THE INTERNET: EXACERBATING WHITE-COLLAR CRIME

Stephen L. Baglione
Robert Diemer
Saint Leo University

Thomas Zimmerer
University of South Florida

ABSTRACT

According to more than 600 seasoned law enforcement professionals from all agencies (i.e., federal, state, sheriff, and municipal), the Internet has become a conduit for white-collar crime, making it easier to perpetrate. These law enforcement professionals believe international and domestic cooperation by government and business must be harnessed to ensure the Internet continues to flourish free of these white-collar criminals. Otherwise, consumers and businesses may be reluctant to use the Internet for e-commerce. And, as the current collateralized mortgage debt crisis illustrates, fear can paralyze our economic system here and abroad.

Keywords: Internet crime and Internet white-collar crime

INTRODUCTION

The Internet may prove to be the most important technological advance in the past decades. Through the Internet, our educational system can provide students of all ages with access to knowledge housed globally. Individuals and families can access information about health and wellness information that may result in rapid response to illness and positive proactive lifestyle changes. The Internet has created a communication vehicle that allows individuals to gain a greater understanding of the world. It is now possible to view images of the world through our computer screens. Citizens of the world can now communicate with limited interference and secondary interpretation.

On a practical operational level, the technology of the Internet continues to evolve in both stability and dependability. For some segments of our population, the Internet is the conduit of primary information and communication. The Internet links individuals as well as businesses, governmental units, and non-profits. Internet usage has increased 362 percent from 2000 to 2009 (www.internetworldstat.com, 2009). Currently 22 percent of the world actively participates online (www.internetworldstat.com, 2009), including over 223 million American users (Central Intelligence Agency, 2008). United States retail e-commerce sales for the fourth quarter of 2008 were $31.7 billion, an increase of .7 percent from the previous year, although still a small portion of total sales at 3.5 percent (United States Census Bureau, 2009). A recent study indicates that 48 percent of Internet users purchased online using a credit card (Pew Center, 2008). The Internet is indispensable for consumer-to-business and business-to-business transactions. Business-to-business e-commerce is now the primary way of interacting to obtain price quotes, place orders, and even track inventory locations. Websites are an indispensable marketing tool conveying ordering information, company history and policies, in-depth product and service descriptions, achievements, and more. Small businesses now can provide constant customer service internationally through a single website.
Despite the positive aspects of the Internet, the largest negative is that criminals have also recognized the Internet’s power. Fraud cybercrime losses increased almost 11 percent in 2008 to $264 million. More than 275,000 complaints alleging online fraud crimes were reported with 72,000 referred to law enforcement nationally (Internet Crime Complaint Center, 2009). In comparison, the U.S. population is growing at less than 1 percent (Central Intelligence Agency, 2009), and violent and property crime both decreased .7 percent and 1.4 percent, respectively in 2007 (FBI.gov, 2009). This number is small in comparison to the estimated $300 to $660 billion cost of white-collar crime annually (Kane & Wall, 2006), but will continue growing as the Internet does. Some cybercrimes can continue in perpetuity. The Conficker virus infected 15 million computers and continues to infect seven million annually (Markoff, 2010). Statistics are unavailable for white-collar crime committed using the Internet.

**REVIEW OF LITERATURE**

Global organized crime has migrated to Internet cybercrime (Williams, 2006). The government has found that traditional organized crime groups are working in foreign countries, which currently provide them with some protection from detection and prosecution. Furthermore, many loose-knit criminal organizations are morphing into “mafia” style groups (Network Security, 2008).

The Internet affords criminals the opportunity to commit fraud with anonymity making it difficult to actually identify the perpetrators, let alone arrest them. A major concern of U.S. law enforcement is that even when identified, it may be legal in the perpetrator’s country of origin. As an example, the Federal Bureau of Investigation (F.B.I.) suspected a Philippine national of spreading the malicious Love Bug virus in 2000 which affected 45 countries doing billions in damages; however, he was not prosecuted because the Philippines did not have cybercrime laws (Brenner & Schwerha, IV 2008). Thirty-four percent of perpetrators of Internet fraud crimes were from foreign countries (Internet Crime Complaint Center, 2009). Hardly anyone has been spared from receiving an e-mail from foreign nationals offering a substantial fee for helping to move large quantities of money internationally. An estimated 10,000 Nigerians engage in Internet fraud (Salu, 2004).

The Internet facilitates many types of white-collar crime. The ubiquitous phishing e-mails promise instant wealth or identify verification because, ironically, your financial account information was compromised over the Internet. Since many phishers pose as well-known institutions and retailers, this strikes at “the heart” of e-commerce trust. “By impersonating financial institutions, phishers can undermine the confidence that customers place in their financial institution’s electronic delivery channels, including call centers, card issuing, and home banking—potentially damaging the institution’s brand and reputation. Phishing can hamper an institution’s ability to attract and retain customers and slow the introduction and adoption of new, revenue-generating banking products and services” (Span, 2004, p. 42). Beyond financial losses, it can damage the institution’s ability to retain, attract, and expand business with customers. “More than three out of four (76%) consumers are experiencing an increase in spoofing and phishing incidents, and according to a recent national study, 35 percent are receiving fake e-mails at least once a week” (McCarrell, 2004, p. 14). Sixty-eight percent of respondents in a national study indicated concern about their credit card number being stolen online, which could erode trust in e-commerce (Pew, 2008). In a study of U.S. banking customers, 65 percent indicated they were less likely to use online banking services because of
online fraud, while 75 percent were less likely to respond to an e-mail from their bank because of online fraud (Wetzel, 2005). It is an international problem: three-quarters of respondents in the European Union reported fear of identity theft has stopped them from purchasing online (Acoca, 2008). Clearly, U.S. citizens are facing fraud on a global level and U.S. businesses are finding that a loss in customer confidence in Internet business is an extremely serious barrier to the continued potential growth of sales and revenues.

A recent survey of 600 IT security experts worldwide found half had suffered "large-scale denial of service attacks by a high level adversary like organized crime, terrorists or nation-state" (Baker et al., 2010 p. 4). Financial information is the most common target of cyber attacks. Twenty-four hours of downtime from an attack, according to respondents, costs an average of $6.3 million. Twice as many respondents believe their industry is more vulnerable than less. Forty percent expect a major attack in their industry this year. The global recession is making it worse. Two thirds believe security resources have reduced because of economic conditions. Fifty-five percent believe laws within their country are inadequate in deterring cyber attacks (Baker et al., 2010).

**United States Government Response**

Local law enforcement has difficulty enforcing laws from outside their specific jurisdiction (Spafford, 2008). Through one of the author’s extensive law enforcement experiences, he has found, it is difficult to determine which criminal justice agency should handle such an incident. What occurs is that local law enforcement, utilizing various investigative methods, lures the suspect to its jurisdiction in order to make the arrest. In other situations, investigators from local agencies or combination of local/state/federal agencies form joint task forces in order to increase their jurisdiction and investigative power. Depending on the crime, distance from the perpetrator's residence, and law enforcement interest, arrests and case closures can be slim and prosecution difficult. A recent case illustrates the problem: The U.S. Department of Justice (D.O.J.) charged 11 individuals with stealing 40 million credit and debit cards from nine major U.S. retailers; three are Estonian, three Ukrainian, two Chinese, one Belarusian, and one of unknown origin (Computer & Internet Lawyer, 2008).

For these reasons, it makes sense that an agency with broad powers and large geographic jurisdiction handle such incidents. This is where the D.O.J. plays an important role. D.O.J. is run by the U.S. Attorney and has jurisdiction to enforce federal laws within any U.S. state or territory. The agency responsible for enforcement in the D.O.J. is the F.B.I. This investigative agency with 12,500 special agents has been tasked with investigating white-collar crimes and crimes perpetrated via the Internet.

After the terrorist attacks on September 11, 2001, the F.B.I. became the lead criminal justice agency in investigating terrorism. From this responsibility, the F.B.I. developed a Cyber Division for the purposes of combating terrorism where the Internet and computer systems are both targeted (Siegel & Senna, 2005). In addition to the F.B.I.'s Cyber Division, several federal agencies joined together to form the Interagency Telemarketing and Internet Fraud Working Group to share information and to target and prosecute individuals committing Internet crimes. This task force is comprised mainly of agents from the F.B.I., Federal Trade Commission, Postal Inspection Service, Security and Exchange Commission, and the Secret Service (Siegle & Senna, 2005). The F.B.I. has also partnered with the National White Collar Crime Center, which includes law enforcement and regulatory agencies from the local, state, federal, and international
communities, to develop the Internet Crime Complaint Center (IC3), which monitors complaints involving Internet-related crimes (Internet Crime Complaint Center, 2009). Non-profit organizations have also joined the battle. The United States Internet Crime Task Force, Inc. is one such organization, a government-assisted agency that shares intelligence, assists victims, and monitors chat rooms for criminal activity (United States Internet Crime Task Force, Inc., 2008).

RESEARCH HYPOTHESES

The authors of this study surveyed law enforcement officers at all government levels on their perception of Internet and white-collar crime facilitated by the Internet. "White-collar crimes are categorized by deceit, concealment, or violation of trust and are not dependent on the application or threat of physical force or violence. Such acts are committed by individuals and organizations to obtain money, property, or services; to avoid the payment or loss of money or services; or to secure a personal or business advantage" (F.B.I., 2010). Bernie Madoff’s $50 billion Ponzi scheme is an example, although only tertiary to the Internet (Creswell & Thomas, 2009). The following hypotheses are proposed:

Hypothesis 1a: Law enforcement believes that the Internet has made white-collar crime easier for criminals;

Hypothesis 1b: Law enforcement believes that most white-collar crime involves the Internet;

Hypothesis 2a: Differences will not exist among agencies (i.e., federal, state, sheriff, or municipal) on whether the Internet has made white-collar crime easier for criminals;

Hypothesis 2b: Differences will not exist between those currently working white-collar crime and those not on whether the Internet has made white-collar crime easier for criminals; and

Hypothesis 3: Law enforcement believes specific white-collar crimes facilitated by the Internet is growing (e.g., identity theft, credit card/ATM fraud, bank fraud, and securities/investment fraud).

RESEARCH METHODS

The authors’ survey incorporated a Literature Review and the knowledge of two law enforcement officers, each with over 25 years of investigative experience, including one of the authors. Through multiple iterations, a rough draft was developed. It was modified repeatedly during the pretest, a protocol analysis with 12 law enforcement officers. The survey included two sections: questions on white-collar crime and the Internet and demographics. The survey was administered nationally through the Multi-Jurisdictional Counter Drug Taskforce Training Center, one of the largest law enforcement training facilities in the country. The authors of this study believe response rates were almost 100 percent. Additional, it was disseminated throughout Florida to local and state law enforcement agencies.

The data were analyzed in SPSS. Data were recorded by one person and reviewed for mistakes by another. Frequencies were then examined to ensure no data outside the range of feasible answers. One-sample t-tests were tested against the scale midpoint of four, with the
anchors being one (strongly agree) to seven (strongly disagree). Analysis of Variance was conducted to determine whether differences exist by law enforcement agency (i.e., federal, state, sheriff, and municipal) and whether the law enforcement agent currently working white-collar crime influences the dependent variables: the Internet has made white-collar crime easier for criminals and most white-collar crime involves the use of the Internet. Pairwise deletion was used (i.e., deleted by individual by question).

Based on the hypotheses, the mathematical models tested are:

\[ E(Y_1) = \alpha + \beta_1 (X_1) + \beta_2 (X_2) + \beta_3 (X_1 \times X_2) \]
\[ E(Y_2) = \alpha + \beta_1 (X_1) + \beta_2 (X_2) + \beta_3 (X_1 \times X_2) \]

where \( Y_1 \) is law enforcement belief that the Internet has made white-collar crime easier for criminals; \( Y_2 \) is law enforcement belief that most white-collar crime involves the use of the Internet. Both \( X_1 \) and \( X_2 \) are categorical variables. The first is the agency employing the law enforcement agent: federal, state, sheriff, or municipal. The four law enforcement agencies were coded as different categories. The second is whether the law enforcement officer currently works white-collar crime (two categories: yes and no). The hypotheses predict that \( \beta_1, \beta_2, \) and \( \beta_3 \) will not be significant for either dependent variable. Beliefs will be universal across law enforcement.

RESULTS

Six-hundred and one surveys were collected. None were unusable due to incomplete data or failure to take the exercise seriously (n=601). The sample represents seasoned law enforcement officers. They averaged more than 12 years of experience, which is high, considering law enforcement officers may retire after 20 years. All levels of law enforcement are represented: federal (8%), state (12%), sheriff (38%), and municipal (43%). Ninety-one percent of the agencies employing our respondents work white-collar crime, varying from little to extensive. Seventy-nine percent of the agencies employing our respondents specifically work Internet white-collar crime, again from little to extensive. Twenty-one percent of respondents work white-collar crime, with nine percent working Internet white-collar crime.

The authors of this study then tested all respondents on their impression of the Internet and white-collar crime (one-sample t-tests). The Internet, according to respondents, is involved with most white-collar crimes \((t(577)=-20.48, p=.000, M=3.25)\). The sample also strongly agrees that the Internet has made white-collar crime easier \((t(590)=-12.82, p=.000, M=2.39)\). (Scale is one strongly agree to seven strongly disagree.) This supports hypotheses 1a and 1b.

The ANOVA results indicate that the agency law enforcement officers work for and whether they work white-collar crime does not influence whether they believe the Internet makes white-collar crime easier or that most white-collar crime involves the Internet (Tables 1 and 2). This partially supports hypotheses 2a and 2b. The ANOVA results, along with one-sample t-test results, offers support for hypotheses 2a and 2b.
The authors of this study identified four categories of white-collar crime that are prevalent on or facilitated by the Internet: identify theft, credit card/ATM fraud, bank fraud, and securities/investment fraud. A startling 89 percent believe identity theft will increase and, equally disturbing, 83 percent believe credit card/ATM fraud will increase in the next three years (Table 3). About half believe bank fraud and securities/investment fraud will grow in frequency over the next three years. Five percent or less of respondents envisions these white-collars crimes decreasing in the next three years. This supports hypothesis three.

The Internet facilitates white-collar crime, and its use as a conduit for crime is growing exponentially. Its worldwide reach makes, according to respondents, global cooperation imperative, \( t(586) = -17.29, p < .000, M = 2.83 \), where one is strongly agree and seven strongly disagree), but valuable resources are being diverted to terrorism \( t(584) = -11.79, p < .000, M = 3.26 \), which is leading to the startling conclusion that law enforcement at all levels is losing the war on white-collar crime \( t(595) = 12.673, p < .000, M = 4.77 \). This sentiment has been echoed by others (Acoca, 2008; Broadhurst, 2006). Cybercrime erodes our legal system’s foundation of national law because the Internet is boundless. Cooperation must include some standardization.
about what constitutes a crime and how it will be handled (Brenner & Schwerha IV, 2008). The problem will only exacerbate. Law enforcement predicts white-collar crime, such as identify theft and credit card fraud which are prevalent on or facilitated by the Internet, will increase dramatically in the next three years, further substantiating the need to curtail this growing plague.

As the Internet becomes further meshed in the commerce and personal lives of all Americans, it is critical for twenty-first century commerce to succeed in protecting this new and vital business tool. Nations that do not rely on the Internet will be left behind in the global competition that dominates, and will continue to dominate our global economy. It links companies and countries globally, and is becoming an indispensable commerce medium. Its elimination or diminishment would sharply curtail international commerce. Dire predictions may seem to be hyperbole, but if individuals lose trust in the Internet as a way to communicate and consummate trade, global Internet commerce may drop dramatically. It is analogous to the global credit crisis infecting companies worldwide from American collateralized mortgage debt, where a downward spiral in the confidence of a firm’s ability to repay a loan is causing many institutions not to lend. Don Brackman, director of the National White Collar Crime Center, believes, “in a technology-driven global market, the inability of consumers to distinguish between legitimate and fraudulent activities poses a serious threat to our economy” (National White Collar Crime Center, 2010, p. 21).

In January 2010, the Pentagon simulated a “cyber attack aimed at paralyzing the nation’s power grids, its communications systems or its financial networks” (Sanger, 2010, p. A1). The results were disheartening: the attacking country could not be identified, and Pentagon leaders realized they lacked the legal authority to counterattack. A similar attack on Google and 30 other companies had just been perpetrated, with “footprints” traced to China.

LIMITATIONS OF THIS STUDY

This study is cross sectional, although the authors did sample from law enforcement professionals with varying degrees of experience. Due to the current lack of published data in this criminal area, the authors could not corroborate the paper’s findings with actual crime statistics since the categories used here are subsumed under larger categories. Many of the law enforcement personnel who participated in the research viewed white-collar crime from the somewhat limited perspective of their duties and responsibilities. The researchers suspect that due to the nature of this type of criminal activity where the perpetrator is seldom within the specific jurisdiction of law enforcement and arrests are rare, and there is a high level of frustration connected with the pursuit of white-collar criminals.

RECOMMENDATIONS FOR FUTURE RESEARCH

Future research should include law enforcement professionals from outside North America. Since the Internet is boundless, these results should hold elsewhere. Finally, the study should be done longitudinally with the same law enforcement professionals surveyed throughout their careers. Future research will need to study in greater detail the international implications of white-collar crime. The Internet has created a tool that allows political and economic opponents of the United States to operate with virtual immunity from prosecution. Future research will need to explore in detail the serious international policy issues regarding this gaping hole in law enforcement.
REFERENCES


About the Authors:

Stephen L. Baglione is Department Chair and Professor of Marketing and Quantitative Methods at Saint Leo University in Florida. He received his doctorate in Marketing from the University of South Carolina. Dr. Baglione has authored or co-authored over 70 refereed journal and proceedings articles for publications.

Robert J. Diemer is a Professor and currently serves as the Director of Graduate Studies in Criminal Justice for Saint Leo University, President of The Society for Public Safety and retired as a career law enforcement officer with over 28 years of varied investigative experience.

Thomas W. Zimmerer currently serves as an adjunct professor in the Center for Entrepreneurship at the University of South Florida. He received his doctorate from the University of Arkansas. Dr. Zimmerer has published 10 textbooks and has authored or co-authored over 200 articles and professional papers.
### APPENDIX

#### SURVEY INSTRUMENT

**SECTION I**

Please place a check in the column that you feel best reflects your degree of agreement with each statement.

<table>
<thead>
<tr>
<th>Your Degree of Agreement with Each Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Strongly Agree</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Law enforcement (all levels) is winning the war against white-collar crime?</td>
</tr>
<tr>
<td>2) Law enforcement at a federal level understands how to combat white-collar crime?</td>
</tr>
<tr>
<td>3) Law enforcement at a state level understands how to combat white-collar crime?</td>
</tr>
<tr>
<td>4) Law enforcement at a local level (sheriff’s offices and municipal police departments) understands how to combat white-collar crime?</td>
</tr>
<tr>
<td>5) Law enforcement at a federal level is allocating the necessary resources to combat white-collar crime?</td>
</tr>
<tr>
<td>6) Law enforcement at a state level is allocating the necessary resources to combat white-collar crime?</td>
</tr>
<tr>
<td>7) Law enforcement at a local level (sheriff’s offices and municipal police departments) is allocating the necessary resources to combat white-collar crime?</td>
</tr>
<tr>
<td>8) The Internet has made white-collar crime easier for criminals?</td>
</tr>
<tr>
<td>9) Most white-collar crime involves the use of the Internet?</td>
</tr>
</tbody>
</table>
10) White-collar crime has grown dramatically since the terrorists' attacks of September 11, 2001?

11) Laws passed in the United States after September 11, 2001 to combat terrorism have been helpful in combating white-collar crime?

12) The war on terrorism has diverted resources away from investigating white-collar crimes?

13) Combating white-collar crime requires greater cooperation among nations?

14) Which agency should have primary investigative responsibility for Internet white-collar crimes (please check all that apply)?
   ___ Federal
   ___ State
   ___ Sheriff
   ___ Municipal
   ___ International (law enforcement outside the United States)

Please place a check mark (☑) in the column indicating whether you believe specific types of white-collar crime will increase, decrease, or remain unchanged (i.e., the number of occurrences) over the next three years.

<table>
<thead>
<tr>
<th>Type of White-collar Crime</th>
<th>Increase or Decrease in the Number of Occurrences of Types of White-collar Crime Three Years from Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank Fraud</td>
<td></td>
</tr>
<tr>
<td>Check Fraud</td>
<td></td>
</tr>
<tr>
<td>Counterfeiting/Forgery</td>
<td></td>
</tr>
<tr>
<td>Credit-card/ATM Fraud</td>
<td></td>
</tr>
<tr>
<td>Embezzlement</td>
<td></td>
</tr>
<tr>
<td>Crime Type</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Identify Theft</td>
<td></td>
</tr>
<tr>
<td>Money Laundering</td>
<td></td>
</tr>
<tr>
<td>Postal Fraud</td>
<td></td>
</tr>
<tr>
<td>Securities/Investment Fraud</td>
<td></td>
</tr>
<tr>
<td>Shoplifting</td>
<td></td>
</tr>
<tr>
<td>Telephone/Telemarketing Fraud</td>
<td></td>
</tr>
</tbody>
</table>
SECTION II

The following questions are for classification purposes only. All information will be combined. Individual responses will remain anonymous.

1) What type of agency do you work for (please check only one):
   ____ Federal  ____ State
   ____ Sheriff  ____ Municipal

2) Your agency’s nationality:
   ____ United States  ____ Canadian
   ____ International (Law enforcement outside the United States)

3) How many years have you worked in law enforcement? ____ Years

4) Does your agency currently work white-collar crimes?
   Not at all  Extensive
   1 2 3 4 5 6 7

5) Do you currently work white-collar crime?  ____ Yes  ____ No

6) How many years have you worked white-collar crime? ____ Years (if zero, please skip to question 8)

7) Have you ever (current or past) worked full-time on white-collar crime?
   ____ Yes  ____ No

8) On average, how many hours a week do you work white-collar crime? ____ Hours

9) Does your agency currently work Internet white-collar crime?
   Not at all  Extensive
   1 2 3 4 5 6 7

10) Do you work Internet white-collar crime?  ____ Yes  ____ No

11) How many years have you worked Internet white-collar crime? ____ Years