Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score

Eileen Decker[*]

INTRODUCTION

Cyberattacks are the fastest growing crime in the U.S.[1] Recent reports indicate a 473% increase in healthcare email fraud over a two-year period,[2] an increase in online crimes against children,[3] an increase in cyberattacks through mobile devices,[4] and a 40.9% increase in global phishing attacks.[5] The large number of victims involved in these attacks leave few people unaffected: an estimated 500 million user accounts were exposed in the Marriott Corporation hack;[6] an estimated 3 billion user accounts were impacted in the Yahoo hack;[7] and an estimated 145.5 million customers were compromised in the 2017 Equifax breach.[8] Government systems are equally vulnerable: the OPM attack disclosed over 21 million highly confidential personnel records at an estimated cost of over $1 billion;[9] the 2018 ransomware attack on Atlanta crippled city services and cost millions;[10] and the City of Baltimore continues to struggle in its recovery from the 2019 attack on its cyberinfrastructure. The financial impact of ransomware attacks in 2015 was estimated to be $325

[*] Eileen M. Decker is the President of the Los Angeles Police Commission; a Fulbright Specialist in Cybersecurity Law & Policy; and an Adjunct Professor in Cybersecurity, Privacy, and National Security Law at USC and UCLA Law Schools. Formerly, she served as the U.S. Attorney for the Central District of California, the Los Angeles City Deputy Mayor for Homeland Security and Public Safety, and Chief of the National Security Section at the United States Attorney's Office in Los Angeles.

[1] STEVE MORGAN, CYBERSECURITY VENTURES, 2019 OFFICIAL ANNUAL CYBERCRIME REPORT 3 (2019), https://perma.cc/RA5W-WMNX; Abigail Summerville, *Protect Against the Fastest-growing Crime: Cyber Attacks*, CNBC (July 25, 2017, 1:12 PM), https://perma.cc/H4QU-ZNA2.

[2] Help Net Security, *Healthcare Email Fraud: Attack Attempts Jump 473% Over Two Years*, HELP NET SECURITY (Feb. 13, 2019), https://perma.cc/X9ZH-6D8Y.

[3] Courtney Fromm, *Internet Crimes Against Children Unit Warns of Increase in Child Exploitation*, FOX 21 NEWS (Mar. 6, 2019, 10:11 PM), https://perma.cc/S56M-S3KK.

[4] Danny Palmer, *Mobile Malware Attacks are Booming in 2019: These are the Most Common Threats*, ZDNET (July 25, 2019, 8:00 AM), https://perma.cc/98PY-3Q2U.

[5] *See 2019 Phishing Trends and Intelligence Report*, PHISHLABS (2019), https://perma.cc/Z2Q3-VGUF.

[6] Nicole Perlroth, Amie Tsang & Adam Satariano, *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES (Nov. 30, 2018), https://perma.cc/3ADL-QHHU.

[7] Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://perma.cc/4P2E-DEN5.

[8] Wash. Post, *Every Type of Personal Data Equifax Lost to Hackers: 145 Million Social Security Numbers, 99 Million Addresses and More*, L.A. TIMES (May 8, 2018, 3:36 PM), https://perma.cc/AW3W-9JXQ.

[9] Chris Townsend, *OPM Breach Cost Could Exceed $1 Billion*, SYMANTEC OFFICIAL BLOG (Mar. 23, 2017), https://perma.cc/TG39-5VPK.

[10] Lily Hay Newman, *Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare*, WIRED (Apr. 23, 2018, 8:55 PM), https://perma.cc/TD7C-GS9R; Morgan Wright, *A Ransomware Attack Brought Atlanta to its Knees – and No One Seems to Care*, THE HILL (Apr. 4, 2018, 11:01 AM), https://perma.cc/V7BZ-F4KV.

million, but by 2017 grew 1400% to $5 billion.[11] As of 2018, malicious cyber activity cost the U.S. economy between $57 and $109 billion annually.[12]

Government agencies and officials repeatedly confirm the seriousness of this modern-day crime spree. According to the U.S. Department of Justice (DOJ):

> Cyber-enabled attacks are exacting an enormous toll on American businesses, government agencies, and families. Computer intrusions, cybercrime schemes, and the covert misuse of digital infrastructure have bankrupted firms, destroyed billions of dollars in investments, and helped hostile foreign governments launch influence operations designed to undermine fundamental American institutions.[13]

In March 2019, former Homeland Security Secretary Kirstjen Nielson offered a dire assessment of the state of criminal cyber conduct:

> Threat actors are mercilessly targeting everyone's devices and networks. They are compromising, co-opting and controlling them, and they are weaponizing our own innovation again against us… Today I am more worried about the ability of bad guys to hijack our networks than their ability to hijack our flights. And I am concerned about them holding our infrastructure hostage, stealing our money and secrets, exploiting children online and even hacking our very democracy.[14]

Despite cybercrime's impact on individuals, businesses, and government, and despite the near universal recognition that this is a mammoth problem, accurate data about the type, frequency, and cost of cybercrime is challenging to obtain. The federal government fails to measure cybercrime in a meaningful way. The FBI manages a voluntary self-reporting online database but admits that it captures only about 12% of cybercrime. Cybercrime data, such as the data cited in this introduction, largely come from private sources whose own sources, methods, and accuracy often cannot be verified.

Identifying, stopping, and punishing cybercriminals and other malicious actors first requires defining and measuring the cybercrime problem with greater accuracy. Accurate assessments can better define the types of cybercrime being committed, the evolving nature of and trends in cybercrime, the training necessary for law enforcement to address the criminal challenge, and the investment government should undertake to tackle and counter the actions of cybercriminals. Experience demonstrates that crime data can successfully be used to counter and address criminal trends and to effectively train and deploy law enforcement officers in the areas where

[11] Wright, *supra* note 10.

[12] COUNCIL OF ECON. ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1 (2018), https://perma.cc/2FL6-GDUL.

[13] U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE xi (2018), https://perma.cc/MTT3-DQCB.

[14] Kirstjen Nielson, Sec'y, Dep't of Homeland Sec., Remarks before the Center for Cyber and Homeland Security at Auburn University (Mar. 18, 2019), https://perma.cc/AZ4N-JLFX.

they are most needed. Absent data that informs cybercrime-fighting decisions, policymakers and criminal justice leaders cannot appropriately respond to this prolific crime.

Cybercrime presents law enforcement with a challenging adversarial situation. To succeed, we need to provide them with the data to fully understand the cyber playing field with greater specificity, to know and understand the rules of the game, to identify our opponents more clearly, and to consistently monitor and assess the cyber-scoreboard. It is only then that we can expect law enforcement to develop effective game-winning strategies to combat this 21st century adversary.

I. CYBERCRIME DATA COLLECTION PROGRAMS

There are two primary mechanisms through which the federal government collects data to measure U.S. crime, specifically: (1) the Uniform Crime Reporting ("UCR") Program, which historically collected crime data through a Summary Reporting System ("SRS") and which is now transitioning into a broader data collection system called the National Incident Based Reporting System ("NIBRS"); and (2) the National Crime Victimization Survey (NCVS), which surveys Americans and captures information about crime.[15] Both programs are important tools for estimating crime in the United States and are used by politicians, policymakers, advocates, law enforcement, and the public in evaluating crime. Neither, however, collects significant, consistent, or detailed data about cybercrime. Instead, the FBI collects cybercrime data through an underutilized, voluntary, self-reporting online system. This information can be supplemented through reports issued by many private sector groups that collect data regarding specific, but frequently unverified, experiences with cybercrime.

A. The UCR Program

The FBI's UCR program seeks to "generate reliable information for use in law enforcement administration, operation, and management; over the years, however, the data have become one of the country's leading social indicators."[16] The UCR program through which law enforcement agencies have traditionally reported crime data to the federal government is called the Summary Reporting System ("SRS"). The SRS tracks data on eight traditionally prevalent violent and property crimes: murder, robbery, rape, aggravated assault, burglary, theft, vehicle theft, and arson (referred to as Part I crimes). The SRS also collects data on 22 crimes traditionally

[15] There are additional crime reporting systems, such as: the Clery Act Collections on Crime on College and University Campuses; the Defense Incident-Based Reporting System; the National Fire Incident Reporting System; the National Child Abuse and Neglect Data System, among others. These important reporting systems are designed to address specific issues and topics, and the focus of this paper is on the comprehensive national crime reporting system.

[16] Fed. Bureau of Investigation, *Uniform Crime Reporting Program*, https://perma.cc/4L5U-36TX.

considered less prevalent, such as assault, forgery, fraud, embezzlement, vandalism, gambling, and vagrancy (referred to as Part II crimes).

This long-established voluntary SRS reporting system was created in 1929 after the International Association of Chiefs of Police (IACP) advocated for the development of a crime data collection program to consistently present national annual crime data. The Chiefs sought to reduce media pressure resulting from their reporting of sporadic crime increases, which often resulted in some police departments "cooking the books" to reduce the amount of recorded crime, even though there was no reduction in reported crime to the police.[17]

The IACP efforts first began in 1927, when it formed its Uniform Crime Records Committee charged with researching and developing a national uniform crime statistics reporting system. The Committee concluded that the offenses that were most well-known to the police would be the appropriate standard for a national crime measurement system.[18] The Committee, therefore, selected seven serious, frequent, and pervasive crimes that were the most likely to be reported to law enforcement: murder, rape, robbery aggravated assault, burglary, larceny/theft, and auto theft.[19]

In 1929, the IACP published an instructional manual for reporting crime statistics along with the definitions of specific crimes.[20] As a result of these efforts, law enforcement agencies from 400 cities submitted the first crime statistics to the IACP, which was then compiled and published in the first national crime report entitled "Uniform Crime Reports for the United States and Its Possessions."[21] In 1930, Congress authorized the Attorney General to collect this crime data,[22] and this authority was delegated to the FBI.[23] This same authority remains in place today and, throughout the years, the FBI has continuously administered the program by annually collecting and compiling crime data from law enforcement agencies across the nation and publishing the combined information.[24] In 1958, the FBI began using this data to estimate annual crime rates for the nation[25] and created a national crime index[26] to serve as a general indicator of national criminality.[27] Since its inception, some modest updates have been made to the

[17] MICHAEL D. MALTZ, BUREAU OF JUSTICE STATISTICS, BRIDGING GAPS IN POLICE CRIME DATA 4 (1999), https://perma.cc/7C3Y-7EBC.

[18] FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, UNIFORM CRIME REPORTING HANDBOOK 2 (2004), https://perma.cc/54FL-P62A.

[19] *Id.*; *see also* CLAYTON J. MOSHER ET AL., MISMEASURE OF CRIME 60 (2002).

[20] MOSHER ET AL., *supra* note 19.

[21] *Id.*

[22] 28 U.S.C. § 534 (2011) (the Attorney General is directed to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records").

[23] UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2.

[24] *See, e.g., 2017 Crime in the United States: About Crime in the U.S. (CIUS)*, FED. BUREAU OF INVESTIGATION, https://perma.cc/FN8C-E662.

[25] MALTZ, *supra* note 17, at 4.

[26] The total number of reported murder, rape, robbery, aggravated assault, burglary, larceny/theft (over $50), and auto theft offenses (arson was added to the index in 1979). MALTZ, *supra* note 17, at 1.

[27] UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2.

program,[28] but the SRS national crime data collection system remains largely built on the original 1929 concepts of crime.

Over the years, the responsibilities of the FBI's UCR program expanded from just the SRS crime data collection program to include the collection of information on other matters. For example, in 1960 the UCR program started to collect national statistics on law enforcement officers killed in the line of duty,[29] and in 1972 assaults on officers were added to the data collection process.[30] In 2015, the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board[31] recommended that the FBI collect data on the use of force by police officers.[32] Four years later, in January 2019, the FBI announced that the UCR program would begin the collection of National Use of Force Data, with the stated goal of collecting a comprehensive view of the circumstances and officers involved in use-of-force incidents.[33]

Congress has also charged the UCR program with the collection of data relating to specific growing national crime trends, which frequently reflect changing national priorities and/or growing concerns of policy makers. For example,

- Hate Crimes: In 1990, Congress passed the Hate Crime Statistics Act[34] requiring the collection of data about "crimes that manifest evidence of prejudice based on race, religion, sexual orientation, or ethnicity."[35] In 1994, Congress amended the Act to include bias against a physical or mental disability.[36]
- Cargo Theft: In 2006, Congress passed the USA PATRIOT Improvement and Reauthorization Act of 2005, which, among other things, requires "that reports of cargo theft collected by federal, state, and local officials are reflected as a separate category in the FBI Uniform Crime Reporting (UCR) System."[37] This addition was deemed necessary "[d]ue to the significant economic impact cargo theft has on the United States

[28] *Id.* (changes to the program occurred over the years when the program sought more specific information on the list of reported crimes. For example: in 1952, collection began on the age, sex, and race of people arrested for crimes; in 1962, through the Supplementary Homicide Report (SHR), collection began on the age, sex, and race of murder victims, the weapon used, and the circumstances surrounding the offense; in 2015, crime data collection began for federal agencies, in an effort to offer a more comprehensive and inclusive view of national crime trends.); FED. BUREAU OF INVESTIGATION, 2017 CRIME IN THE UNITED STATES: FEDERAL CRIME DATA (2017), https://perma.cc/U7NM-X3JW.

[29] UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2.

[30] *Id.*

[31] *The CJIS Advisory Process: A Shared Management Concept*, FED. BUREAU OF INVESTIGATION, https://perma.cc/834W-ZE5N (The CJIS Advisory Policy Board advises the FBI Director on a number of matters, including the UCR.).

[32] *National Use-of-Force Data Collection*, FED. BUREAU OF INVESTIGATION, https://perma.cc/RH2V-NLUZ.

[33] *Id.*

[34] 28 U.S.C. § 534 (2011); *see also* WILLIAM J. KROUSE, CONG. RESEARCH SERV., RL33403, HATE CRIME LEGISLATION 8 (2010), https://perma.cc/5ZMQ-LL8P.

[35] UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 3.

[36] *See id.*; *see also* 28 U.S.C. § 534.

[37] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 307(d), 120 Stat. 192, 240 (2006).

economy, and the potential for use by terrorist organizations."[38] The first publication of cargo theft data was in 2013.[39]

- Human Trafficking: In 2008, Congress passed the William Wilberforce Trafficking Victims Protection Reauthorization Act, requiring the collection of human trafficking offense data and requiring distinctions be made between prostitution, assisting or promoting prostitution, and purchasing prostitution.[40] The first Human Trafficking Report was published in 2013.

Separate reports are now issued to reflect the UCR program's data collection for hate crimes, cargo theft, and human trafficking, which were mandated by Congress.[41] This data is not reflected in the SRS annual national crime report, which is still fundamentally based on the IACP's 1929 definitions of Part I and Part II crimes.

On two occasions, the crimes reported to the SRS program were changed or modified:

- Arson: Congress mandated the collection of arson data in 1978,[42] and in 1982 Congress required the FBI to permanently count arson as a Part I offense.[43]
- Rape: In 2012, the definition of rape was updated. The new definition, long advocated for by sexual assault survivors and advocates, was intended to be more inclusive of all forms of sexual penetration and a better reflection of state criminal codes. Collection of the more expansive data began in 2013.[44]

Overall, the addition of crimes to the UCR program for data collection purposes is rare, and it is especially rare for changes to be made to the original list of Part I and Part II crimes collected through the SRS program. The additions made, usually mandated by Congress, reflect changing social norms, changes in the criminal justice system, and societal expectations that did not exist when the 1929 crime data collection system was originally established. Even with relatively modest changes to the crime data collection program, it typically takes years for local law

[38] FED. BUREAU OF INVESTIGATION, 2017 CRIME IN THE UNITED STATES: CARGO THEFT, https://perma.cc/62U2-JJTK.

[39] *Id.*

[40] *See* FED. BUREAU OF INVESTIGATION, HUMAN TRAFFICKING IN THE UNIFORM CRIME (UCR) PROGRAM (2013), https://perma.cc/F4FF-RWBH; *see also* 22 U.S.C. §§ 7101-7114 (2019).

[41] Annual publications are currently produced from the data received from more than 18,000 city, university and college, county, state, tribal, and federal law enforcement agencies that voluntarily participate in the UCR program. Specifically: The NIBRS; the SRS; the Law Enforcement Officers Killed and Assaulted Program; and the Hate Crime Statistics Program. Compilations are created for Cargo Theft, Human Trafficking, and topical studies, and new National Use-of-Force Data Collection. *Uniform Crime Reporting Program*, FED. BUREAU OF INVESTIGATION, https://perma.cc/2RRZ-337B; *Hate Crime Statistics*, FED. BUREAU OF INVESTIGATION, https://perma.cc/XYZ5-P4ST.

[42] UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18, at 2; *see also* 15 U.S.C. § 2220(a)(4) (2000).

[43] UNIFORM CRIME REPORTING HANDBOOK, *supra* note 18; Anti-Arson Act of 1982, 18 U.S.C. § 844(f)(3) (1982).

[44] *See Crime in the United States 2013: Rape*, FED. BUREAU OF INVESTIGATION, https://perma.cc/5T5V-5GGK; FED. BUREAU OF INVESTIGATION, FREQUENTLY ASKED QUESTIONS ABOUT THE CHANGE IN THE UCR DEFINITION OF RAPE (2014), https://perma.cc/Z29T-G237; *An Updated Definition of Rape*, U.S. DEP'T OF JUSTICE (Jan. 6, 2012), https://perma.cc/99CL-AQXN.

enforcement agencies to adjust to any changes or modifications.[45] As reflected in the years it takes to adopt even Congressionally mandated changes, the system does not easily adapt to changes in criminal behavior, emerging criminal trends, or the development of new crimes in the computer era, such as ransomware or sextortion. As noted by the National Academy of Sciences when evaluating the UCR program:

> The problem with the list of crimes developed by the assembled police chiefs in the late 1920s is not that it is uninformative—the original Part I crimes were chosen in large part for their salience to the general public, and they remain serious events of interest today. Rather, the issues are that the list of Part I crimes have so successfully "defined"—and limited—what is commonly meant by "crime in the United States" and that the lists of both Part I and Part II crimes have remained so relatively invariant over the years.[46]

B. The National Incident Based Reporting System

While the crime data collected through the UCR's SRS Program remains critically important, the data is limited and fails to capture the details and scope of criminal conduct in America. Recognizing this, the FBI is transitioning the SRS reporting system into a new reporting system called the National Incident Based Reporting System ("NIBRS"). This latest iteration of a national crime reporting system, NIBRS is designed to provide more comprehensive information about each criminal incident, such as the nature of the specific offense that occurred, the characteristics of the victims and offenders, and the type and value of the property. According to the FBI:

> NIBRS captures details on each single crime incident—as well as on separate offenses within the same incident—including information on victims, known offenders, relationships between victims and offenders, arrestees, and property involved in crimes. Unlike data reported through the UCR program's traditional Summary Reporting System (SRS)—an aggregate monthly tally of crimes—NIBRS goes much deeper because of its ability to provide circumstances and context for crimes…[47]

In contrast to the SRS program, which essentially provides a tally of the most serious crime that occurred in any incident, the NIBRS report includes every crime committed during the incident, details about the injuries that occurred, the weapons used, and the location of each

[45] *See, e.g.*, HUMAN TRAFFICKING IN THE UNIFORM CRIME REPORTING (UCR) PROGRAM, *supra* note 40 (data collected in the first few years following implementation is generally less reliable than after the category becomes more established).

[46] NAT'L ACAD. OF SCIENCES, ENG'G & MED., MODERNIZING CRIME STATISTICS: REPORT 1 – DEFINING AND CLASSIFYING CRIME 63 (Janet L. Lauritsen & Daniel L. Cork eds., 2016).

[47] *National Incident-Based Reporting System (NIBRS)*, FED. BUREAU OF INVESTIGATION, https://perma.cc/XYN7-LEEJ.

crime.[48] The NIBRS Program will also collect data on a more expansive list of crimes, at least 52 offenses, thereby greatly increasing the amount of information obtained from the traditional UCR reports. The data collected, therefore, is expected to present a better reflection of crimes occurring in the U.S. and will allow for greater research and analysis into the complexities of crime.[49]

President Obama's Task Force on 21st Century Policing encouraged participation in NIBRS, finding that greater acceptance of it "could also benefit policing practices and research endeavors."[50] It is anticipated that NIBRS data will further support the traditional purposes of police data collection programs in that it will allow law enforcement officers to focus on the type of resources they need to combat crime in their region, to allow law enforcement agencies with similar crime problems to work together more closely, and to allow law enforcement to be more accountable to the public for their crime-fighting efforts.[51]

The transition to NIBRS, however, has been extremely slow. The origins of NIBRS date back to the early 1980s when the DOJ formed a task force that generated a report entitled *The Blueprint for the Future of the Uniform Crime Reporting Program*, which eventually evolved into NIBRS.[52] As of 2017, the FBI reports that 42% of law enforcement agencies in the nation were reporting their crime data through NIBRS.[53] The full transition to the NIBRS Program is now expected to be in 2021, nearly 40 years after it was initially conceived.

Despite the slow transition, NIBRS has generated hope that it will modernize crime data collection systems.[54] However, even this updated crime counting system fails to emphasize the depth and gravity of cybercrime. Of the 52 NIBRS "Group A Offenses" (i.e., the most serious offenses), only one category, listed under fraud offenses, called "hacking/computer invasion," is designated for cybercrime. The remaining 51 categories focus on what may be considered more traditional street crimes that local law enforcement agencies are known to handle, such as arson,

[48] Nat'l Inst. of Justice, *Sources of Crime Data: Uniform Crime Reports and the National Incident-Based Reporting System*, U.S. DEP'T OF JUSTICE (2009), https://perma.cc/7XMX-7LB9.

[49] *Id.*

[50] OFF. OF CMTY. ORIENTED POLICING SERV., U.S. DEP'T. OF JUST., PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING: FINAL REPORT OF THE PRESIDENT'S TASK FORCE ON 21ST CENTURY POLICING 20 (2015), https://perma.cc/ERT3-6MMF.

[51] Ryan Sibley, *The Benefits of Criminal Justice Data: Beyond Policing*, SUNLIGHT FOUND. (May 1, 2015), https://perma.cc/KY2E-437N.

[52] NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 39 (citing EUGENE C. POGGIO ET AL., BUREAU OF JUSTICE STAT., BLUEPRINT FOR THE FUTURE OF THE UNIFORM CRIME REPORTING PROGRAM – FINAL REPORT OF THE UCR STUDY (1985)); Jeffrey Fisher, *NIBRS: The Future of U.S. Crime Data*, POLICE CHIEF MAGAZINE, Oct. 2017, at 48, https://perma.cc/U8YD-A9PT.

[53] The 2017 NIBRS report contains about 5.4 million incidents with over 6 million listed criminal offenses, with approximately 61% were property crimes, 23% were crimes against persons, and 16% were crimes against society. *2017 NIBRS Crime Data Released*, FED. BUREAU OF INVESTIGATION (Dec. 10, 2018), https://perma.cc/6LHV-XVDQ.

[54] FED. BUREAU OF INVESTIGATION, CRIMES AGAINST PERSONS, PROPERTY, AND SOCIETY (2018), https://perma.cc/7BXB-JHC9.

aggravated assault, burglary, vandalism, drug trafficking offenses, wire fraud, murder, human trafficking, shoplifting, theft, larceny, robbery, rape, stolen property, and weapons violations.[55]

Despite the continued focus on more traditional street crimes, the NIBRS system offers promise in the added crime details it captures. As noted in its 2019 User Manual:

> To combat the growing problem of computer crime (i.e., crimes directed at and perpetrated through the use of computers and related equipment), NIBRS provides the capability to indicate whether a computer was the object of the reported crime and to indicate whether the offenders used computer equipment to perpetrate a crime.[56]

The system also allows for coding when the crime takes place in cyberspace.[57] Further, the NIBRS system is upgraded periodically to add more specific categories, such as the January 1, 2019 expansion of the cargo theft category to include hacking or computer invasion as a means to accomplish the crime.[58]

Nevertheless, the data collection system remains deficient in that it fails to focus on cybercrime, fails to account for the full range of computer-generated crimes, and continues to focus on traditional street and property crimes that were historically captured under the UCR's SRS program. In conducting its independent evaluation of NIBRS, the National Academy of Sciences noted that although NIBRS captures more detailed information on many crimes, the system still does not fully account for a full range of internet-enabled crimes and that "NIBRS core development work and structuring took place in the late 1980s, and it is not clear that its design has kept pace with the times."[59]

The failure of crime tracking systems to keep pace with the times was illustrated when DOJ issued its 2018 Cyber Digital Task Force Report, identifying the most common cybercrimes: (1) Damage to computer systems (to include Distributed Denial of Service (DDoS) attacks, ransomware attacks, and destructive attacks); (2) Data theft (to include hacks aimed at stealing personal identifiable information and the theft of intellectual property); (3) Fraud/carding schemes; (4) Crimes threatening personal privacy (to include sextortion, non-consensual pornography (frequently called revenge pornography), cyber-enabled stalking and harassment, swatting, and doxxing); and (5) Crimes threatening critical infrastructure.[60] These cybercrimes are executed through the use of social engineering, phishing schemes, business e-mail compromise, the use of malware and botnets, and criminal infrastructure platforms.[61] Despite

[55] FED. BUREAU OF INVESTIGATION, 2019 NATIONAL INCIDENT-BASED REPORTING SYSTEM USER MANUAL 16-19 (2018), https://perma.cc/C2SS-METM; *2017 National Incident-Based Reporting System: Data Tables*, FED. BUREAU OF INVESTIGATION (2017), https://perma.cc/7V64-FKKE.

[56] NATIONAL INCIDENT-BASED REPORTING SYSTEM USER MANUAL, *supra* note 55, at 152.

[57] *Id.* at 86.

[58] *Id.* at 2, 70.

[59] NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 8.

[60] REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE, *supra* note 13, at 23-34.

[61] *Id.* at 35-37.

42% of police agencies reporting crime through NIBRS, none of the cybercrimes highlighted by DOJ were mentioned in the 2017 crime report, the most recent full-year crime report issued.[62] Similarly, these pervasive cybercrimes are not mentioned in the 2018 preliminary data report.[63]

C. National Crime Victimization Survey

While the UCR's SRS/NIBRS data is based on reported crime captured by police departments, the annual National Crime Victimization Survey ("NCVS") is an effort to capture information about crime victims and on the number of unreported crimes.[64] The survey includes approximately 240,000 annual interviews regarding the frequency, characteristics, and consequences of criminal victimization. For each incident, the survey collects information about the offender, the nature of the crime, the nature of any injury, the use of weapons, the economic consequences of the crime, whether the crime was reported to police, and the victim's experience with the justice system.[65]

> As a survey, the level of detail that can be gathered by the base NCVS is immense …The flexibility of the survey's content makes it possible to articulate very fine categories of crime, with different attributes such as weapon use or the value of property involved in an incident—at the expense of precision and volatility in estimates. Simultaneously, NCVS publications focus on coarser constructs such as all "violent crime," all "property crime," or all acts of serious violence between family members, because those broader categories (and changes over time within them) can be estimated more precisely.[66]

In 2005, the NCVS program conducted a survey focused on cybercrime. The survey found:

- 67% of responding businesses reported being the victim of at least one cybercrime;
- 86% of victimized businesses detected multiple cyber incidents; and
- 43% of victimized businesses detected 10 or more incidents during the year.[67]

Despite this now fourteen-year-old survey demonstrating the significant impact cybercrime has on businesses, no subsequent survey has focused on collecting cybercrime data.

D. Internet Crime Complaint Center

[62] *See 2017 National Incident-Based Reporting System: Data Tables*, *supra* note 55.

[63] *2018 Crime in the United States: Table 1*, FED. BUREAU OF INVESTIGATION, https://perma.cc/6BYH-7XVF.

[64] The NCVS objectives: (1) developing detailed information about the victims and consequences of crime, (2) estimating the number and types of unreported crimes, (3) providing uniform measures of selected types of crimes, and (4) permitting comparisons over time and population types (e.g., urban, suburban, and rural). Congressional Research Service, *How Crime in the United States is Measured*, January 3, 2008.

[65] Erika Harrell et al., *Data Collection: National Crime Victimization Survey (NCVS)*, BUREAU OF JUSTICE STAT. (2018), https://perma.cc/4YWH-GZ5D.

[66] NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 51, 54.

[67] Harrell et al., *supra* note 65.

Unlike traditional crime data collection programs, whereby law enforcement agencies report their crime statistics to the federal government, the FBI's cybercrime data tracking program is a self-reporting online portal called the Internet Crime Complaint Center (the "IC3"). Established in 2000, the IC3 is the system through which the FBI receives internet-related crime complaints directly from victims. Through this voluntary online reporting system, cybercrime victims can self-report their incident, and, in turn, the FBI can analyze the reported incidents and their relationship to other cybercrimes.

According to the FBI, the IC3 has four core functions: (1) collecting Internet crime reports; (2) analyzing data collected to discover emerging threats or trends; (3) alerting the public of ongoing scams for awareness purposes; and (4) aggregating similar complaints to refer cases to law enforcement for potential investigation.[68]

Since its inception, the FBI has received 4,415,870 complaints through the online IC3 portal.[69] Over the last five years, the IC3 has received an average of almost 300,000 complaints per year. In 2018, the IC3 platform received a total of 351,936 complaints with losses exceeding $2.7 billion, almost double the amount of losses reported in 2017.

The 2018 Annual Internet Crime Report summarizes the most recent IC3 complaints filed and demonstrates that serious cybercrimes are impacting large numbers of victims. Specifically, the IC3 received over 20,000 complaints regarding business email compromise schemes with corresponding losses exceeding $1.3 billion; 51,146 extortion complaints (defined as denial of service, sextortion, government impersonation, and data breaches) with corresponding losses of over $83 million (representing a 242% increase from the 2017 report); and 14,408 tech support fraud complaints with corresponding losses of nearly $39 million (representing a 161% increase from the 2017 report).[70] These serious and prevalent cybercrimes, described in the 2018 IC3 Report, are not reflected in the crime reports submitted by local law enforcement in the UCR's SRS/NIBRS database.[71]

The FBI promotes and encourages the use of the IC3 portal through its website and public service announcements.[72] While the nature and scope of the cybercrimes reported to the IC3 are significant, IC3 reporting remains relatively low compared to the prevalence of cybercrime. The number of IC3 reports increased only about 50,000 in the one-year period between 2017 and 2018. In 2016, 16 years after its inception, the then-head of the IC3, Donna Gregory, admitted

[68] FED. BUREAU OF INVESTIGATION, 2017 INTERNET CRIME REPORT 6 (2018).

[69] FED. BUREAU OF INVESTIGATION, 2018 INTERNET CRIME REPORT 5 (2018), https://perma.cc/K8RF-XTFM.

[70] *Id.*

[71] *See 2017 National Incident-Based Reporting System: Data Tables*, *supra* note 55 (showing that some of the crimes may be categorized as a fraud committed by using a computer, but there is no distinction made as to whether that fraud was committed as a business email compromise scheme, an impersonation scheme, tech support fraud, or hacking scheme).

[72] Fed. Bureau of Investigation, *Reporting Cyber Crime is as Easy as IC3*, YOUTUBE (May 7, 2018), https://perma.cc/XG4M-WY5W (involving *Criminal Minds* actress Kirsten Vangsness, who plays "Penelope Garcia," describing the IC3 cybercrime fighting mission as "Fighting back is as easy as IC3!").

that the center was capturing only about 10 to 12% of all estimated cybercrime victims in the U.S.[73]

E. Private Cybercrime Reporting and Analysis

While formal and consistent law enforcement-based cybercrime reporting systems either do not exist or are deficient, many private, non-profit, and academic organizations engage in efforts to capture the volume and scope of cybercrime. For example, Verizon publishes an annual Data Breach Investigations Report. The 2019 report found that ransomware constituted nearly 24% of malware attacks, outsiders committed 69% of attacks on businesses, public sector entities represented 16% of breach victims, and the health care industry represented 15% of breach victims.[74] In its Ninth Annual Cost of Cybercrime Study, Accenture attempted "to quantify the annual economic cost of cyberattacks by analyzing trends in malicious activities over time"[75] and included information from 11 countries across 16 industries. This study determined that the average number of security breaches an organization experiences increased from 130 in 2017 to 145 in 2018 (an 11% increase), and the annual average cost of cybercrime increased from an average of $11.7 million in 2017 to 13 million in 2018 (with cybercrime costs increasing 72% over the previous 5 years).[76] McAfee's Economic Impact of Cyber Crime Report found that ransomware is the fastest-growing cybercrime tool and that the theft of intellectual property accounts for at least a quarter of cybercrime.[77] CISCO's recent annual report describes the cyberattack landscape, the varieties of malware including self-propagating malware, and the challenges presented by the Internet of Things (IoT).[78]

While the corporate reports and surveys provide compelling information about the state of cybersecurity and cybercrime, the data collection points and the consistency of each reporting mechanism are not verifiable. Frequently, the reports highlight the work conducted by the individual business publishing the report and reflect the limited scope of the problem presented to them by their clients. Nevertheless, in the absence of a national measurement, these reports are useful in providing important information.[79]

Other studies, primarily generated in the non-profit and academic arena, focus on specific crimes. For example, in March 2016, the Brookings Institute issued the first in-depth study of the modern Internet crime of sextortion. Sextortion, in its simplest form, is "old-fashioned extortion or

[73] Al Baker, *An Iceberg of Unseen Crimes: Many Cyber Offenses Go Unreported*, N.Y. TIMES (Feb. 5, 2018), https://perma.cc/TX8G-EM9R.

[74] VERIZON, 2019 DATA BREACH INVESTIGATIONS REPORT 5, 11 (2019).

[75] KELLY BISSELL ET AL., ACCENTURE, THE COST OF CYBERCRIME: NINTH ANNUAL COST OF CYBERCRIME STUDY 3 (2019), https://perma.cc/TTW4-XD2D.

[76] *Id.* at 11.

[77] *The Economic Impact of Cybercrime – No Slowing Down*, MCAFEE (Feb. 2018), https://perma.cc/5PUN-CGK3.

[78] *See* CISCO, ANNUAL CYBERSECURITY REPORT 2018 (2018), https://perma.cc/UA96-SZ4C.

[79] Corporate data notification laws now exist, requiring notifications to victims and/or state Attorneys General where personal information was compromised. *See, e.g.*, CAL. CIV. CODE §§ 1798.29(a), (e), (f); CAL. DEP'T OF JUSTICE, OFF. OF THE ATTORNEY GEN., DATA SECURITY BREACH REPORTING, https://perma.cc/5MA5-NWBT.

blackmail, carried out over a computer network, involving some threat—generally but not always a threat to release sexually-explicit images of the victim—if the victim does not engage in some form of further sexual activity."[80] The Brookings study reviewed court cases and public records in which it identified 78 perpetrators of this offense who impacted more than 3,000 victims. Three years later, the Lawfare Blog published a March 2019 update to the study, identifying 124 additional perpetrators of this offense and thousands of additional victims.[81] According to the 2016 Brookings Institute report, approximately 85% of all sextortion cases involve minor victims and the majority of adult victims are female.[82]

Another sextortion study revealed that one out of every four victims were twelve years old or younger when sextorted, and two out of every three victims were girls under age sixteen.[83] The studies established that the virtual nature of sextortion means that children who are well-protected in the physical world can be exposed to a heightened level of vulnerability in their homes, making this a crime of particular concern when it comes to the safety and protection of children.[84] Experts also recognized an alarming uptick in the number of sextortion victims who attempted suicide after being sextorted because they are unable to cope with the pressure, abuse, and humiliation that accompanies the crime.[85] According to a study conducted by Thorn, one in three victims never tells anyone about the abuse, 53% of victims surveyed disclosed the sextortion to a friend, 26% reported it to a media platform, and only 17% reported the crime to law enforcement.[86] Demonstrating the brutality of the crime and law enforcement's frequent lack of understanding and failure to address it, one University of Utah student, Lauren McClusky, reported her sextortion to the University's campus police department but they failed to address the issue.[87] The man who extorted her eventually murdered McCluskey.

The FBI does not currently track sextortion. In response to the findings uncovered in the Brookings study, then-Senator Barbara Boxer requested that the DOJ provide information regarding its specific tracking of sextortion. The DOJ responded that it is "committed to sustaining and improving its vigorous enforcement efforts against sextortion crimes" but that tracking such criminal conduct would be difficult. The DOJ response also noted that it would be difficult to track cyber-stalking and cyber-harassment because the manner in which crimes are counted is not

[80] Benjamin Wittes, *Sextortion*, BROOKINGS 1 (May 2016), https://perma.cc/6M32-95B2; EXEC. OFF. OF U.S. ATTORNEYS, U.S. DEP'T OF JUSTICE, CYBER MISBEHAVIOR BULL. NO. 64-3 (May 2016) at 6, https://perma.cc/PM8A-6RNZ.

[81] Katherine Kelley, *New Data on Sextortion: 124 Additional Public Cases*, LAWFARE BLOG (Mar. 19, 2019, 10:24 AM), https://perma.cc/3RAV-Z9B2.

[82] *Id.*; *cf.* EUROPOL, ONLINE SEXUAL COERCION & EXTORTION AS A FORM OF CRIME AFFECTING CHILDREN 17-18 (May 2017), https://perma.cc/58MX-79PT.

[83] THORN, SEXTORTION IS AN EMERGING FORM OF ONLINE ABUSE, https://perma.cc/3ADA-ZTQ3.

[84] CYBER MISBEHAVIOR, *supra* note 80, at 44 ("it's literally happening in the palms of children's hands, including the places they should feel most safe—their homes.").

[85] *See* Libby Brooks, *Suicide Prevention Plan Needed for Child Victim of 'Sextortion' – Expert*, THE GUARDIAN (Nov. 29, 2017, 1:25 PM), https://perma.cc/S9U6-4H3K.

[86] THORN, *supra* note 83.

[87] Jill McCluskey, *Jill McCluskey: The University of Utah Didn't Take Our Daughter's Concerns Seriously, and It's Not Holding Anyone Accountable*, SALT LAKE TRIBUNE (Jan. 10, 2019), https://perma.cc/9PXL-DZCC.

internet-based.[88] The 2016 DOJ letter illustrates the fact that cybercrimes are not counted, and the depth of the cybercrime problem is unknown.

II. THE IMPORTANCE OF CYBERCRIME DATA COLLECTION

The reports produced by government and non-governmental organizations alike demonstrate the significance, prevalence, and pervasiveness of cybercrime, suggesting that cybercrime more than satisfies the IACP's original criteria for selecting the crimes subject to data collection. While there are many non-governmental organizations that produce cybercrime data, consistent nationally generated cybercrime data is critically important to advancing our understanding of the crime problem and to ensuring the proper allocation of resources to address it.

A. The Impact of Robust Crime Data Collection

Policy makers, law enforcement officials, students, researchers, media outlets, and members of the public use nationally collected crime data to respond to and develop policies in response to crime trends.[89] As FBI Director Chris Wray stated with the release of the 2017 Crime Report that summarized the annual collection of the UCR's SRS/NIBRS data:

> With richer data, we can more easily identify crime patterns and trends, understand how and why certain crimes are happening, and find the best way to prevent them. Information like this helps leaders decide how to allocate resources and helps counter misconceptions about the scope and nature of crime in the United States.[90]

Congress relies on the development of accurate crime data. First, as noted previously, Congress periodically mandates the collection of specific data when it is concerned about growing crime trends. For example, the Hate Crimes Statistics Act of 1990, requiring the collection of data on crimes involving prejudice based on race, ethnicity, religion, or sexual orientation, developed over growing concern about the increasing number of hate crimes and the unreliability of data collected by third parties.[91] Congress also uses FBI-collected crime data to develop national policy and respond to crime trends. For example, in the 103rd Congress, the Community Oriented Policing Services (COPS) program was created to provide law enforcement agencies with grants to hire, rehire, and redeploy law enforcement officers to

[88] Letter from Peter Kadzik, Assistant Attorney Gen. for the Office of Legislative Affairs, U.S. Dep't of Justice, to the Honorable Barbara Boxer, U.S. Senate (July 14, 2016), https://perma.cc/4GYN-RV54.

[89] NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 85.

[90] CHRIS WRAY, FED. BUREAU OF INVESTIGATION, UNIF. CRIME REPORTING PROGRAM: MESSAGE FROM THE DIRECTOR (2018), https://perma.cc/E9K3-YSMF.

[91] NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 90.

engage in community policing.[92] Congress specifically cited to both the UCR's SRS program and NCVS crime statistics to explain the need for more community policing officers.[93] Congress also uses UCR crime data to develop formula allocations for certain grant programs such as the Edward Byrne Memorial Justice Assistance Grant (JAG) program.[94]

Academic analysis of national crime data has also been critical in understanding the nature of crime, in offering law enforcement different perspectives about crime, and in enhancing understanding about community safety. For example, NYU's Brennan Center conducted a detailed evaluation of crime in the United States, for the 25-year period of 1990 to 2016, using the UCR's SRS/NIBRS data and determined:

- The national crime rate peaked in 1991 at 5,856 crimes per 100,000 people, and has generally been declining ever since;
- Crime largely declined over the course of 25 years to about half of what it once was (declining from 1991's rate of 5,856 crimes per 100,000 to 2016's rate of 2,857); and
- While crime peaked nationally in 1991, in the 30 largest cities, the overall crime rate was higher in 1990, at 10,244 crimes per 100,000 people. Since then, the crime rate in these cities has declined by 63.9%, reaching 3,702 crimes per 100,000 people in 2016.[95]

Law enforcement also uses the crime data that it collects. One of the better-known uses of consistently collected and verifiable crime data is the CompStat system. CompStat's often-stated goals are: (1) timely and accurate information or intelligence; (2) rapid deployment of resources; (3) effective tactics; and (4) relentless follow-up.[96] CompStat introduced aggressive data-utilization that helped to professionalize policing, provide a management structure to police work, and was significantly responsible for bringing policing into the information age. American criminologist Lawrence W. Sherman commented that: "Since 1975, nothing has done more than the CompStat idea to increase the availability of evidence for tracking police performance at micro levels of activity."[97]

While CompStat can assume many variations, at its core police departments collect and analyze crime data from their communities and use it for strategic decision-making and operational or tactical decisions.[98] Departments also use the data to discuss the nature of

[92] Violent Crime Control and Law Enforcement Act of 1994, Pub. L. 103-322, 108 Stat. 1796, 1808-15.

[93] NATHAN JAMES, CONG. RESEARCH SERV., RL34309, HOW CRIME IN THE UNITED STATES IS MEASURED 1 (2008), https://perma.cc/28UV-E9Z8.

[94] *See* NATHAN JAMES, CONG. RESEARCH SERV., RS22416, EDWARD BYRNE MEMORIAL JUSTICE ASSISTANCE GRANT PROGRAM: LEGISLATIVE AND FUNDING HISTORY (2013).

[95] MATTHEW FRIEDMAN, AMES C. GRAWERT & JAMES CULLEN, BRENNAN CTR. FOR JUSTICE , CRIME TRENDS: 1990-2016, 1, 3, 9 (2017), https://perma.cc/X4VQ-LTKK.

[96] BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE, COMPSTAT: ITS ORIGINS, EVOLUTION, AND FUTURE IN LAW ENFORCEMENT AGENCIES 2 (2013), https://perma.cc/86B4-22A6.

[97] Lawrence W. Sherman, *The Rise of Evidence Based Policing: Targeting, Testing, and Tracking*, 42 CRIME & JUST. 1, 37 (2013); DR. OLIVER ROEDER, LAUREN-BROOKE EISEN & JULIA BOWLING, BRENNAN CTR. FOR JUSTICE, WHAT CAUSED THE CRIME DECLINE? 66 (2015), https://perma.cc/Z5TU-APSQ.

[98] *See, e.g.*, Malcolm K. Sparrow, *New Perspectives in Policing: Measuring Performance in a Modern Police Organization*, NAT'L INST. OF JUSTICE 25-29 (Mar. 2015), https://perma.cc/QQA7-CTQK (Some Compstat systems have been expanded to include measurements outside traditional crime statistics, to include things like response

emerging and continuing crime problems in different areas of their jurisdiction, to track problem areas and the efforts they use to address crime and to provide information to the public about their community. It also compels police departments to "own" their crime problems.[99]

In a study focusing on identifying the reasons for the decline in the national crime rate, the Brennan Center concluded that CompStat-type programs had an impact.[100] Specifically, the study analyzed the UCR's SRS/NIBRS national crime data to conduct the first national city-level empirical analysis of the effect of CompStat on reducing crime, and found that the use of "CompStat-style programs is responsible for a 5 to 15% decrease in crime in cities where the programs were implemented."[101] The report found that the use of CompStat is associated with a 12% decrease in violent crime, an 11% decrease in property crime, and a 13% decrease in homicides. The report emphasized, "the result for property crime is strongly statistically significant."[102]

Due to its success in reducing crime and, consequently, its widespread adoption by police departments across the nation, CompStat is considered a critical tool to successful policing and for police management.[103] William J. Bratton, frequently credited with the development of and widespread implementation of CompStat, refers to the crime analysis system as a "department's bottom line, the best indicator of how the police are doing, precinct by precinct and citywide."[104] In describing its success in addressing crime and in highlighting the impact of crime data collection, Bratton explains: "After all, you can't fix what you can't measure. You can expect what you inspect."[105]

The CompStat analysis process focuses almost exclusively on reported UCR Part I crimes (murder, robbery, rape, aggravated assault, burglary, theft, vehicle theft, and arson).[106] As reflected in their joint study of the CompStat system, the Bureau of Justice Assistance and the Police Executive Research Forum found that: "The purpose of the [CompStat] inspection is to uncover performance inhibitors, with a focus on helping reduce Part I crimes."[107] The principal data source used in the analysis is "reported crime," and the objective sought by this process is to

times, measures of enforcement productivity, and community satisfaction surveys. Further, it is important to note there has been some criticism of CompStat and data driven policing, particularly in recent years, arguing that the data collected is not the best metric for measuring the performance of modern police departments.); JAMES J. WILLIS ET AL., POLICE FOUNDATION, COMPSTAT IN PRACTICE: AN IN-DEPTH ANALYSIS OF THREE CITIES 1-4, 48, 71 (2015), https://perma.cc/429Y-NSND.

[99] NAT'L ACAD. OF SCIENCES, ENG'G & MED., *supra* note 46, at 87.

[100] Oliver Roeder et al., *What Caused the Crime Decline?* BRENNAN CTR. FOR JUSTICE 75 (2015), https://perma.cc/SR6Y-HW9Y.

[101] *Id.*

[102] *Id.*

[103] BUREAU OF JUSTICE ASSISTANCE, *supra* note 96, at 20, 26-29.

[104] William J. Bratton, *Great Expectations: How Higher Expectations for Police Departments Can Lead to a Decrease in Crime*, *in* NAT'L INST. OF JUSTICE, MEASURING WHAT MATTERS 11, 15 (Robert H. Langworthy ed., 1999), https://perma.cc/7MLD-T6B8.

[105] WILLIAM J. BRATTON & ZACHARY TUMIN, COLLABORATE OR PERISH: REACHING ACROSS BOUNDARIES IN A CONNECTED WORLD 16 (Random House, 2012).

[106] WILLIS ET AL., *supra* note 98, at 12, 14, 49, 51.

[107] BUREAU OF JUSTICE ASSISTANCE, *supra* note 96, at 11.

lower specific Part I crime numbers.[108] The UCR's data collection system combined with CompStat's analysis process focusing on Part I crimes is now the general model law enforcement uses to measure its success and effectiveness in enhancing public safety.[109] Simply put, the data collected drives policing models.

The impact of the CompStat system's almost singular focus on the UCR's Part I crime, and its general failure to address non-Part I crime, was described by multiple police departments in a National Institute of Justice CompStat study, where officers acknowledged that:

- "If something is not shown at Compstat, no one cares about it . . . it means that you are not paying attention to it . . . you are not accountable for it;"
- "We only look at the Part I numbers. We are missing part of the big picture. We do not look at simple assaults or livability issues, and we need to move toward this;" and
- Like police radar systems, with Compstat "[i]f something is not on the radar, it is invisible."[110]

The report concluded that it was also likely that supervisory officers would not be held accountable for non-Part I crimes that are omitted from the CompStat process.[111] Thus, while CompStat has been successful in contributing to crime reduction and focusing departments on unified policing objectives, criminal activity that is omitted from the definition of Part I crime, such as cybercrime, is unlikely to capture the universal attention of local law enforcement. Instead, law enforcement's attention remains steadfastly focused on the 1929 crime categories that the IACP determined were, at the time, the most serious, frequent, and pervasive.[112]

The robust collection of crime data offers many benefits to enhancing public safety. It allows law enforcement to more accurately define crime problems in their communities, inform the public about crime trends, obtain additional funding and resources to address their specific problems, and make operational decisions to address crime. Crime data collection programs, in combination with CompStat methodologies, successfully creates a system whereby law enforcement takes responsibility for and is held accountable for the crimes they are measuring, while simultaneously creating a robust national system of data-focused policing. The emergence of CompStat as a tool that utilizes and analyzes the collected crime data has also contributed to the professionalization of policing. Congress and other policy makers also benefit from the crime data collection programs to assist them in establishing crime-fighting priorities and goals.

[108] Sparrow, *supra* note 98, at 2-4.

[109] *See, e.g.*, *2018 January – June Preliminary Semiannual Uniform Crime Report: Table 1*, FED. BUREAU OF INVESTIGATION (2018), https://perma.cc/KYF3-BWDK; *CompStat: Week 34*, CHI. POLICE DEP'T (2019), https://perma.cc/HH3A-7366; *CompStat: August 19-25*, POLICE DEP'T CITY OF N.Y. (2019), https://perma.cc/FTX5-9AGN; *CompStat: Citywide Profile*, L.A. POLICE DEP'T (2019), https://perma.cc/HT2Z-YLYK.

[110] WILLIS ET AL., *supra* note 98, at 53.

[111] *Id.*

[112] *Id.* (It remains to be seen how the migration to the NIBRS system, and its more expansive view of crime it seeks to capture, might impact the evolution of the CompStat crime analysis process or whether CompStat will continue to be focused almost exclusively on the historic definition of Part I crime.).

Collectively, all of these advancements in public safety are due, in part, to robust crime data collection.

B. The Impact of Insufficient Cybercrime Data

In contrast to robust crime data collection, the failure to count cybercrime means that we are failing to accurately measure all criminal conduct, failing to adequately warn the public about the various dangers in the computerized world, and failing to modernize policing. As a result, law enforcement agencies, particularly those who rely on traditional CompStat methods to monitor performance and set goals, are not analyzing the nature or seriousness of cybercrime in their jurisdictions, are not developing strategies to address it, and are not holding themselves accountable for its growth.

The inadequacy of current data collection systems can be illustrated by analyzing the limited cybercrime data that is available and comparing it to the robust general crime data collected. For example, the FBI's 2017 crime report lists 4,761 bank robberies (with an average loss of $3,483), and 8,402 gas station robberies (with an average loss of $1,087). These are important crimes worthy of data collection and police investigation. Yet, by comparison, the FBI's IC3 Annual Report, which captures only about 12% of cybercrimes, suggests that there are many more significant cybercrimes that should be counted, including: 20,373 business email compromise crimes with $1.2 billion in losses, 100 payroll diversion schemes with $100 million in losses, 14,408 tech support fraud cases with $39 million in losses, and 51,146 extortion complaints with $83 million in losses. Modern crime can no longer be measured by the limited 1929 standards.

As the Police Executive Research Forum ("PERF") stated in its 2018 report on crime:

> The United States is experiencing a transformation in how criminals are using technology to invent new types of crime[] and are creating new methods for committing traditional crimes. These developments are fundamental in nature…. Data collection is more than just an academic undertaking to support research. The fact that we don't know the true nature of crime in our country should be a concern. Data helps to drive policy, resources, and operations.[113]

Former Philadelphia Police Department Commissioner Nola Joyce commented that: "What we know about [crime] is above the surface. But in terms of value, and in terms of harm, a lot of that crime is below the surface…." [114] "[W]ithout timely, accurate data on crime, criminal justice leaders cannot see and respond coherently to national trends or make informed policy and spending decisions or tailor deployment strategies to best battle them."[115]

[113] POLICE EXEC. RESEARCH FORUM, NEW NATIONAL COMMITMENT REQUIRED: THE CHANGING NATURE OF CRIME AND CRIMINAL INVESTIGATIONS 4, 7 (2018), https://perma.cc/82WD-54GN.

[114] Baker, *supra* note 73.

[115] *Id.*

This sentiment was also expressed by the 21st Century Policing Task Force, which noted that the development of mature crime analysis and CompStat systems allows law enforcement to effectively develop policy and deploy resources for crime prevention, but that the lack of data collection and real-time analysis is "especially critical in light of the threats from terrorism and cybercrime."[116]

Furthermore, while national data in traditional crime categories, such as homicides, aggravated assaults, and other criminal conduct have steadily decreased for at least the last 25 years,[117] these numbers do not reflect the growing cybercrime trends and that many crimes may have transitioned into cyberspace where crimes are not being officially counted. Given the lack of comprehensive data collection systems and the severe underreporting of computer-enabled crimes, there is currently no way to accurately measure the number of these offenses or their monetary impact on victims and the national economy. This lack of data makes it difficult for law enforcement agencies to formulate strategies and devote the resources needed to combat the problem, especially since police departments are now data-driven enterprises. Further, the missing cybercrime information also allows public officials to promote success in lowering crime rates,[118] when in fact modern crime may just be hidden in the anonymity of the cyber world:

> "Without a more comprehensive set of crime statistics, we cannot know whether the large-scale declines in the 1990s in traditional and well-measured violent and property crimes reflect broader declines in crime, or whether these recorded changes were offset by notable increases in alternative and newly-emerging forms of crime that are not captured in current data systems."[119]

Failure to collect data, and to instead rely on incomplete self-reporting cybercrime systems and studies, allows law enforcement and government officials to effectively abdicate responsibility for this growing crime trend. It also discourages victims from reporting crimes due to the concern that nothing will be done or that law enforcement simply does not have the means to address cybercrime, encouraging hack-backs and other private sector responses. Effective data collection requires law enforcement to own the cybercrime problem, much like they own homicides, robberies, and other crimes that happen within their jurisdictions.

C. Modernizing Cybercrime Data Collection

[116] OFF. OF CMTY. ORIENTED POLICING SERV, *supra* note 50, at 33.

[117] FREIDMAN ET AL., *supra* note 95; John Gramlich, *5 Facts About Crime in the U.S.*, PEW RESEARCH CTR. (Oct. 17, 2019), https://perma.cc/LZS8-HRQZ.

[118] *Morning Joe: Interview with New York City Mayor Bill de Blasio* (MSNBC television broadcast Feb. 17, 2018), https://perma.cc/8UV6-CCC8; *Mayor: Crime Down in Every Major Category in LA Last Year*, CBS L.A. (Jan. 28, 2019, 5:58 PM), https://perma.cc/S5E6-YRG3.

[119] POLICE EXEC. RESEARCH FORUM, *supra* note 113, at 10.

Given the importance of data to understanding modern crime problems, obtaining resources to address crime, gaining the attention of local law enforcement, and developing strategies to lower crime rates, it is critical that cybercrime data be counted and collected in a consistent and robust manner.

Changing or even mandating additional crime data collection requirements for local law enforcement is challenging. There are approximately 18,000 federal, state, county and local law enforcement agencies in the United States,[120] and each has limited resources available to dedicate to enhanced data collection. Historically, congressional crime data mandates take years to adopt, as evidenced by the years-long efforts to add hate crimes, cargo theft, and human trafficking to national crime databases. The multi-decade effort to migrate to a more sophisticated collection of crime data under the NIBRS system, from the now well-established but basic SRS system, highlights the challenges of adopting new methodologies. This is true even though there is general agreement that more data would assist in developing better policing policies, allow for the more effective allocation of resources, and ensure more effective police deployment and operations.

The extended length of time required to adapt to new data collection systems, however, is not a new phenomenon. For many years following the 1929 adoption of the UCR, there was insufficient data to estimate nationwide crime. In fact, from approximately 1930 to 1957, the FBI could only publish crime data in tables according to the size of reporting jurisdictions. The FBI did not publish aggregated nationwide crime data until 1958, when it was determined that sufficient data was being collected and reported that represented the nation as a whole.[121]

The time needed to ensure accurate cybercrime counts should not, therefore, impede the necessary effort. While NIBRS may not be perfect, the decades-long effort to develop a more sophisticated crime data collection process holds great potential. It does, however, need to be more robust and develop a strong focus on cybercrime. Congress should consider mandating the collection of cybercrime data, as it previously required with hate crimes, cargo theft, and human trafficking. The FBI along with its CJIS Advisory Policy Board, [122] which includes representatives from the IACP and other law enforcement organizations, should take a renewed focus on the cybercrime collection process. This process should include the expansion of the NIBRS categories to emphasize and include all forms of cybercrime and ensure that the NIBRS user manual – which provides direction and examples on how to categorize crime – focuses on cybercrime and provides specific instructions on the reporting of cybercrime (to include ransomware, cyber-stalking, sextortion, and other prevalent forms of cybercrime).[123] Grants and other funding mechanisms, which are frequently available to encourage local crime data

[120] BUREAU OF JUSTICE STAT., U.S. DEP'T OF JUSTICE, NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 1 (2016), https://perma.cc/6WBH-QEEU.

[121] MALTZ, *supra* note 17, at 4.

[122] *The CJIS Advisory Process*, *supra* note 31.

[123] *See* NATIONAL INCIDENT-BASED REPORTING SYSTEM USER MANUAL, *supra* note 55 (which does not include instructions for ransomware, cyber-stalking, sextortion, and other prevalent forms of cybercrime).

collection efforts, should be available[124] to ensure that police departments, especially the smaller departments across the nation, are capable of and encouraged to report cybercrime. Further, annual NIBRS reports highlighting cybercrime trends should be issued in conjunction with the FBI's annual IC3 report, in an effort to provide a comprehensive overview of cybercrime in the nation and encourage reporting within the NIBRS system.

Accurately counting cybercrime will be a challenging national effort. Yet, the need to have access to this data has never been greater, and the consequences have never been as dramatic. As the Council of Economic Advisors noted in its 2018 report: "the field of cybersecurity is plagued by insufficient data… Cyber protection could be greatly improved if data on past breaches and cyberattacks were more readily shared…"[125]

CONCLUSION

Without breaking or entering, cybercriminals are stealing our property. Without touching or assaulting, cyber-predators are committing severe personal violations. Without physically touching our valuables, cyber-thieves are stealing our intellectual and personal property. To ignore and not count these crimes is to ignore the very nature of 21st century living.

Absent significant efforts to measure cybercrime, we will never know the true nature of crime in our country and we will never know the full count. Fundamental to correcting any problem is identifying it. With 90% of American adults now using the Internet,[126] the volume of cybercrime is likely to continue to increase making data collection imperative to effectively managing this problem. It is past time that we know the score.

[124] *See, e.g.*, Press release, Bureau of Justice Stat., FBI and Bureau of Justice Statistics Award $24.2 Million to Law Enforcement Agencies to Support National Crime-Reporting Infrastructure (Sept. 27, 2016), https://perma.cc/8NZE-YPT4.

[125] COUNCIL OF ECON. ADVISORS, *supra* note 12, at 30.

[126] Monica Anderson et al., *10% of Americans Don't Use the Internet. Who are they?*, PEW RESEARCH CTR. (Apr. 22, 2019), https://perma.cc/8VHH-L4GG.