8-2010

Old Wine in New Bottles: Investigating how Information Technology is Enabling "Old Criminals" to access "New Venues"

Jason Thatcher
Clemson University, jason.b.thatcher@gmail.com

Terry Leap
Clemson University

Ryan Wright
University of San Francisco

Old Wine in New Bottles: Investigating how Information Technology is Enabling "Old Criminals" to access "New Venues"

Panel Proposal

ABSTRACT

The purpose of this panel it is to evoke a discussion that examines how cybercriminals translate methods for stealing data, identities, and money from individuals and organizations from the face-to-face world to an information technology (IT) enabled environment. Specifically, this panel will: 1) give members of the audience an opportunity to learn about contemporary theories of the psychology behind white collar crime (e.g, securities fraud, identity theft, phishing), 2) engage the audience in a discussion of how IT plays a role in enabling transfers of "criminal behavior" from traditional contexts to online contexts, and 3) to review challenges and opportunities for researchers seeking to investigate IT-enabled criminal behavior.

Keywords

Social Engineering, White Collar Crime, Phishing, Online Fraud, Computer Crime, Electronic Evidence

PANEL TOPIC AND TARGET AUDIENCE

Our discussion of White collar cybercrime will be facilitated by Dr. Jason Thatcher. White collar cybercrime is a "variety of frauds, schemes, and commercial offenses by businesspersons, confidence men, and public officials. It includes a broad range of nonviolent offenses that have cheating as their central element. Consumer fraud, bribery, and stock manipulation are examples (Business Dictionary, 2009)." The panel's audience will be of interest to IS security researchers, interested in applying contemporary theories and methods to studying cybercrime. Specifically, the panel will review two sets of IT-enabled crimes: White Collar and Identity Theft.

Dr. Terry Leap, author of Dishonest Dollars: The Dynamics of White-Collar Crime, will review a model that describes the motivations of the individual perpetrator. His work suggests that cyber-criminals commit crimes out of rational choice, weighing the perceived costs and benefits of each criminal act (rational choice theory). This theory also recognizes that influences such as personality disorders, utility for money, individual impulsiveness, and propensity for risk affect this cost-benefit calculus. In terms of the social context, his model suggests that organizations and societies both facilitate and proscribe criminal behaviors. For example, some organizations are crime coercive (e.g., organized crime), whereas most organizations are, to varying degrees, crime facilitative. Organizational influences include job flexibility, decentralized structures, ethical policies, the multinational expansion of organizations, and security systems. Society also encourages and discourages white-collar crime through the degree that it places on individual wealth, its views on corruption and dishonesty, and the laws it enacts.

Dr. Leap will outline various primary and facilitative white-collar crimes that information technology enables. Primary crimes are the end-result of criminal activities (e.g., securities fraud). Facilitative crimes include mail and wire fraud (especially computer crimes), conspiracy, money laundering, tax evasion, and perjury. The crimes that perpetrators decide to commit are usually a function of their knowledge, skills, and abilities as well as their "specialized access" to victims and assets. He will discuss the aftermath of IT-enabled white-collar criminals by examining the individual, organizational and societal costs of crime. These costs include economic, psychological, and social costs. Many white-collar crimes, however, are probably not detected, so the effects of such crimes are difficult to assess.

Dr. Ryan Wright will outline different ways that IT-enables content-related and contextual deception tactics. Content-related tactics refers to cues that omit or distract consumers from relevant information that allows them to fully understand the implications of responding to a phishing email. Contextual related tactics refers to falsely representing key elements of the message such as the source or context for taking action. He will then discuss ways that IT-enables white-collar criminals to use such tactics to deceive, steal, and engage in malfeasance. Through his review of deception tactics, Dr. Wright will illustrate why consumers fall prey to phishing tactics.

Through reviewing contemporary thinking on white collar crime and how it is enabled by information technology, we hope to stimulate new thinking about how to detect and contain online criminals among IT scholars.

PANEL OBJECTIVE

The purpose of the panel is threefold: 1) to give the members of the audience an opportunity to review state-of-the-art theory and innovative ideas related to cybercrime, 2) to start to engage the IS community in the examining different ways to understanding how and why cybercrime takes place, for example, the majority of IS research on phishing examines webpages, not the psychology of the criminal or victim, and 3) to present alternative theoretical approaches to studying cybercrime in IS, in order to stimulate a discussion that will encourage the audience to consider different ways to approach studying crime and to extend research on cybercrime from the enabling technology to also the psyche of the criminal.

Disseminating new approaches to studying cybercrime is extremely important. Although we are all well-aware of IT-enabled crimes such as Enron, relatively little IS research has examined the "psychology" of the white collar cybercriminal nor "manipulated deceptive tactics" employed by such cybercriminals. Further, our panel will stimulate thinking on the relative value of case study based (e.g., examining prominent white collar criminals) vs. experiment based (e.g., examining technology enabled deception tactics efficacy) in informing our thinking about cybercrime. We believe that this discussion will be helpful in stimulating thinking of individual faculty members and departments that are working to identify the best approaches to study cybercrime.

PANEL FORMAT

The panel presentation will be consistent of three distinct segments. First, the moderator Dr. Thatcher will introduce the panelist and outline the agenda for the panel presentation (5 minutes). Second, Dr. Leap will present a review of a general model of white collar crime and how IT enables such crimes. (15 minutes) Next, Dr. Wright will discuss IT enabled deception tactics and the psychology behind their effectiveness (10 minutes. Finally, the panel will be opened to discuss questions related to theories and methods employed to study IT-enabled white collar crime. The questions may include the following:

1. How do you translate traditional theories of white collar criminal behavior to cybercrime? How does the psychology of white collar criminals influence their choice of tactics to commit cybercrime?
2. How can researchers conduct case based research examining white collar cybercriminals?
    a. How to surmount challenges of gaining access to white-collar criminals?
    b. Methods and challenges to conducting case based examinations of white-collar criminals?
    c. How to examine means by which information technology enables white collar crime?
    d. What is the role of archival data in researching white collar cybercrime?
3. How can researchers conduct laboratory experiments examining white collar cybercrime?
    a. Problems and pitfalls associated with winning institutional review board approval for experiments on cybercrime?
    b. How to emulate social engineering tactics employed in phishing and other white collar crime in experiments?
    c. How to capture "criminal" and "victim" behavior in online environments?
    d. What is the role of confederates when researching white collar cybercrime?

As typical with panel presentation, finally, the moderator will open the floor up to the audience for questions to the panel regarding white collar crime and cybercrime (30 plus minutes).

BIOS OF THE PANELISTS

Facilitator: Jason Thatcher is an Associate Professor in the Department of Management at Clemson University. He holds B.A.'s in History (Cum Laude) and Political Science (Cum Laude) from the University of Utah as well as a M.P.A. from the Askew School of Public Administration and Policy and a Ph.D. in Business Administration from the College of Business at Florida State University. **Dr. Thatcher's research examines the influence of individual beliefs and characteristics on adaptive and maladaptive uses of information technology.** He also studies strategic and human resource management issues related to the effective application of information technologies in organizations. His work appears in MIS Quarterly, Journal of Management Information Systems, IEEE Transactions on Engineering Management, American Review of Public Administration, Organizational Behavior and Human Decision Processes as well as the Journal of Applied Psychology.

Terry Leap is a full professor at Clemson University. Dr**. Terry Leap's** research interests are in the areas of human resource management, ethics, and deviance in organizations. Professor Leap is the author of **Dishonest Dollars: The Dynamics of White-Collar Crime** (Cornell University Press, 2007), **Tenure, Discrimination, and the Courts** 2nd ed.(Cornell University Press, 1995). He is also author of **Collective Bargaining and Labor Relations**, 2nd ed. (Prentice-Hall, 1995) and **Personnel/Human Resource Management**, 2nd ed. (Macmillan, 1993). In addition, Professor Leap has published articles in the Academy of Management Journal, Harvard Business Review, MIT Sloan Management Review, Journal of Management, Industrial Relations, Human Relations, Industrial and Labor Relations Review, and others. He served as chair of the Department of Management from 1999-2006. Dr. Leap currently teaches graduate and undergraduate courses in human resource management and white-collar crime.

Ryan Wright is an assistant professor at University of San Francisco. He holds a Ph.D. from Washington State University in Management Information Systems. Ryan's research interests take a behavioral approach to understanding how current technologies can be used to enable secure and efficient e-business transactions. **He has just completed a series of field based experiments examining deception and cybercrime that are starting to appear in journals such as the *Journal of MIS*, *Group Decision and Negotiation* and other peer-reviewed journals.** Ryan has also presented his research at leading conferences such as the ICIS, HICSS and AMCIS. Also, Ryan has won university-wide and college-wide awards in recognition of his classroom excellence. In addition to academic achievements, Ryan's professional experience includes tenure as CTO of a successful startup, time in management at Amoco Oil (now BP Amoco), consulting projects for the US Department of Commerce and expert testimony for the Attorney General's Office of Washington State.

EQUIPMENT NEEDED

Basic audio-visual equipment will be required to present the review state-of-the-art practices in and innovative ideas related to master's level education. This includes a projector and a screen.