VOLUME19, ISSUE 3, PAGES 16–32 (2018)

Criminology, Criminal Justice, Law & Society

CRIMINOLOGY, CRIMINAL JUSTICE, LAW & SOCIETY

E-ISSN 2332-886X
Available online at
https://scholasticahq.com/criminology-criminal-justice-law-society/

White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?

Brian K. Payne

Old Dominion University

ABSTRACT AND ARTICLE INFORMATION

The study of white-collar crime has evolved over the past eight decades. So too has the nature of white-collar crime. Varieties of white-collar crime have changed as the types of occupations evolved. One change in the occupational arena that has likely impacted white-collar crime involves technological changes. In particular, with the advent of the computer, new opportunities for crime have developed within the workplace and outside of it. Few studies, however, have explored cybercrime within a white-collar crime framework. To address this void in the literature, in this study, a sample of 109 cases investigated by the U.S. Department of Justice are reviewed in order to determine how these cybercrimes can be characterized as white-collar crimes.

Article History:

Received January 16, 2018
Received in revised form June 21, 2018
Accepted June 25, 2018

Keywords:

cybercrime, white collar crime

In 1939, Edwin Sutherland introduced the concept of white-collar crime in his presidential address to the American Sociological Association, an academic speech receiving unprecedented media coverage and calling attention to crimes in various areas including the medical profession, the political arena, the securities industry, and the banking system, to a name a few (American Sociological Association, n.d.; Sutherland, 1940). A decade later he wrote about the concept in his seminal work *White-Collar Crime*, where he defined the behavior as "crime committed by a person of respectability and high social status in the

Corresponding author: Brian K. Payne, Ph.D. Department of Sociology and Criminal Justice, Old Dominion University, 1 Old Dominion University, Norfolk, Virginia, 23529, USA.
Email: bpayne@odu.edu
This research is supported in part by NSF under grant DGE-1723635

course of his occupation" (Sutherland, 1949, p. 9). Here again, Sutherland discussed an assortment of crimes committed by businesses and business representatives.

Of course, Sutherland did not talk about cybercrime. After all, because the technological revolution had not yet occurred, the term cybercrime had not yet been legally or socially constructed. It was not until at least two decades after Sutherland published his *White-Collar Crime* tome when it was recognized how technology was beginning to shape new types of crime. John Draper, also known as Captain Crunch because he was able to use a whistle that came from a cereal box to hack into phone lines in the early seventies, has been identified as one of the first individuals to commit cybercrime (James, 2009). By the end of the seventies, states had begun to develop computer crime statutes to guard against a seemingly new type of offense. By the turn of the century, concern about cybercrime was beginning to escalate.

By all accounts, cybercrime has increased dramatically. Research on the topic has also increased, but few researchers have explored cybercrime within the workplace. Failing to consider the overlap between cybercrime and white-collar crime potentially limits our current understanding about both types of crimes. Indeed, in most businesses, computers are a routine part of the workplace. Consequently, opportunities to use those computers (and computer technology) to perpetrate white-collar offenses have evolved. Maintaining current awareness about white-collar crime requires at least some attention to the role of cyber technology in relation to white-collar offending. Our empirical understanding about cybercrimes occurring in the workplace has not, however, evolved.

To fill this void in the literature, in this study a sample of "white-collar cybercrimes" investigated by the U.S. Department of Justice is examined with an aim towards identifying the overlap between white-collar crime and cybercrime. Identifying the similarities and differences between the two offense categories has implications for policy, theory, and future research. Regarding policy, identifying patterns surrounding white-collar cybercrime will shed some light on appropriate response strategies for these offenses. Such understanding is needed in order to determine whether response strategies should be guided by white-collar crime response strategies, cybercrime response strategies, or another set of response strategies.

In terms of theory, researchers have examined how various criminal behaviors are socially and legally constructed. Determining whether there is overlap between white-collar crime and cybercrime will help to identify whether the criminal constructs evolved in similar ways. In addition, it has been argued that deterrence theories (and deterrence strategies) are not easily applicable to white-collar criminals (Henning, 2015). If there is overlap between white-collar crime and cybercrime, one might question how deterrence theory applies in "white-collar cybercrimes."

In terms of research implications, understanding the basic dynamics of white-collar cybercrimes will provide a foundation from which others can further explore this specific type of white-collar crime. Through examining specific white-collar crime offense types, researchers have generated a great deal of understanding about those offenses. Our current understanding of those offense types (e.g., Medicaid fraud, academic fraud, environmental crime, sales fraud) can be traced to early studies focused on the basic dynamics of those crimes (Clinard, Quinney, & Wildeman, 1994; Dabney, 2013; Helfgott, 2008; Miethe, McCorkle, and Listwan, 2007). .

Literature Review

Criminologists spend a great deal of their effort studying types of crime, focusing on their characteristics, causes, consequences, and effective response strategies. The value of using a typology approach to studying and teaching about crime is that such an approach helps criminologists to bring together hundreds of different types of behaviors within specific crime categories in an effort to identify crime patterns (Clinard et al., 1994;Helfgott, 2013). White-collar crime and cybercrime are two types of crime that have received varying levels of attention from criminologists. What is not entirely clear, however, is the degree of overlap between these crime categories. As will be shown below, a number of similarities (and differences) exist between white-collar crime and cybercrime. After discussing the differences, attention will be given to similarities. This will be followed by rationale for studying the overlap between the two types of crimes, focusing on what can be called "white-collar cybercrime."

Differences Between White-Collar Crime and Cybercrime

Just as two types of cancer are both types of cancer, this does not mean that the two are the same. Colon cancer and skin cancer, for example, are varieties of cancer, but they have different causes, consequences, and remedies. In a similar way, while both are types of crime, differences exist between white-collar crime and cybercrime. These difference include the following:

- There are distinct forms of each type of crime.

- Cybercrime has more of an international focus.
- Cyber offenders tend to be younger offenders.
- Cybersecurity has been constructed as a national threa Cybercrime has been constructed as a national threat, as opposed to white collar crime. Cybersecurity is the tool intended to provide protection from this threat. In this sense, weak or ineffective cybersecurity is also seen as a national threat.
- Trust is manifested differently in the two types of crime.
- The education of the offenders may vary in white-collar crime and cybercrime (Payne, 2017).

To begin, while both white-collar crime and cybercrime capture various specific types of crime, the specific crime categories do not always overlap. These specific crime categories will be discussed below. For now, it is safe to suggest that certain types of cybercrime cannot be conceived of as white-collar crimes and certain types of cybercrime cannot be conceived of as white-collar crime. Consider the following:

- Cyberbullying in high school is a form of cybercrime, but it is not a form of white-collar crime.
- Child pornography is a form of cybercrime, but it is not a form of white-collar crime.
- Cyber hacking might represent a form of white-collar crime in some cases, but not others.
- Doctors who overcharge Medicaid are committing a white-collar crime, but not a cybercrime.
- Businesses that pollute the environment are committing a white-collar crime, but not a cybercrime.
- Businesses that engage in false advertising are committing a white-collar crime, but not a cybercrime (Payne, 2017).

The basic point is that the offense domain for white-collar crime and cybercrime is expansive, with many offense categories exhibiting no overlap.

Another difference between the two offense categories is that cybercrime has more of an international focus. Virtually any cybercrime could be committed across country borders. The same cannot be said of white-collar crime. In fact, a commonly cited challenge that arises in cybercrime investigations is the fact that the offenses can easily be committed across country borders (Brenner, 2006). To be sure, certain types of white-collar crime can be international in scope, and white-collar crime is an international problem; however, the very nature of some forms of white-collar crime (involving direct interactions between professionals and consumers/victims) suggests that the setting for these offenses is more often limited to the physical workplace where the offense occurs.

In addition to differences in the scope of the offenses, cyber offenders tend to be younger offenders than white-collar offenders. Hackers and malware writers tend to be in their 20s (Holt, Strumsky, & Smirnova, 2012). The average age of cyber bullying offenders and victims also appears to be younger (Marcum, Higgins, Freiburger, & Ricketts, 2012). After reviewing investigations by the agency's National Cyber Crime Unit, Britain's National Crime Agency (2017) recently reported an average age of 17 years for cyber offenders. Research has found that white-collar offenders (on average) begin their offending in their mid-30s and continue into their 40s (Weisburd & Waring, 2001). A more recent study of Norwegian offenders found the average age of white-collar offenders (at conviction) to be even higher at an average of 48 years old (Gottschalk, 2013).

A third difference between white-collar crime and cybercrime has to do with the construction of cybersecurity as a national threat. Unlike white-collar crime, cybersecurity has been defined as a national threat. Research shows that U.S. presidents "have linked the emerging problem of cybercrime with already established problems of national security or international security" (Hill & Marion, 2016a, p. 11). Elsewhere, Hill and Marion (2016b) examined how Presidents Obama, Clinton, and Bush addressed cybercrime in speeches related to cyber issues. The authors found that when discussing these issues, Clinton and Bush connected cyber issues to national security in half of their cyber speeches (which meant that Bush discussed cyber national security in 53 speeches and Clinton mentioned the topic 55 times). Obama connected cyber and national security themes in 70% (n=115) of his speeches on cyber issues. By comparison, politicians rarely, if ever, define white-collar crime as a national security threat.

Another difference between white-collar crime and cybercrime is that trust is manifested differently in the two types of crime. White-collar crime, at its very core, involves offenses that are based on violations of trust. Sutherland (1940) pointed this out in his presentation to the American Sociological Association when he introduced the concept. He said, "the varied types of white-collar crimes in business and the professions consist principally of violation of delegated or implied trust" (p. 3). We trust our doctors to treat us appropriately. We trust our financial advisors to invest our money appropriately. We trust judges to follow the law. With white-collar business professionals, we trust them to treat consumers and

members of the public ethically and fairly. Thus, the violation of trust distinguishes white-collar crimes from traditional crimes (Friedrichs, 2009). The role of trust is a little different for cybercrime. Generally speaking, we do not trust people with our computer information, nor do we trust that others will "leave us alone" on our computers. That is why individuals have multiple passwords and spend hundreds on virus protection packages. Regarding passwords, one recent estimate suggests that "the average business employee must keep track of 191 passwords" (Security Magazine, 2017, para. 1 np). Additionally, consumers spend nearly $5 billion a year on anti-virus protection packages (McMillan, 2012). The distinction between trust applications in white-collar and cybercrime is subtle, but significant. In particular, while consumers routinely engage in efforts to prevent cybercrime (presumably because of a lack of trust), they are not socialized to consistently engage in the same types of prevention activities to fend off white-collar crimes. As Friedrichs (2009) notes, "a great deal of variability exists in the degree of trust involved in relationships and transactions" (p. 9). Elsewhere, it has been noted that establishing trust in an online business relationship "is not as easy as through human-buyer/human-seller interaction" (Ceaparu, Demner, Hung, Zhao, & Shneiderman, 2002, p. 90).

Regarding education of offenders, for the most part, the path to a white-collar profession goes through college. Of course, many white-collar professionals never went to college, but the vast majority have been to college. In fact, for some white-collar professions (e.g., doctors, lawyers, professors, etc.), college degrees are required. White-collar offenders from those professions would then, by default, have college degrees. Among cybercriminals, it may be wrongly assumed that these offenders have high levels of education or intelligence. Hackers have varying levels of knowledge that are used to assign them status in the hacker community. Not all hackers have high levels of knowledge, and those hackers with higher levels of knowledge might "use the power they have gained to censor and admonish [new hackers] who ask for such knowledge" (Nycyk, 2016, p. 94). Some research suggests that many hackers have "minimal higher education" (Holt et al., 2012; p. 901).

Similarities Between White-Collar Crime and Cybercrime

Beyond the mere fact that both cybercrime and white-collar crime are labels used to describe categories of crime, several similarities exist between the two phenomena. These include the following:

- The impact on businesses and consumers outweighs the impact of other crimes.
- The nature of victimization differs from street crime.
- Both types have specialized police units designed to respond to them.
- There is a large "dark figure" of white-collar crime and cybercrime.
- Conceptual ambiguity makes it harder to study and understand the topics.
- The setting where the offenses occur are different from traditional crimes.
- They are both related to occupational crime.
- Neither are central to the study of crime and criminal justice.
- White-collar and cybercrime capture specific types offenses.
- These themes are discussed below.

To begin, regarding their impact on businesses and consumers, both cybercrime and white-collar crime can dramatically (and negatively) impact businesses and consumers. A study by the Association of Certified Fraud Examiners (ACFE, 2016) estimated that the "typical organization" lost 5% of its revenue to fraud in 2015. The median loss per fraud case was estimated at $145,000. Cybercrime estimates are similarly high. The Ponemon Institute (2017) estimates that that the average the cost of a data breach (in a sample of 419 companies) was $3.62 million. While high, this estimate was actually down from $4 million the prior year. By comparison, FBI (2017) data estimate the average reported robbery to cost victims $1,400. Suffice it to say that white-collar crime and cybercrime present significant costs to businesses. These costs are passed on to consumers (Friedrichs, 2009).

Another similarity has to do with the nature of victimization for white-collar crime and cybercrime. For example, for both types of offenses, victims may not realize they have been victimized until long after the victimization has occurred. In a similar way, the consequences of the victimization may surface long after the actual offense was committed. In traditional street crimes, victims typically "know" almost immediately that they have been victimized. Another similarity related to the nature of victimization is that both cybercrime and white-collar crime can impact large numbers of victims. A data breach by a hacker can harm thousands of citizens, just as a crime by a corporation can (environmental crime, for example, could create untold damage for entire communities).

One can point to the need for specialized police units in responding to white-collar crime and cybercrime as another similarity between the two types of offenses. Many specific types of white-collar crime (health care fraud, environmental crimes,

economic crimes, etc.) have specialized police unites assigned to respond to these offenses (Payne, 2017). In a similar way, cybercrime units and digital forensics units have been developed in some police departments in order to strengthen the response to cyber offenses. Whether for white-collar crime or cybercrime, these specialized units are justified in that they provide criminal justice officials specialized knowledge needed to respond to these crimes. Also, the majority of policing for both types of offenses is done at the federal level.

Another similarity between white-collar crime and cybercrime is that both have an enormous "dark figure" when considering efforts to estimate the extent of crime. Criminologists use the phrase "dark figure" to refer to the amount of crime that occurs without officials knowing about those crimes. According to one cybercrime expert, "the dark figure is very high, as it deals with crimes that cannot be detected without a high level of investigation" (Agustina, 2015, p. 35). Others have explored whether the apparent crime drop in property crimes since the 1990s can be attributed to undetected incidents of online property offenses (Tcherni, Davies, & Lizotte, 2016). Similar comments have been made about white-collar crime. In the words of one author team, "the 'dark figure' of white-collar crime is undoubtedly much larger than it is for other forms of crime" (Benson, Kennedy, & Logan, 2016, p. 93).

In addition, both white-collar crime and cybercrime suffer from what can be coined conceptual ambiguity. In other words, both crime categories have been accused of being vaguely defined. With white-collar crime, concerns about conceptual ambiguity arose soon after Sutherland first introduced the crime. Scholars questioned whether behaviors that were never criminally prosecuted could be labeled crimes and even debated what was meant by the phrase "white-collar" (Payne, 2017). As Felson and Eckert (2016) note, "'white-collar crime' is poorly named, because any work, any professional or occupational role, can get involved in crime" (p. 177). The concept of cybercrime has faced similar scrutiny. In fact, many different terms have been used to describe what is seemingly the same behavior. For example, the dated term of "computer crime" was replaced with terms such as "Internet crime," "online crime," "cyber deviance," and other terms.

Offense setting is another similarity between cybercrime and white-collar crime. In particular, both types of offenses typically occur in settings different from where traditional street crimes occur. Simply put, white-collar crimes frequently happen in the suites, not on the streets, while cybercrimes "occur" in cyberspace. The setting where these offenses occur partly explains the larger dark figure associated with the crime types.

White-collar and cybercrime are also similar in that they are both related to *occupational crime.* The notion of occupational crime can be traced to Clinard and Yeager (1980) who, in response to some of the ambiguity surrounding Sutherland's white-collar crime topic, recommended that the broader term be categorized into two subtypes: occupational crime and corporate crime. The former type of crime refers to criminal acts by workers during the course of their job, while the latter refers to crimes by corporations that are designed to further the interests of the corporation. In terms of the overlap between occupational crime, white-collar crime, and cybercrime, it seems plausible to suggest that while occupational crimes have been categorized within a white-collar crime typology, cybercrimes could be categorized within both a white-collar crime typology and an occupational crime typology. In other words, in some cases, some types of white-collar crimes might be cybercrimes (e.g., if a white-collar professional engages in hacking), while others might be categorized as occupational crimes (e.g., if a low-level employee steals computer passwords and sells them). The degree to which cybercrimes can be conceptualized as workplace crimes has not been established in prior research. This study aims to begin to fill that void.

Yet another similarity between white-collar crime and cybercrime is that neither of the offense types are central to the study of crime and criminal justice. Criminologists have used the phrase "disappearing act" in reference to an apparent reduction in criminological studies on certain types of white-collar crime (Lynch, McGurrin, & Fenwick, 2004). More recently, a study of the coverage of white-collar crime in criminological scholarship and coursework found that the topic receives minimal coverage (McGurrin, Jarrell, Jahn, & Cochrane, 2013). Focusing on the coverage of cybercrime in criminal justice programs and criminal justice scholarly journals, a similar conclusion was made about cybercrime (Payne & Hadzhidimova, in press).

A final similarity between white-collar crime and cybercrime is that each of them are labels used to categorize a range of other offense types. For example, white-collar crime has been described as including the following types of crimes:

- *Crime in sales and service systems* – this includes crime in retail settings, the automotive industry, the hotel industry, restaurants, the insurance arena, and other occupational settings designed to sell goods or provide consumers services.
- *Crime in the criminal justice system* – this includes police corruption, crimes by lawyers,

judicial misconduct, and crimes by correctional officers.

- *Crime in the political system* – this includes crimes committed by politicians or their aides as part of their legislative activities.
- *Crime in the educational system* – this includes crimes committed in the educational arena by teachers, professors, education employees, and students that are connected to their specific roles in the educational setting.
- *Crime in the religious system* – this includes crimes committed by religious professionals that are conducted in conjunction with their clerical duties.
- *Crime in the health care system* – this includes crimes committed by doctors, nurses, aides, and other health care professionals while providing health care.
- *Crime in the economic system* – this includes crimes committed in an effort to unfairly take advantage of the economy and economic institutions (e.g., insider trading, crimes in stock market or commodities offenses, etc.)
- *Crime in the housing system* – this includes crimes committed in the housing industry such as mortgage fraud and provision of unsafe housing.
- *Corporate crime* – this includes crimes committed on behalf of the corporation or business (price gouging, false advertising, etc.)
- *Environmental crime* – this includes crimes against the environment conducted in the course of a legitimate occupational activity.
- *Crime in the technological system* – this includes technological crimes committed in or against the workplace (Payne, 2017).

Friedrichs (2009) describes another type of white-collar crime that does not fit nicely in the above categories – contrepreneurial crime, which is a term that Friedrichs attributes to Francis (1988). The word "contrepreneur" combines the phrases "con artist" and "entrepreneur" and describes those situations when offenders "[carry] out a swindle while appearing to be engaged in a legitimate enterprise" (p. 200). They key here is that victims view the offender as carrying out a legitimate business or a legitimate activity, but the offender is not actually a legitimate business or enterprise (despite their appearance as one). In the same section where he discusses entrepreneurial crime, Friedrichs also describes "technocrime," which is analogous to crimes committed in the technological system. Most of these offenses could also be captured under the heading of cybercrime.

Just as there are types of white-collar crime, there are also types of cybercrime. One author team describes the following categories:

- *Computer hacking* – refers to efforts to illegally access computer or network accounts of individuals, businesses, agencies, or others.
- *Malware and automated computer attacks* – refers to efforts to release viruses, trojans, or other forms of malware into a computer or network.
- *Digital piracy and intellectual property theft* – refers to efforts to steal digital property or other forms of intellectual property including movies, music, software, books, and so on.
- *Economic crime and online fraud* – refers to efforts to steal from individuals through fraudulent activities using the Internet, email, or other electronic communication tools.
- *Pornography, prostitution, and sex crimes* – refers to the use of the electronic technology to commit crimes related to child pornography, prostitution, and other sex offenses.
- *Cyberbullying, online harassment, and cyberstalking* – refers to the use of technology to bully, harass, or stalk individuals.
- *Online extremism, cyber terror, and cyber warfare* – refers to the use of technology, the Internet, or other forms of digital technology to promote alternative beliefs, fear, or harm that is tied to political ideology (Holt et al., 2015).

Recognizing that there are similarities between white-collar crime and cybercrime, as well as important conceptual, theoretical, and practical differences, it is important to consider the degree to which overlap exists between the offense categories. Certainly, some types of cybercrime are committed in the workplace, and some white-collar crimes involve the use of cyber technology. With this conceptual overlap in mind, in this study, attention is given to what can be called "white-collar cybercrime." White-collar cybercrime refers to cybercrimes that are also white-collar crimes.

Related to Friedrichs' concept of technocrime, white-collar cybercrime places the focus of the offense on the role of the workplace and the technology, rather than just the technology. Concluding his discussion about technocrime, Friedrichs (2010) wrote, "it should be obvious that the problem of crimes committed in cyberspace will increase in the future and will increasingly be a key element of different forms of white-collar crime" (p.217). While Friedrichs' prediction is accurate, the topic has rarely been addressed in the criminological literature. Some authors have examined technocrime from a broader orientation (Gagnon, 2008; Leman-Langlois, 2008),

but few have considered the overlap between white-collar crime and cybercrime. Li (2008) makes reference to the phrase and cites a news article on the "white-collar hacker," and some reporters have discussed "white-collar Internet crime" in reference to white-collar crimes committed through the Internet (O'Connell, 2011). Mohamed (2013) points out that "white-collar cybercrime...is not sufficiently reported due to reluctance or ignorance" (p. 68). This possibly explains why no criminological studies have empirically examined connections between white-collar crime and cybercrime. Filling this void, this study addresses the following questions: (1) What types of white-collar cybercrime are committed?; (2) What are the patterns surrounding those offenses?; and, (3) How does the criminal justice system respond to white-collar cybercrimes?

Method

To address these questions, a content analysis was conducted using press releases describing 109 "white-collar cybercrimes" available online from the Department of Justice's Computer Crime and Intellectual Property Section. Cases were included if they included a cyber component and if the offense could be classified as a white-collar crime. The operationalization of white-collar crime was determined by whether the offense could be described as a "legitimate white-collar crime" (meaning that the offense was committed by a worker or former worker in relation to his or her legitimate occupation) or as a "contrepreneurial crime" (meaning that the offender used the guise of a legitimate occupation/business endeavor to commit the offense).

Other types of cybercrime were excluded because of a desire to develop an understanding about those types of crimes involving workplace-related cyber offenses. Researchers often focus on specific types of white-collar crime in an effort to create basic awareness about types of crimes that have been rarely addressed. For example, studies have focused on crimes such as Medicaid fraud (Jesilow, Geis, & Harris, 1995), patient abuse in nursing homes (Payne & Gainey, 2006), and automobile repair fraud (Jesilow, 1982). In addition, researchers have recognized that the characteristics of white-collar crime are distinct from other frauds, which further supports the decision to focus solely on white-collar cyber offenses (See Steffensmeir, 1989).

Cases reported between 2015 and 2017 were included in the analysis. The coding included the variables gender, age, whether the offense had an international connection, if the offender committed the offense as a current or former offender, who the victim was, number of offenders, specific type of crime committed, and whether the offense would be classified as a legitimate white-collar crime or contrepreneurial white-collar crime. If the majority of the offense was clearly tied to a legitimate occupational enterprise, these were coded as "legitimate white-collar crimes." If the majority of the offense appeared to be tied to an illegitimate enterprise, these were coded as "contrepreneurial white-collar crimes." Both are types of white-collar crime described in the literature. As noted above, the latter refers to situations where con artists use entrepreneurial efforts to form illegitimate enterprises.

Press releases varied in the amount and types of detail included. Some included information about an offender being arrested or indicted, while others included information about the offender being sentenced or convicted. Press releases that described multiple offenders were coded so that multiple offenders were coded separately only if full information about the case resolution was present. Otherwise, just the primary offender and relevant information was included in the study.

Results

Table 1 provides an overview of the results from the content analysis of the 109 press releases. As shown in the table, the vast majority of offenders described in the press releases were males, with just seven of the 109 offenders being females. In terms of victimization, the public and the offender's employer were targeted most often, though the film/entertainment industry was targeted in 12% of the cases (n=13). Roughly one-fourth (n=26) of the offenses had an international connection (e.g., either the offender was from another country or acted in concert with someone from another country). More than half of the offenses (n=59) reported only single offenders, while just under half of the offenses involved multiple offenders (n=40).

Table 1: Sample Characteristics

	n	%
Gender		
Male	102	93.5
Female	7	6.5
Legitimate White-collar Crime	47	43.1
Contrepreneurial White-collar Crime	62	56.9
Number of offenders		
One	59	54.1
More than one (group)	50	45.9
International connection	26	23.9
Victim		
Public	46	42.2
Offender's Employer	33	30.3
Film/entertainment industry	13	11.9
Government	6	5.5
Other	12	10.1
Specific Offense Type*		
Counterfeit goods (distribution, etc.)	28	25.7
Theft of secrets	21	19.2
Hacking	19	17.4
Crime in online sales	18	16.5
Unauthorized access	16	14.8
Piracy/copyright violations	16	14.8
Destruction of property	12	11.0
Identity theft	9	8.3
Fraud	9	8.3
Crime in the economic system	7	6.4
Crime in the health care setting	4	3.7
Crime in the criminal justice system	2	1.8
Sentence*		
Prison	44	83.0
Probation/Supervised Release	21	39.6
Restitution	28	51.9
Fine	7	13.2
Age		
Below 30 years	15	16.3
Above 30 years	77	83.7

*the numbers and percentages exceed what might be expected because offenders could have committed multiple offenses or received multiple sentences. Also, not all press releases included resolved cases. Some announced arrests or indictments, without information on sentences.

More than 80% of the offenders were in their 30s or above, which suggests a slightly higher age range than other cybercrime studies (Holt et al., 2012). However, this may be a result of the fact that the study is focusing on a subset of cybercrime offenders (e.g., white-collar cybercriminals), as well as the sample including only offenders who are in contact with the justice system. Overall, the average age of the sample was 39.1 years.

Regarding white-collar crime categorization, 62 of the offenses were classified as contrepeneurial crimes while 47 were classified as "legitimate white-collar crimes," meaning that the business/employee/employer involved in the offense was functioning solely in a legitimate manner. To demonstrate the differences, consider the following four examples quoted from the press releases:

- *Contrepreneurial*: "[the offender committed] crimes related to his operation of "Codeshop," a website he created for the sole purpose of selling stolen credit and debit card data, bank account credentials and personal identification information — obtained through illegal hacking and phishing schemes — for financial gain" (U.S. Department of Justice, 2017, August 25)
- *Contrepreneurial*: "[the offender] participated in a scheme to create and sell malware that could be used to spy on and steal personal information from a Google Android cell phone without the owner's knowledge. [The offender] crafted a piece of malware ultimately named "Dendroid" which, through the use of a binder, could hide itself within a Google App and then download onto a Google Android phone when the user of that phone downloaded the Google App from a place such as the Google Play Store." (U.S. Department of Justice, 2015, August 25)
- *Legitimate*: "[The company] maintained computer servers related to the dispensing machines at its facility in Niles. [The offender] worked at the facility as a contractor from November 2014 to February 2016, after which his access to Grainger's servers was deactivated. [The offender] hacked into the servers on several occasions in July 2016, the indictment states." (U.S. Department of Justice, 2017, December 14)
- *Legitimate:* "Acting Manhattan U.S. Attorney Joon H. Kim said: "[The offender] admitted to hacking into a competitor's computer network and stealing client data to boost the value of ***, a company he founded. [The offender] then attempted to sell [his company] – a company he grew using the stolen information -- to the very company he had hacked. For his criminal attempts to gain an unfair business edge, [the offender] has now been sentenced to prison." (U.S. Department of Justice, 2017, October 6)

Counterfeit goods violations (*n*=28) were the most common specific offense type, perhaps partly due to the fact that the cases reviewed were from the Computer Crime and Intellectual Property Section Some of the counterfeit goods cases may have been more of an "intellectual property" offense than a cybercrime. They were included in this study only if there was some (even if it were minor) cyber component to the offense. Theft of secrets (*n*=21), hacking (*n*=19), and crime in online sales (*n*=18) were the next most common specific offense types. The latter type included those offenses in which it was clear that offenders used online mechanisms to sell goods illegally. In fact, eBay was mentioned in nine of the press releases as being one of the outlets for the sales.

Regarding criminal justice processing, 53 of the press releases included conviction and sentencing information. Of those cases in which the sentence was reported, prison sentences were the most common sanction with 44 of the 53 (83%) sentenced offenders being incarcerated. Restitution (*n*=28) was the next most common sanction, followed by probation/supervised release (*n*=21). Some offenders received multiple sanctions (e.g., prison and restitution, prison followed by supervised release).

Table 2 provides additional details about the sanctions given to offenders. The average prison sentence was 195.77 months, though this mean was inflated due to two outlier sentences. In fact, the range of the prison sentences went from one month to 1,380 months. The median prison length was 29.5 months. The mean probation sentence was 38.57 months. The mean restitution amount was $1.1 million. Here again, a wide range (e.g., 1,334 to 12.9 million) inflated the mean. The median restitution amount was $63,497.

Table 2: Average Sanctions Given to Offenders

	Median	Mean	(*SD*)	Range
Prison (*n*=44)	29.5 months	195.77	15.24	1 to 1,380 months
Probation/SR (*n*=21)	36 months	38.57	15.25	6 to 60 months
Restitution (*n*=28)	$63947	$1,139,350.82	2,837,695	1,334-12.9 million
Fine (*n*=7)	$5000	$4785.71	3169.39	1000-10,000

Table 3 shows the differences between the "legitimate white-collar crimes" and the "contrepreneurial white-collar crimes." Several differences were found. First, contrepreneurial white-collar crimes were more likely to have international connections, with nearly a third of them being internationally connected in comparison to 15% of legitimate white-collar crimes,$\chi 2$ (1, N=109) = 3.6, $p \leq .05$). Second, the contrepreneurial crimes were more likely to involve groups, with nearly two-thirds of the contrepreneurial offenders working with others and just one-fifth of the legitimate white-collar offenders doing so, $\chi 2$ (1, N=109) = 20.1, $p \leq .001$). Third, differences were found in specific offense types, with contrepreneurial white-collar offenders being more likely than legitimate white-collar offenders being more likely to commit counterfeit goods violations, $\chi 2$ (1, N=109) = 7.2, $p \leq .01$), piracy/copyright violations (Chi Square = 10.4, $p \leq .001$), and fraud (p= .04, *Fishers Exact Test*), while legitimate white-collar offenders were more likely than contrepreneurial offenders to commit theft of secrets, $\chi 2$ (1, N=109) = 28.8, $p \leq .001$), unauthorized access, $\chi 2$ (1, N=109) = 19.3, $p \leq .001$), and destruction of property offenses, $\chi 2$ (1, N=109) = 13.0, $p \leq .001$). In addition, legitimate white-collar offenders were more likely than contrepreneurial offenders to be sentenced to probation, $\chi 2$ (1, N=109) = .4.85, $p \leq .05$). There were no differences in likelihood of prison sentences between the offense categories.

Table 3: Legitimate White-Collar Crime and Contrepreneurial Crime Characteristics

	Legitimate White-Collar Crime		Contrepeneurial Crime	
	n	%	*n*	%
Internationally Connected*	7	14.9	19	30.6
Group Offense***	10	21.3	40	64.5
Specific Offense Type^				
Counterfeit goods (distribution, etc.)**	6	12.8	22	35.5
Theft of secrets***	20	42.6	1	1.6
Unauthorized access***	15	31.9	1	1.6
Piracy/copyright violations				
Destruction of property***	11	23.4	1	1.6
Identity theft	2	4.2	7	11.3
Fraud*	1	2.1	8	12.9
Piracy/Copyright violations***	1	2.1	15	24.2
Sentence^				
Prison	19	82.6	25	83.3
Probation*	13	56.5	8	26.7

^The numbers and percentages exceed what might be expected because offenders could have committed multiple offenses or received multiple sentences. Also, not all press releases included resolved cases. Some announced arrests or indictments, without information on sentences.
*$p \leq .05$, **$p \leq .01$,***$p \leq .001$

Table 4 shows gender comparisons. Given the small number of female offenders, these findings should be interpreted with caution. Cross tabulations were conducted comparing gender to dependent variables of interest. Due to low cell sizes, one-tailed Fisher's exact tests were used to determine whether statistically significant gender differences existed. Just one difference was found from the cross tabulations. Females were more likely than males to commit their offenses in groups. In fact, each female committed her white-collar cybercrime in a group, in comparison to 42% of males (Fisher's exact=.003). While there were few gender differences found, females were older (50.8 years) than male offenders (38.37 years) t(90)=-2.85, $p \leq .05$, but age was reported for just five of the seven female offenders.

Table 4: Gender Patterns

	Male		Female	
	n	%	*n*	%
Legitimate White-Collar Crime	45	44.1	2	28.6
Contrepreneurial White-Collar Crime	57	55.9	5	71.4
Group Offense**	43	42.2	7	100.0
International connection	25	24.5	1	14.3
Specific Offense Type^				
Counterfeit goods (distribution, etc.)	27	26.5	1	14.3
Theft of secrets	21	20.6	0	0.0
Hacking	18	17.8	1	14.3
Crime in online sales	4	4.4	3	16.7
Unauthorized access	6	6.5	1	6.3
Piracy/copyright violations	14	13.7	2	28.6
Destruction of property	12	11.8	0	0.0
Identity theft	5	5.0	2	22.2
Fraud	8	7.8	1	14.3
Sentence^				
Prison	43	86.0	1	33.3
Probation	19	38.0	2	66.7
Restitution	27	52.9	1	33.3
Fine	7	14.9	0	0.0

^the numbers and percentages exceed what might be expected because offenders could have committed multiple offenses or received multiple sentences. Also, not all press releases included resolved cases. Some announced arrests or indictments, without information on sentences.
**$p \leq .01$

Table 5 shows international patterns. Here again, small cell sizes led to the use of Fisher's exact test for some comparisons. A few differences were found. First, offenses with international connections were more likely to be committed in groups than U.S.-based offenses, $\chi 2$ (1, N=109) =13.3, $p \leq .001$). In addition, internationally-connected offenders were less likely to commit crime in online sales (p=.004, *Fisher's Exact Test)* and unauthorized access offenses (p=.01, *Fisher's Exact Test),* but more likely to commit identity theft (p=.05, *Fisher's Exact Test*) and fraud (Fisher's exact=.001). Not surprisingly, probation/supervised release was rarely used in cases involving internationally-connected offenders (p=.034, *Fisher's Exact Test*).

Table 5: International Patterns

	United States		Internationally Connected	
	n	%	*n*	%
Group Offense***	30	36.1	20	76.9
Specific Offense Type^				
Counterfeit goods (distribution, etc.)	22	26.5	6	23,1
Theft of secrets	15	18.1	6	23.1
Hacking	12	14.5	7	26.9
Crime in online sales**	18	21.7	0	0.0
Unauthorized access**	16	19.3	0	0.0
Piracy/copyright violations				
Destruction of property	11	13.3	1	3.8
Identity theft*	4	4.8	5	19.2
Fraud***	2	2.4	7	26.9
Piracy	13	15.7	3	11.5
Sentence^				
Prison	34	79.1	10	100.0
Probation/Supervised Release*	20	46.5	1	10.0
Restitution	25	56.8	3	30.0
Fine	7	16.3	0	0.0

^the numbers and percentages exceed what might be expected because offenders could have committed multiple offenses or received multiple sentences. Also, not all press releases included resolved cases. Some announced arrests or indictments, without information on sentences.
*$p \leq .05$, **$p \leq .01$,***$p \leq .001$

One difference was found regarding sanctions given to international offenders. The average prison sentence length for internationally connected offense was 368.2 months, in comparison to an average of 28.6 months for domestic white-collar cybercrimes, t(9.0)_t=-2.0, p<.05. While statistically significant, of the 10 international offenders for whom a prison sentence was reported, two of those received exorbitantly high sentences (1,140 months and 1,380 months). When removing those two outliers, the statistically significant differences were no longer significant.

Table 6 shows age differences between variables of interest. Four differences were found. First, legitimate white-collar cyber offenders were older (41.8 years) than contrepreneurial white-collar cyber offenders (36.7 years); t(90)=-2.5, $p \leq .05$). Second, internationally-connected white-collar cyber offenders were younger (35.1 years) than U.S.-based offenders (40.0 years) t(90)=1.8, p <.05). Third, those who committed their offenses in groups were younger (36.5 years) than were those who acted alone (40.9 years)t(90)=2.1, p<.05). Fourth, hackers were younger (32.6 years) than were other offenders (40.2 years) t(27.8)=3.71, p<.001). In fact, across all offense types, hackers were the youngest.

Table 6: Age Patterns

	Yes		No	
	x	*SD*	*x*	*SD*
Legitimate White-Collar Crime*	41.8	10.0	36.7	9.7
Internationally Connected*	35.1	6.6	40.0	10.6
Group Offense*	36.5	9.7	40.9	10.2
Specific Offense Type				
Counterfeit goods (distribution, etc.)	39.9	13.2	38.8	9.0
Theft of secrets	41.7	9.6	38.4	10.2
Hacking***	32.6	6.2	40.2	10.3
Crime in online sales	39,8	11.2	38.9	10.0
Unauthorized access	37.4	5.4	39.5	10.9
Piracy/copyright violations	38.1	9.3	39.2	10.4
Destruction of property	35.1	7.5	29.6	10.4
Identity theft	34.8	6.3	39.3	10.3

*$p \leq .05$, ***$p \leq .001$

Discussion

This study explored the patterns surrounding white-collar cybercrime, a topic seemingly rarely considered in the criminological literature. The findings suggest that white-collar cybercrime has similarities to both white-collar crime and cybercrime, though some apparent differences also arise. White-collar cybercrime is similar to white-collar crime and cybercrime in that the bulk of offenses are committed by males. This pattern is found in white-collar crime studies (Steffensmeier, Schwartz, & Roche, 2013) and cybercrime studies (Higgins, Wolfe, & Marcum, 2008). Alternatively, white-collar cybercrime offenders appeared to be older than what is found in other studies focusing on specific types of cybercrimes (Holt et al., 2012). To be sure, hackers were the youngest offenders in this study, though their average age was in the thirties. Also, when convicted, white-collar cyber criminals were likely to receive a prison sentence. In addition, "legitimate white-collar cyber criminals" appeared to be significantly different from "contrepreneurial white-collar cyber criminals." Collectively, these findings have important implications for policy/practice, theory, and research.

First, recognizing that there is overlap between white-collar crime and cybercrime, experts should identify strategies that are effective for responding to each crime type in an effort to shed some light on appropriate response strategies. For the most part, separate investigation strategies are used for white-collar crimes and cybercrimes. In some cases, it could be that strategies used to respond to white-collar crime can be incorporated into the cybercrime investigations and vice versa. Such a response will ensure that the investigation techniques are tailored to the dynamics of the offense.

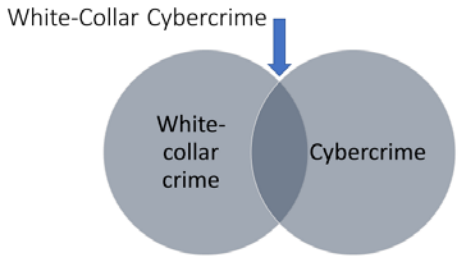
Second, and somewhat related, the "group" dynamics in this study demonstrate that a sizable proportion of white-collar cybercrimes were done in groups. It has been suggested elsewhere that white-collar crime investigators seek out the "least culpable" offender in order to get them to participate in the investigation early on (Payne, 2017). This suggestion would seem to be slightly more appropriate for the contrepreneurial white-collar cyber crimes, which were more likely than legitimate white-collar offenses to be committed in groups.

Third, professionals must resist the temptation to conflate white-collar crime and cybercrime. They are two completely different types of crime categories. There is even great variation between "legitimate white-collar cybercrime" and "contrepreneurial white-collar crime." Conflating white-collar crime and cybercrime will lead to a number of issues such as artificially exaggerating the extent of both crime types, misstating the causes of the two types of crime, and masking appropriate intervention strategies.

Fourth, while avoiding the temptation to conflate white-collar crime and cybercrime, professionals at the same time must not lose sight of the fact that a sizable portion of cybercrimes are, in fact, white-collar cybercrimes. It has been suggested that "disgruntled

employees are the greatest threat to a computer's security" (Sinod & Reilly, 2000, p. 7). Another expert suggested that cyber intrusions are "usually not an 'outside' job" (Minnaar, 2013, p. iii). Figure 1 provides an illustration that helps to demonstrate the overlap between white-collar crime and cybercrime. It is this overlap that includes cases that can be called white-collar cybercrime. If insiders truly are the biggest threat to cybersecurity, attacking the problem as a business problem (or a white-collar crime) problem would seem to be an appropriate step.

Figure 1: Overlap Between White-Collar and Cybercrime



These findings also have implications for theory. First, consider the counterfeit goods crimes and the online sales crimes. It is widely known that consumers have begun to shop more online than they do in physical stores. This change in consumer behavior has led to the closure of several retail outlets. From a criminological perspective, the change in consumer behavior would also present different opportunities for crime. More specifically, it would seem that routine activities theory (see Cohen & Felson, 1979) would support the notion that a shift in vulnerable targets has occurred for offenses tied to consumer behavior.

Second, and also related to routine activities theory, it is important to suggest that the findings described in this study might actually reflect the "routine activities" of the "capable guardians" (e.g., law enforcement) more so than the behavior of "motivated offenders." Consider, for example, that no internationally-connected offenders were convicted of unauthorized access or online sales crimes. Does that mean that internationally-connected offenders are not committing those offenses? Of course not! It likely means that it is easier for law enforcement to catch domestic offenders who commit these crimes. What this suggests is that – at least for white-collar cybercrime – capable guardianship is a fluid variable that is related to both offender characteristics and offense type.

Third, though there are so few female white-collar cyber offenders in the sample, or perhaps because there were so few female white-collar cyber offenders in the study, implications related to patriarchal theory arise. Are there so few female white-collar cyber offenders females are dissuaded from science and engineering (e.g., cyber) fields? Also, while it is interesting that none of the female white-collar cyber offenders "acted alone," one must ask whether their role in the offense was subservient to the male offender. As well, one must question whether female offenders were used as pawns in order to sustain a conviction. Of course, it must be noted that males represent the majority of offenders in most crime categories. The question that arises is whether the reasons for their low offending rates in white-collar cyber offenses are different from those reasons they rarely commit other crimes, and it is important to determine whether their roles as co-conspirator (rather than sole offender) transcend across offense types.

A fourth implication has to with deterrence theory. Finding that the vast majority of white-collar cyber offenders who were sentenced received a prison sentence runs counter to claims that white-collar offenders are treated leniently. Of course, it could be, as Gerber (1994) has noted, that once a white-collar offender gets to the conviction stage, their high likelihood of incarceration masks the fact that most white-collar offenders never enter the justice process to begin with. Either way, publicizing the fact that convicted white-collar cyber offenders are being sentenced to prison can be seen as a form of general deterrence, or at least as an effort towards achieving general deterrence ideals. In fact, presumably the purpose of the Department of Justice press releases is, in part, based on deterrence assumptions.

This study is not without limitations. As noted in the literature review, both white-collar crime and cybercrime have large dark figures. Given that this study focused on reported offenses, it is not clear whether unreported offenses would exhibit the same patterns. After all, it has been suggested that businesses sometimes avoid reporting victimization to authorities because they do not want the negative publicity (Friedrichs, 2009). Just as likely is the possibility that businesses do not know they have been victimized, or they do not know who committed the offense. Second, the cases included in this study are only those that members of the Computer Crime and Intellectual Property Section share with the public. Again, this extends the potential dark figure even more. Another limitation is that the sample focuses only on cases handled in the United States. Given the international nature of these crimes, it is plausible that other countries would exhibit different patterns.

Conclusion

Despite these limitations, a number of questions surface for future research studies. First, researchers should explore ways to assess the dark figure of white-collar cybercrimes. Whether through self-report surveys or some other strategy, better understanding is needed about this behavior. Second, researchers should more fully explore the role of gender in white-collar cybercrimes. Why are there so few women represented in these offenses? Is it because of structural biases limiting women's occupational opportunities, or is it a result of better occupational socialization for female employees? Third, researchers should explore how white-collar contrepreneurial cybercrimes have evolved over time. A few decades ago, telemarketing fraud was believed to be rampant. Have those frauds been replaced with white-collar contrepreneurial cybercrimes? If so, what will these crimes "look like" in the future? Finally, researchers should explore how white-collar cybercrimes compare to and can be distinguished from other types of cybercrime. Expanding our efforts to understand white-collar cybercrime will help us to understand how the technological revolution has shaped, and will continue to shape, crime in the workplace and crime in cyberspace.

References

Agustina, J. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, 9(1), 35-54. doi: 10.5281/zenodo.22239

American Sociological Association. (n.d.). *Edwin Hardin Sutherland*. Retrieved from: http://www.asanet.org/about-asa/asa-story/asa-history/past-asa-officers/past-asa-presidents/edwin-h-sutherland.

Association of Certified Fraud Examiners. (2016). *Report to the nations on occupational fraud and abuse*. Retrieved from http://www.acfe.com/rttn2016/costs.aspx

Benson, M., Kennedy, J., & Logan, M. (2016). White-collar and corporate crime. In B.M. Huebner & T.S. Bynum (Eds.), *The handbook of measurement issues in criminology and criminal justice* (pp. 92–110). West Sussex, UK: Wiley.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, *46*(4-5), 189–206. doi: 10.1007/s10611-007-9063-7

Ceaparu, I., Demner, D., Hung, E., Zhao, H., & Shneiderman, B. (2002). "In web we trust": Establishing strategic trust among online customers. In R. T. Rust & P.K. Kannan (Eds.), *E-service: New directions in theory and practice* (pp. 90–107). New York, NY: Routledge.

Clinard, M., & Yeager, P. (1980). *Corporate crime*. New Brunswick, NJ: Free Press.

Clinard, M.B., Quinney, R., & Wildeman, J. (1994). *Criminal behavior systems: A typology*. Cincinnati: Anderson Publishing.

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

Dabney, D. (2013). *Crime types: A text/reader*. New York: Wolters Kluwer.Federal Bureau of Investigation. (2017). *Crime in the United States.* Retrieved from https://ucr.fbi.gov/crime-in-the-u.s.

Felson, M., & Eckert, M. (2016). *Crime and everyday life* (5th ed.). Thousand Oaks, CA: Sage.

Francis, D. (1988). *Contrapreneurs*. Toronto, Ontatio, Canada: MacMillan.

Friedrichs, D. (2009). *Trusted criminals* (4th ed.). Belmont, CA: Cengage.

Gagnon, B. (2008). Cyberwars and cybercrimes. In S. Leman-Langlois (Ed.), *Technocrime: Technology, crime, and social control* (pp. 46–65). New York, NY: Routledge.

Gerber, J. (1994). "Club Fed" in Japan? Incarceration experiences of Japanese embezzlers. *International Journal of Offender Therapy and Comparative Criminology*, *38*(2), 163–174. doi: 10.1177/0306624X9403800208

Gottschalk, P. (2013). Victims of white-collar crime. *Matters of Russian and International Law*, *3*(3), 91-109.

Helfgott, J.B. (2008). *Criminal behavior: Theories, typologies, and criminal justice*. Thousand Oaks, CA: Sage.

Henning, P. J. (2015). Is deterrence relevant in sentencing white-collar criminals? *Wayne Law Review*, *61*(1), 27–59.

Higgins, G., Wolfe, S., & Marcum, C. (2008). Music piracy and neutralization: A Preliminary Trajectory Analysis from Short-Term Longitudinal Data. *International Journal of Cyber Criminology*, *2*(2), 324-336.

Hill, J., & Marion, N. (2016a). Presidential Rhetoric and Cybercrime: Tangible and Symbolic Policy

Statements. *Criminology, Criminal Justice Law, and Society, 17*(2), 1–17.

Hill, J., & Marion, N. (2016b). Presidential rhetoric on cybercrime: Links to terrorism? *Criminal Justice Studies, 29*(2), 163–177. doi: 10.1080/1478601X.2016.1170279

Holt, T., Strumsky, D., & Smirnova, O. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(1), 891-903.

James, R. (2009). Cybercrime. *Time*. Retrieved from http://content.time.com/time/nation/article/0,8599,1902073,00.html

Jesilow, P., Geis, G., & Harris, J. (1995). Doomed to repeat our errors. *Social Justice, 22*(2), 125–138.

Jesilow, P. (1982). Deterring automobile repair fraud. (Doctoral dissertation). University of California, Irvine, CA.

Leman-Langois, S. (2008). Introduction: Technocrime. In S. Leman-Langlois (Ed.), *Technocrime: Technology, crime, and social control* (pp. 1–13). New York, NY: Routledge.

Li, X. (2008). The criminal phenomenon on the Internet. *University of Ottawa Law and Technology Journal, 5*, 125–140.

Lynch, M. J., McGurrin, D., & Fenwick, M. (2004). Disappearing act: The representation of corporate crime research in criminology journals and textbooks. *Journal of Criminal Justice, 32*(5), 389–398. doi: 10.1016/j.jcrimjus.2004.06.001

Marcum, C.D., Higgins, G.E., Freiburger, T.L., & Ricketts, M.L. (2012). Battle of the sexes: An examination of male and female cyberbullying. *International Journal of Cyber Criminology, 6*(1), 904–911.

McGurrin, D., Jarrell, M., Jahn, A., & Cochrane, B. (2013). White-collar crime representation in the criminological literature revisited, 2001-2010. *Western Criminology Review, 14*(2), 3–19.

McMillan, R. (2012). Is anti-virus protection a waste of money? Retrieved from https://www.wired.com/2012/03/antivirus/

Miethe, T.D., McCorkle, R.C., & Listwan, S.J. (2007). *Crime profiles: The anatomy of dangerous persons, places, and situations.* Los Angeles, CA: Roxbury.Minnaar, A. A. (2013). Editorial: Information security, cybercrime, cyberterrorism and the exploration of cybersecurity vulnerabilities. *Southern African Journal of Criminology, 26*(2), 1–4.

Mohamed, D. (2013). Combating the threats of cybercrime in Malaysia. *Computer Law and Security Review, 29*(1), 66–76. doi: 10.1016/j.clsr.2012.11.005

National Crime Agency. (2017). Young cyber criminals motivated by peer respect and accomplishment. Retrieved from http://www.nationalcrimeagency.gov.uk/news/1068-young-cyber-criminals-motivated-by-peer-respect-and-accomplishment

Nycyk, M. (2016). The new computer hacker's quest and contest with the experienced hacker. *International Journal of Cyber Criminology, 10*(2), 92–109. doi: 10.5281/zenodo.163402/

O'Connell, B. (2011). FBI says white collar cyber crime tops 300,000 in '10. *Business Insider*. Retrieved from http://www.businessinsider.com/fbi-says-white-collar-cyber-crime-tops-300000-in-10-2011-3.

Payne, B. K. (2017). *White-collar crime: The essentials* (2nd ed.). Thousand Oaks, CA: Sage.

Payne, B. K., & Gainey, R. R. (2006). The criminal justice response to elder abuse in nursing homes. *Western Criminology Review, 7*(3), 67–81.

Payne, B. K., & Hadzhidimova, L. (in press). *Cybercrime and criminal justice: Exploring the Intersections*. International Journal of Criminal Justice Sciences.

Ponemon Institute. (2017). *2017 cost of data breach study.* Retrieved from https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-15763&S_PKG=ov58441

Security Magazine. (2012). Average business employee has 191 passwords. Retrieved from https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords

U.S. Department of Justice. (2017, December 14). I.T. specialist arrested for allegedly hacking into servers of north suburban company where he formerly worked as contractor. Retrieved from https://www.justice.gov/usao-ndil/pr/it-specialist-arrested-allegedly-hacking-servers-north-suburban-company-where-he.

U.S. Department of Justice. (2017, October 6). Oilpro.com founder sentenced to prison for hack into competitor's computer system. Retrieved from https://www.justice.gov/usao-sdny/pr/oilprocom-founder-sentenced-prison-hacking-competitor-s-computer-system.

U.S. Department of Justice. (2017, August 25). Operator of global crime unit pleads guilty to access device fraud and aggravated identity theft. Retrieved from https://www.justice.gov/usao-edny/pr/operator-global-cybercrime-marketplace-pleads-guilty-access-device-fraud-and-aggravated.

U.S. Department of Justice. (2015, August 25). CMU student pleads guilty to designing malware, selling it on hacker forum. Retrieved from https://www.justice.gov/usao-wdpa/pr/cmu-student-pleads-guilty-designing-malware-selling-it-hacker-forum.

Sinrod, E. J., & Reilly, W. P. (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws. *Santa Clara Computer and High Technology Law Journal, 16*(2), 177–232. Retrieved from http://www.sinrodlaw.com/cybercrime.doc

Steffensmeier, D., Schwartz, J., & Roche, M. (2013). Gender and twenty-first-century corporate crime: Female involvement and the gender gap in Enron-era corporate frauds. *American Sociological Review, 78*(3), 448–476. doi: 10.1177/0003122413484150

Steffensneier, D. (1989). On the "causes" of white-collar crime. *Criminology, 27*(2), 345–358. doi: 10.1111/j.1745-9125.1989.tb01036.x

Sutherland, E. (1949). *White collar crime*. Austin, TX: Holt, Rinehart & Winston.

Sutherland, E. (1940). White-collar criminality. *American Sociological Review, 5*(1), 1–12. doi: 10.2307/2083937

Tcherni, M., Davies, A., & Lizotte, A. (2016). The dark figure of online property crime. *Justice Quarterly, 33*(5), 890–911. doi: 10.1080/07418825.2014.994658

Weisburd, D., & Waring, E. (2001). White-collar crime and criminal careers. New York, NY: Cambridge University Press.

About the Author

Brian K. Payne, Ph.D. is the vice provost for academic affairs and professor of sociology and criminal justice at Old Dominion University. He received his PhD in criminology from Indiana University of Pennsylvania. His research interests are in the areas of cybercrime, electronic monitoring, and white-collar crime. He has published eight books and more than 160 journal articles. His research appears in outlets such as *Justice Quarterly*, *Crime and Delinquency*, *Criminology and Public Policy*, *Deviant Behavior*, and *Criminal Justice Studies*.