only including data up to 3 months post pandemic-onset. This leaves a looming gap in knowledge about the long-term state of overall cybercrime victimization trends in the U.S. following the beginning of the COVID-19 pandemic.

Chapter 3: Data and Methods

Current Study

The current research helps to fill a gap in existing literature concerning cybercrime trends in the United States during the COVID-19 pandemic. This study uses U.S.-based data through 2023 to examine general cyber-enabled and cyber-dependent crime trends. The research employs an Interrupted Time Series Analysis to compare annual crime complaints and resulting financial loss from years before and after the declaration of COVID-19 as a global pandemic. Based on the earlier review of literature, the tenets of the routine activities theory, and the context of the COVID-19 pandemic, the current research poses the following hypothesis:

H1. Cybercrime victimization increased in the United States after the declaration of the COVID-19 pandemic.

This work aims to build upon existing literature by utilizing aggregate data and extending the post-pandemic analysis beyond what previous research has included.

Data

This research uses data from the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) annual reports. IC3 reports are publicly-accessible sources that provide information aggregated by year about the quantity and types of Internet crime reported to the IC3. IC3 data is gathered through self-reported victimization complaints completed by individuals on the IC3 website. Individuals may file a complaint on their own accord or oftentimes are directed to do so by local and state

law enforcement agencies (Internet Crime Complaint Center 2022). These complaints may be filed by the victim themself or on behalf of another person who was victimized. Complaints may be filed for crimes that were completed as well as unsuccessful attempts at criminal activity.

The IC3 defines Internet crime as "any illegal activity involving one or more components of the Internet, such as websites, chat rooms, and/or email. Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers" (Internet Crime Complaint Center n.d.). These crimes include, but are not limited to, credit card fraud, phishing, spoofing, and malware. A full list of cyber-enabled and cyber-dependent crimes and their definitions as provided by the IC3 can be found in Appendix A.

Data from each annual IC3 Report from 2005 to 2023 were used to create the dataset for this project. This wide range of years was selected purposefully with the intent of including cybercrime trends through various phases and changes in technology prior to the COVID-19 pandemic. The recorded dependent variables are Internet Crime Complaints Received and Financial Loss.

Measures

Dependent Variables

Internet Crime Complaints Received. The annual IC3 reports provide a consistent measure of the total number of reported cybercrime complaints for each year. As previously noted, the IC3's definition of this measure is all-encompassing and does not specify any excluded Internet-related crime types (see Appendix A).

This metric is not limited to solely completed crimes and does include crime attempts as well, and the difference between attempted versus completed crimes is not distinguishable in the data.

Financial Loss. The IC3 reports provide a measure of estimated total financial losses as a result of Internet crime each year[1]. Comparing the amount of financial loss per year as a result of cyber victimization may be another signal of cybercrime trends. While the *Internet Crime Complaints Received* measure may include crime suspicions or attempts, this measure will only reflect successfully completed Internet crimes by reflecting the resulting financial loss.

Independent Variables

Presence of the COVID-19 Pandemic. The primary independent variable in the current study is the absence or presence of the COVID-19 pandemic. This potential effect of the pandemic on the aforementioned dependent variables was explored through three measures: Year, Presence of COVID-19, and Years Since 2020. The Year measure represents the year from which the IC3 annual report data was collected, ranging from 2005 to 2023. The Presence of COVID-19 measure was coded as a binary indicator variable denoting whether the yearly data was from before or after the declaration of COVID-19 as a global pandemic. Years 2005–2019 were coded as '0' indicating the absence of the pandemic, and years 2020-2023 were coded as '1' indicating the presence of the pandemic and stay-at-home measures[2]. The *Years*

[1] Financial Loss data was not provided in the IC3 report for the year 2010. The analysis of Financial Loss was completed treating 2010 as a NULL value.
[2] While COVID was not declared a pandemic until March of 2020, the year is coded as '1' because the data is aggregated for the entire year and a majority of months in 2020 saw the presence of the pandemic.

Since 2020 variable was coded in a similar fashion, with 2005–2019 being coded as '0' and 2020-2023 being coded as '1'–'4' respectively.

Analytical Method

This study employs an interrupted time series analysis (ITSA) to examine cybercrime trends before and after the onset of the COVID-19 pandemic. ITSA models are useful in examining these pre-vs.-post trends when the interruption is a discrete event, such as a policy change or natural disaster. In the case of COVID-19, the discrete interruption occurred on March 11, 2020, when the start of the pandemic was officially declared.

The ITSA model used examines the magnitude and significance of associations between *Year, Presence of COVID-19, and Years Since 2020* on both dependent variables: *Internet Crime Complaints Received and Financial Loss.* The relationship between variables was analyzed using the regression model:

$$\mathbf{(Y \sim T + D + P)}$$

where *Y* represents the dependent variable, *T* represents the year, *D* represents the presence of the COVID-19 pandemic, and *P* is the number of years since the beginning of the pandemic.

Chapter 4: Results

Descriptive Statistics

Comparing pre-vs-post measures for both dependent variables may provide insight into the cybercrime landscape before and after the pandemic onset. It is important to note that the measures of pre-pandemic statistics will provide a better picture of that crime landscape than in the post pandemic, as there is significantly more pre-pandemic data to analyze than there is post-pandemic data.

A total of 19 data points were analyzed for the *Crime Complaints Received* variable. The pre-interruption complaint data (n = 15) had a reported mean of 293,706 (SD = 61,522) and the post-interruption data (n = 4) had a reported mean of 830,132 (SD = 35,875). Notably, the post-interruption data had a higher mean but a smaller standard deviation than pre-pandemic, indicating less variability in the rates post-pandemic. This may suggest that complaints were fluctuating or continually rising before 2020, but after 2020 they increased significantly and remained around that higher measure in the following years.

A total of 18 data points were analyzed for the *Financial Loss* variable, as the 2010 IC3 report did not provide this estimate for that year. The pre-interruption financial data (n = 14) had a reported mean of $1,004,906,442 ($SD$ = $962,567,180) and the post-interruption data (n = 4) had a reported mean of $8,475,000,000 ($SD$ = $3,173,621,700). Given that both the average and variation increased after the onset of the pandemic, it may be the case that there was a spike in financial loss when the pandemic began that has continued to escalate in the years following.

Interrupted Time Series Analysis

The ITSA regression analyses yielded multiple significant results. The first analysis was used to examine the relationships between the predictor variables and number of Internet Crime Complaints Filed (Table 1). This analysis found that Year (*T*) had a significant positive relationship with Internet Crime Complaints Filed (β = 10067.38, p = .002). The relationship between these variables indicates that prior to the onset of the pandemic, cybercrime was increasing significantly. Also significant with Internet Crime Complaints Filed was Pandemic Presence (D) (β = 411091.35, $p < .001$). This signifies that the already increasing levels of cybercrime were exacerbated when the COVID-19 pandemic began in 2020.

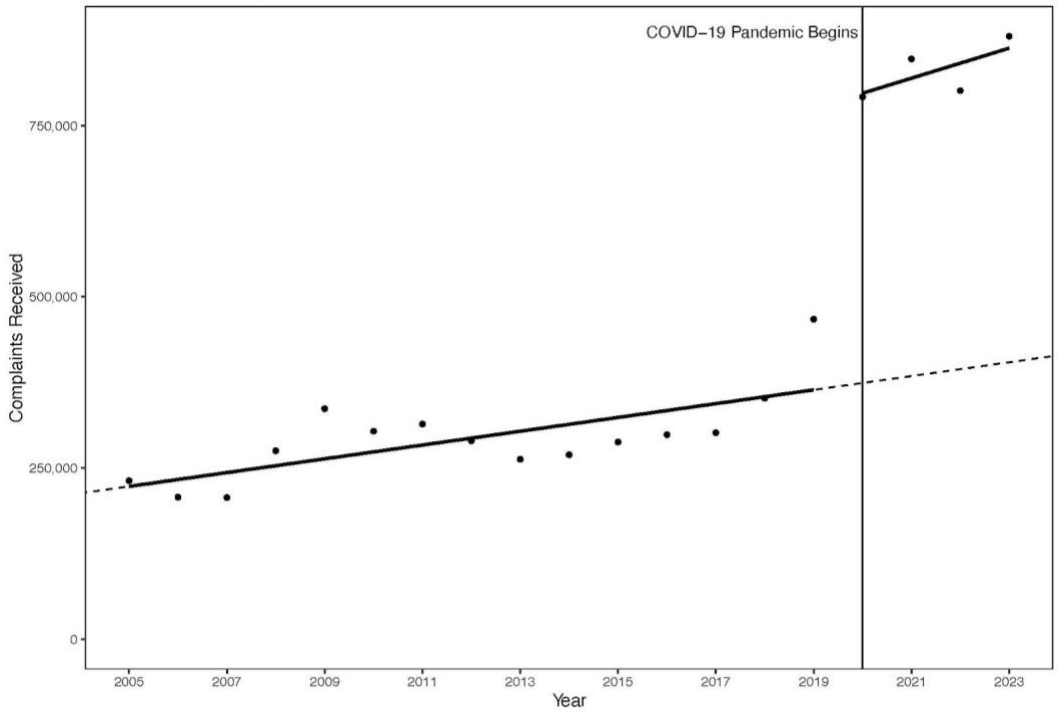
Table 1: Complaints Filed Regression Model Summary

Variable	β	Standard Deviation
Year (T)	10067.38**	2722.75
Pandemic Presence (D)	411091.35***	60127.00
Years Since 2020 (P)	11877.82	20556.32

*Note. * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$*

Figure 1 is a visual representation of the regression model between the predictor variables and Internet Crime Complaints Filed. While the slope remained relatively stable, at *T*=2020 there is a large immediate increase in the number of complaints filed. This is representative of the significance of the COVID-19 pandemic in predicting complaints filed.

Figure 1: Complaints Filed Time Series



The second regression model was used to examine relationships between the predictor variables and recorded Financial Loss (Table 2). This analysis found that Year (*T*) had a significant positive relationship with Financial Loss (β = 180891836.78, $p < .001$). The relationship between these variables indicates that prior to the onset of the pandemic, as time passed, significantly increasing financial losses were being suffered due to cybercrime victimization. Years Since 2020 (P) was also a positive, significant predictor of Financial Loss (β = 2649108163.22, $p < .001$). This signifies that while financial loss rates were already growing prior to the pandemic, they began increasing at a significantly higher rate with each year that passed beyond 2020.

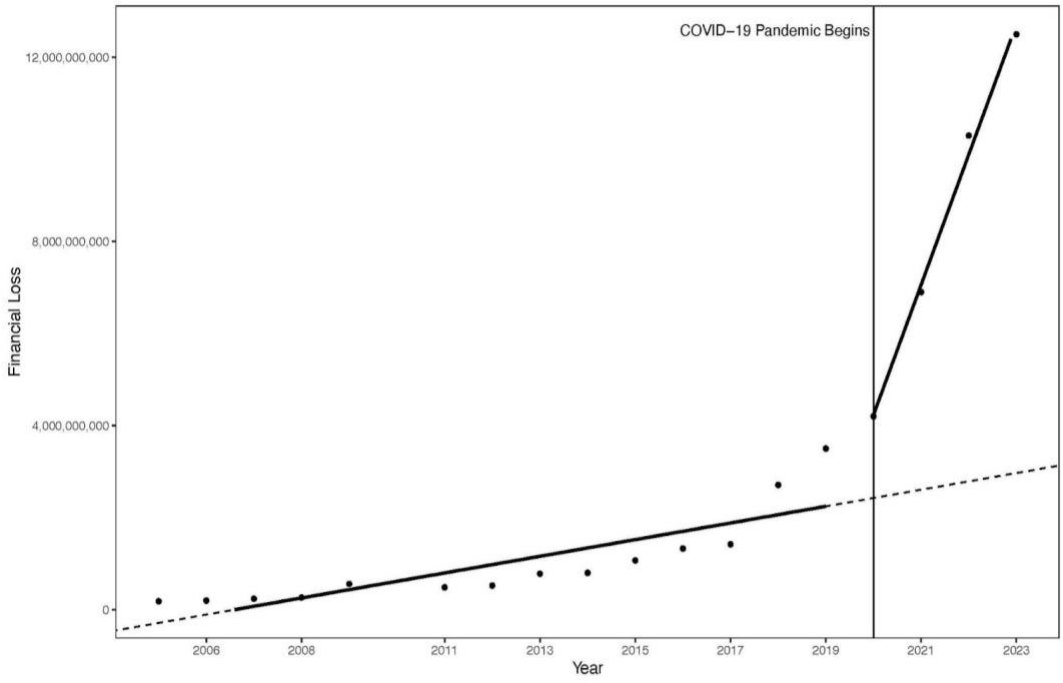
Table 2: Financial Loss Regression Model Summary

Variable	β	Standard Deviation
Year (T)	180891836.78***	31729910.34
Pandemic Presence (D)	-845307608.39	695374369.92
Years Since 2020 (P)	2649108163.22***	237747577.30

Note. $p < 0.05$, $p < 0.01$, $p < 0.001$

Figure 2 is a visual representation of the regression model between the predictor variables and Financial Loss. At *T*=2020, there is a steep increase in the rate of financial loss, which continues to grow through the end of the graph. This is representative of the number of years since 2020 being a significant predictor of financial loss.

Figure 2: Financial Loss Time Series



Chapter 5: Discussion

The results of the analyses provide important insights to the story of cybercrime trends during and after the COVID-19 pandemic. The decreased variability found in pre-vs-post measures of *Internet Crime Complaints Filed* suggests that there was a more consistent pattern of online criminal activity following the onset of the pandemic. Figure 1, which illustrated a sudden, drastic increase in reports filed beginning in 2020 directly parallels the immediate shift to a virtual environment that was experienced after the start of the pandemic.

Figure 2 shows a surge in the rate at which financial loss is occurring as a result of cybercrime and may indicate increasing levels of success in the tactics being employed by cybercriminals. The increase seen immediately in complaints received and gradually in the financial losses recorded visualize the complex dynamic that exists when attempting to measure cybercrime. By exploring both of these variables, the results serve provide both quantitative and qualitative descriptions of cybercrime trends. In combination, these variables provide a birds-eye view of overall cybercrime victimization, a measure that is not yet available in any official data.

This overall increase in cyber victimization directly reflects the established changes in routine activities that occurred during the pandemic. This is consistent with the findings by Rosenfeld and his colleagues (2023) who attributed a decrease in property crime to the shift away from the street and into the home. The findings of the current study support the previous notion that the change in lifestyle as a result of the pandemic was associated with a change in crime trends.

The results of this study likely differ from the previous findings of Hawdon and colleagues (2020) due to both the vastly different time frames and data sources analyzed. Whereas the previous work sampled data from major cities and examined less than 12 weeks of post-pandemic trends, the current research utilized aggregate data to observe general trends and was able to extend analysis to 4 years post-pandemic. The differing findings between short and long-term studies and the varying potential data sources for measuring cyber victimization shows the lack of research in the area and highlights the need for further clarification.

Limitations

Examining the limitations of the current study may help guide future research directions. The looming issue surrounding the examination and measurement of cybercrime trends is the lack of comprehensive data on the subject. At this time, although currently in progress, there exists no Department of Justice taxonomy for cyber-enabled and cyber-dependent crimes (Cain and Goodwin 2023). This prohibits any cyber-specific data collection by the National Incident Based Reporting System, which serves as the official crime statistics measure for the United States. This prohibits researchers from making accurate comparisons of cybercrime data due to varying cybercrime definitions and measurements by jurisdiction. Lack of official reporting measures not only makes research advancements in the area difficult, but also leaves the U.S. worse off as it comes to protecting from and defending against cyberattacks.

This lack of official data leaves current research to depend primarily on self-reported data, as is the case with the IC3 annual reports. This means that the quantity

and quality of available data relies on a victim's knowledge that (1) they were victimized and (2) this entity exists for them to report the crime to. Given these reasons, it is likely that the annual IC3 report data is a rather conservative measure of cybercrime statistics.

Future Directions

Given the limitations with current cybercrime reporting practices and with the self-reported nature of the IC3 annual report data, it is crucial that previous work, including the current study, are replicated as better data sources become available. Future research should also continue to extend the current analysis beyond four years to see if the sudden increase in complaints remains at this post-pandemic level as well as if recorded financial losses continue to trend upward. To advance the current work on routine activities theory in the cyberspace, researchers may consider investigating the nature of online offending and can utilize the COVID-19 pandemic in ways similar to the current research. This work should examine whether pre-pandemic street criminals shifted to online criminal activity in a way similar to victims moving online, or if the identified increase in cyber victimization is attributed to non-standard criminal actors who only commit crimes via computer. In terms of security and policy-related research, future studies should examine trends of individual types of cybercrime to determine if any specific types of cyberattack should be the focus of security efforts in the post-pandemic world.

Chapter 6: Conclusion

Amid the COVID-19 pandemic, criminal justice researchers focused primarily on how property and street crime were changing as everyday life shifted to a virtual environment. Yet, within this discourse lies a glaring oversight: the potential for crime to escalate in the online domain. The current research aimed to address this gap by determining the magnitude of crime threats in the cyberspace. The analysis revealed an upward trend of the number and severity of cybercrime attempts following the pandemic's inception in 2020. These findings highlight the need to broaden COVID-related crime research to include the digital landscape.

Beyond the implications that this research has regarding the implementation of cybersecurity measures, it also highlights another crucial gap: the collection of cybercrime data. This research points to cybercrime as being a growing crime tactic, but this will be a difficult one to combat without proper documentation of attacks. As society continues to build both in-person and virtually, crime serves to become more complex and technologically innovative. By prioritizing this growing threat, society can better equip itself to confront the evolving threats posed by cybercriminals, ultimately fostering a safer and more secure digital environment.

Appendices

APPENDIX A. IC3 CYBERCRIME DEFINITIONS

Advanced Fee: An individual pays money to someone in anticipation of receiving something of greater value in return, but instead, receives significantly less than expected or nothing.

Business Email Compromise (BEC): BEC is a scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments. These sophisticated scams are carried out by fraudsters by compromising email accounts and other forms of communication such as phone numbers and virtual meeting applications, through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Botnet: A botnet is a group of two or more computers controlled and updated remotely for an illegal purchase such as a Distributed Denial of Service or Telephony Denial of Service attack or other nefarious activity.

Confidence/Romance Fraud: An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator. This includes the Grandparent's Scheme and any scheme in which the perpetrator preys on the complainant's "heartstrings."

Credit Card Fraud/Check Fraud: Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism (ACH. EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Data Breach: A data breach in the cyber context is the use of a computer intrusion to acquire confidential or secured information. This does not include computer intrusions targeting personally owned computers, systems, devices, or personal accounts such as social media or financial accounts.

Employment: An individual believes they are legitimately employed and loses money, or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Government Impersonation: A government official is impersonated in an attempt to collect money.

Harassment/Stalking: Repeated words, conduct, or action that serve no legitimate purpose and are directed at a specific person to annoy, alarm, or distress that person. Engaging in a course of conduct directed at a specific person that would cause a reasonable person to fear for his/her safety or the safety of others or suffer substantial emotional distress.

Identity Theft: Someone steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes and/or (account takeover) a fraudster obtains account information to perpetrate fraud on existing accounts.

Investment: Deceptive practice that induces investors to make purchases based on false information. These scams usually offer the victims large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).

IPR/Copyright and Counterfeit: The illegal theft and use of others' ideas, inventions, and creative expressions – what's called intellectual property – everything from trade secrets and proprietary products and parts to movies, music, and software.

Lottery/Sweepstakes/Inheritance: An Individual is contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative.

Malware: Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

Non-Payment/Non-Delivery: Goods or services are shipped, and payment is never rendered (nonpayment). Payment is sent, and goods or services are never received, or are of lesser quality (non-delivery).

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder to another individual or business.

Personal Data Breach: A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Phishing: The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Real Estate: Loss of funds from a real estate investment or fraud involving rental or timeshare property.

SIM Swap: The use of unsophisticated social engineering techniques against mobile service providers to transfer a victim's phone service to a mobile device in the criminal's possession.

Spoofing: Contact information (phone number, email, and website) is deliberately falsified to mislead and appear to be from a legitimate source. For example, spoofed phone numbers making mass robo-calls; spoofed emails sending mass spam; forged websites used to mislead and gather personal information. Often used in connection with other crime types.

Tech Support: Subject posing as technical or customer support/service.

Threats of Violence: An expression of an intention to inflict pain, injury, self-harm, or death not in the context of extortion.

Bibliography

AJMC Staff. 2021. “A Timeline of COVID-19 Developments in 2020.” *The American Journal of Managed Care*. Retrieved (https://www.ajmc.com/view/a-timeline-of-covid19-developments-in-2020).

Anon. n.d. “Cyber Choices.” *National Crime Agency*. Retrieved May 9, 2024 (https://nationalcrimeagency.gov.uk/cyber-choices).

Ashby, Matthew P. J. 2020. “Initial Evidence on the Relationship between the Coronavirus Pandemic and Crime in the United States.” *Crime Science* 9(1):6. doi: 10.1186/s40163-020-00117-6.

Buil-Gil, David, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. 2021. “Cybercrime and Shifts in Opportunities during COVID-19: A Preliminary Analysis in the UK.” *European Societies* 23(sup1):S47–59. doi: 10.1080/14616696.2020.1804973.

Cain, Marisol, and Gretta Goodwin. 2023. *Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics*. United States Government Accountability Office.

CDC. 2023. “CDC Museum COVID-19 Timeline.” *Centers for Disease Control and Prevention*. Retrieved October 11, 2023 (https://www.cdc.gov/museum/timeline/covid19.html).

Cohen, Lawrence E., and Marcus Felson. 1979. “Social Change and Crime Rate Trends: A Routine Activity Approach.” *American Sociological Review* 44(4):588–608. doi: 10.2307/2094589.

Cullen, Francis T., Robert Agnew, and Pamela Wilcox, eds. 2021. *Criminological Theory: Past to Present*. 7th ed. Oxford University Press.

Dearden, Thomas E., and Petter Gottschalk. 2023. "Convenience Theory and Cybercrime Opportunity: An Analysis of Online Cyber Offending." *Deviant Behavior* 0(0):1–13. doi: 10.1080/01639625.2023.2246626.

Haan, Katherine. 2023. "Remote Work Statistics & Trends In 2023." *Forbes Advisor*. Retrieved (https://www.forbes.com/advisor/business/remote-work-statistics/).

Hawdon, James, Katalin Parti, and Thomas E. Dearden. 2020. "Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment." *American Journal of Criminal Justice* 45(4):546–62. doi: 10.1007/s12103-020-09534-4.

Holt, Thomas J., and Adam M. Bossler. 2008. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization." *Deviant Behavior* 30(1):1–25. doi: 10.1080/01639620701876577.

Internet Crime Complaint Center. 2005. *2005 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2006. *2006 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2007. *2007 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2008. *2008 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2009. *2009 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2010. *2010 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2011. *2011 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2012. *2012 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2013. *2013 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2014. *2014 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2015. *2015 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2016. *2016 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2017. *2017 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2018. *2018 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2019. *2019 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2020. *2020 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2021. *2021 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2022. *2022 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. 2023. *2023 Internet Crime Report*. Federal Bureau of Investigation.

Internet Crime Complaint Center. n.d. "Internet Crime Complaint Center(IC3) | FAQs." Retrieved November 7, 2023 (https://www.ic3.gov/Home/FAQ).

Johnson, Shane D., and Manja Nikolovska. 2022. "The Effect of COVID-19 Restrictions on Routine Activities and Online Crime." *Journal of Quantitative Criminology*. doi: 10.1007/s10940-022-09564-7.

Kemp, Steven, David Buil-Gil, Asier Moneva, Fernando Miró-Llinares, and Nacho Díaz-Castaño. 2021. "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19." *Journal of Contemporary Criminal Justice* 37(4):480–501. doi: 10.1177/10439862211027986.

Koppel, Stephen, Joel A. Capellan, and Jon Sharp. 2023. "Disentangling the Impact of Covid-19: An Interrupted Time Series Analysis of Crime in New York City." *American Journal of Criminal Justice* 48(2):368–94. doi: 10.1007/s12103-021-09666-1.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. “Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic.” *Computers & Security* 105:102248. doi: 10.1016/j.cose.2021.102248.

Maimon, David, and Eric R. Louderback. 2019. “Cyber-Dependent Crimes: An Interdisciplinary Review.” *Annual Review of Criminology* 2(1):191–216. doi: 10.1146/annurev-criminol-032317-092057.

Miró, Fernando. 2014. “Routine Activity Theory.” Pp. 1–7 in *The Encyclopedia of Theoretical Criminology*, edited by J. M. Miller. Wiley.

Miró-Llinares, Fernando, and Asier Moneva. 2019. “What about Cyberspace (and Cybercrime alongside It)? A Reply to Farrell and Birks ‘Did Cybercrime Cause the Crime Drop?’” *Crime Science* 8(1):12. doi: 10.1186/s40163-019-0107-y.

Parker, Kim, Juliana Menasce Horowitz, and Rachel Minkin. 2022. “COVID-19 Pandemic Continues To Reshape Work in America.” *Pew Research Center*. Retrieved (https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/).

Perera, Ashlyn. 2024. “Routine Activities Theory: Definition & Examples.” *Simply Psychology*. Retrieved May 9, 2024 (https://www.simplypsychology.org/routine-activities-theory.html).

Regalado, Jullianne, Anastasiia Timmer, and Ali Jawaid. 2022. “Crime and Deviance during the COVID-19 Pandemic.” *Sociology Compass* 16(4):e12974. doi: 10.1111/soc4.12974.

Rosenfeld, Richard, Bobby Boxerman, and Ernesto Lopez. 2023. *Pandemic, Social Unrest, and Crime in U.S. Cities*. Council on Criminal Justice.

Stickle, Ben, and Marcus Felson. 2020. “Crime Rates in a Pandemic: The Largest Criminological Experiment in History.” *American Journal of Criminal Justice* 45(4):525–36. doi: 10.1007/s12103-020-09546-0