Check for updates

Crime & Delinquency
1–20
© The Author(s) 2022
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/00111287221092713
journals.sagepub.com/home/cad
SAGE

Risk Avoidance Behavior on Darknet Marketplaces

Christian Jordan Howell[1], David Maimon[2], Robert C. Perkins[2], George W. Burruss[1], Marie Ouellet[2], and Yubao Wu[2]

Abstract

The current study employs a quasi-experimental design to test the efficacy of situational crime prevention (SCP) in understanding risk avoidance behavior in a darknet environment. Specifically, we deployed a web scraper to extract data from a popular darknet market. We then used these data to assess change in vendors and customers' behavior following the deliverance of a warning message from the market administrator regarding the former market administrator's intention to scam market participants. In the one-month following the message, vendors posted fewer advertisements and customers spent less and made fewer transactions on the marketplace. These findings expand the scope of SCP and provide evidence for Hutchings and Holt's notion that darknet markets can be disrupted by means of gossip.

Keywords

situational crime prevention, cyber crime, darknet markets, risk avoidance, offender decision making

[1]University of South Florida, Sarasota, USA
[2]Georgia State University, Atlanta, USA

Corresponding Author:
Christian Jordan Howell, University of South Florida, 8350 N Tamiami Trail, Sarasota, FL 34243, USA.
E-Mail: cjhowell@usf.edu

Introduction

Inquiry into the techniques offenders use to avoid the risks of detection by law enforcement and victimization by adversaries dates back to the 1930's with Sutherland's (1937) study on professional thieves. He found successful thieves tended to select jobs unlikely to result in arrest or leave incriminating evidence. Such thieves also employed predetermined strategies to avoid conviction when apprehended by the police. Multiple scholars have since expanded upon Sutherland's classic work and have garnered insight into how different types of offenders comply with the rationale proposed by rational choice theoreticians (Jacques & Reynald, 2012), and avoid risks specific to their trade (e.g., Jacobs, 1993; Johnson & Natarajan, 1995; Weisburd et al., 2006; Wright & Decker, 1996). For example, Atlas (1990) and Jacques and Reynald (2012) employed theoretical constructs from situational crime prevention (SCP) (Clarke, 1995) to better understand how offenders apply risk avoidance techniques to avoid detection and their own victimization. They found offenders reverse engineer the situational techniques meant to prevent the occurrence of crime to instead reduce the risks associated with police apprehension and victimization. These scholars suggest the decision to apply risk avoidance techniques goes beyond weighing the risks and rewards of the specific action in question; rather, risk avoidance involves an interactional social process that relies on informal information channels and assessing those channels' credibility to determine the best course of action while initiating a criminal event (Dickinson & Wright, 2015).

Although past criminological research has reported that gossip from informal communication channels alters offenders' decision to offend (Dickinson & Wright, 2015; Jacques & Reynald, 2012), this research has been unable to establish causality due to the nature of the research designs employed. Moreover, while this past research focused on offenders' decisions to initiate offline crimes such as drug dealing and auto theft, the relationship between gossip relayed through informal communication channels and offenders' decision-making is less clear in the context of cyberspace.

In recent years, scholars have attempted to fill this gap in the literature. For example, Maimon et al. (2021) conducted two experiments using a sample of active hackers and found gossip relating to law enforcement operations reduces the frequency and severity of reoffending. Notably, it is unclear how these findings generalize to other forms of offenses carried out in cyberspace, such as purchasing and selling illicit products on darknet markets. However, scholars, such as Hutchings and Holt (2017), have theorized that darknet markets can be disrupted through the administration of gossip, a phenomenon referred to as "lemonization." Thus, drawing on the assumption that cybercriminals engage in risk avoidance behavior when exposed to gossip warning them of risks (Maimon et al., 2021), we assess Hutchings and Holt's (2017) notion that darknet markets can be disrupted (or lemonized) by means of gossip. Specifically, we assess whether a gossip message, warning users of an exit scam, altered the behavioral patterns of those users (i.e., customers and vendors) on the market.

To establish whether this form of gossip triggers risk avoidance, we employed a one-group pretest-posttest quasi-experimental design (Campbell & Stanley, 1963, p.47). To gather data for the study, we developed and deployed a web scraper to extract information from the darknet market Silk Road 3.1 on a weekly basis throughout 2019. During the data collection process, the administrator of the market posted a warning message directly to the market's forum and on other darknet platforms warning users that a former administer was planning to scam market participants. Providing support for the SCP framework and demonstrating the importance of informal communication channels in eliciting behavioral change, we found vendors posted fewer advertisements and customers reduced the amount of money spent and the number of transactions made on the market upon receiving the warning message. Migration from the market, as we will discuss in more depth below, demonstrates the effectiveness of "lemonization" as a proactive disruption tactic.

Theoretical Background

Rational Choice and Situational Crime Prevention

The rational choice perspective is an economic based model that suggests if for a given person the expected utility of an act (either legal or illegal) is greater than the expected utility of other alternatives, the person will resume the act (Becker, 1968). Adopting the rational choice model yet acknowledging the ineffectiveness of the criminal justice system to detect, punish, and prevent crime, Jeffery (1971) and Newman (1972) were working in the early 1970s toward devising environmental solutions for crime reduction. Jeffery (1971) published *Crime Prevention Through Environmental Design*, which argued the criminal justice system should be more proactive in its approach to curtail criminal events from occurring. More specifically, he suggested the abandonment of punishment and treatment philosophies in favor of a preventative approach geared toward manipulating the physical environment conducive to crime. Shortly thereafter, Newman (1972) coined the term "defensible space," which argued that crime can be mitigated through environmental design. For example, grouping housing units in a fashion that facilitates surveillance, establishes certain pathways for movement, and defines certain areas of activity, which, in turn, leads residents to adopt territorial attitudes and create self-policing measures. These social and architectural alterations combine to decrease opportunities conducive to crime.

Clarke, in continuation of the event-based perspective to crime reduction, developed SCP. In essence, this framework attempts to curtail crime by manipulating the specific situational characteristics conducive to criminogenic engagement (Clarke, 1980; Welsh & Farrington, 2009). The main premise behind SCP states that offenders operate with agency: crime is a choice that can be altered through decreasing the rewards and increasing the pains associated with the event (Clarke, 1980). Although some level of rationality is assumed, SCP contends that offenders operate with bounded rationality, "a decision-making process in which offenders weigh only a few aspects of a limited number of alternatives and ignore the rest" (Jacobs & Wright, 2010, p. 1741). Unlike most dispositional theories of crime, SCP is especially useful in providing practical efforts to reduce offending. These techniques are laid out by Clarke and his colleagues (Clarke, 1995; Cornish & Clarke, 2003), and fall into one of five categories: increase the efforts, increase the risk, reduce the rewards, reduce provocations, and reduce excuses.

Similar to the way SCP techniques are used by law enforcement and potential victims to prevent crime, several scholars suggest that criminals also adopt these techniques to avoid police apprehension and their own victimization (Atlas, 1990; Jacques & Reynald, 2012). For example, Atlas (1990) noted that offenders use defensible space techniques to survey other people approaching the area. Through this strategy, criminals can create communication channels, warn others when law enforcement is approaching, and even hinder law enforcement efforts all together. Through physical alterations such as boarded windows, peepholes, and reinforced doors, criminals use defensible space techniques to create "offensible space." Thus, criminals can reverse engineer classic crime reduction techniques to gain the advantage over law enforcement and avoid personal risk. More recently, Jacques and Reynald (2012) found drug dealers use a range of prevention-oriented techniques to reduce their likelihood of apprehension and victimization. Examples of these techniques include intermittent selling, utilization of stash spots, customer screening, avoidance in carrying paraphernalia, and the use of consistent pricing. According to these scholars, "by increasing the efforts or risks of victimizers and law enforcement officials, and also by reducing their rewards, provocations, and excuses, adversarial behavior is reduced." (p. 286).

Information sharing between criminals is key in their efforts to alter environmental and situational factors that may result in their own arrest or victimization. For example, Sutherland (1937) discussed how professional thieves would share information related to target selection and police activity to avoid risks (e.g., detection and sanction) and maximize gains (e.g., monetary earnings). Moreover, Dickinson and Wright (2015) conducted a series of in-depth interviews with active drug dealers and found that offender decision-making and risk avoidance behavior is an interactional social process largely influenced through informal communication. More specifically, criminals rely on gossip to avoid police detection and victimization by employing the informal communication channels available to those operating in this logistical capacity. Importantly, research on intrapersonal communication has long recognized people are more likely to have faith in messages delivered by credible sources (Hovland & Weiss, 1951). Once offenders hear about a conveyed threat (e.g., arrest or victimization), they often implement self-protection measures, such as reducing the frequency and severity of the criminal acts in which they are engaged (Moeller et al., 2016).

Given the apparent success of SCP in reducing criminal incidents in the physical world, it stands to reason that cybercrime incidents can also be reduced through cyber-environmental alterations. Indeed, a large body of literature exists across disciplines that demonstrate the utility of SCP in cyberspace (see Howell (2021) for a detailed overview). Moreover, and much like offenders in the physical world, cyber offenders have demonstrated an uncanny ability to reverse engineer the situational crime prevention tactics meant to curtail crime to evade risk in a manner consistent with the notions set forth by Jacques and Reynald (2012) and Dickinson and Wright (2015). For example, Holt et al. (2008) examined how consumers of sex work use open-web forums to avoid the risk of detection. One forum post reads:

> “If anyone attempts to use Kenney park, be advised that I saw at least 3 officers doing foot patrol walking through woods. [I] Askd [sic] one of the officers (since I was there, sitting on my hood eating a late lunch) and he said the staties are going to be regularly patrolling the park and they will be attempting to have a walking a patrol hitting the spot. . .to clean things up.”

In this example, the forum is used to establish communication channels and warn other members about law enforcement activity. Offenders use these anonymous channels to avoid being arrested in the physical world (also see Aldridge & Askew, 2017).

Risk Avoidance in Darknet Markets

In a similar manner, offenders utilize darknet markets to avoid police detection and reduce susceptibility to victimization. Access to the darknet, and illicit markets existing on the darknet (such as Silk Road 3.1), requires the use of special software such as The Onion Router (Tor). Tor enables anonymous communication by concealing the user's location and grants access to sites hosted on the onion router. Importantly, Tor and other anonymizing technology (e.g., I2P and Freenet) was intended to increase privacy and security for Internet users around the globe. Darknet markets emerged as a byproduct of anonymity and should not be viewed as synonymous with the Tor project. An interested reader can learn more about Tor by visiting their official site, (https://www.torproject.org/).

Darknet markets serve as virtual meeting places for deviants, drug users, entrepreneurs, fences, and political activists, which support the commerce of illegal goods sold anonymously (Martin, 2014; Ouellet et al., 2022). These transactions are made with an anonymous source, in hopes of acquiring an illegal product or service, and therefore are not backed by buyer-protection services, such as used by PayPal. Additionally, a disgruntled customer of illegal goods cannot (without facing the possibility of sanction) report theft to the police, nor can they retaliate against an anonymous seller (Bergeron et al., 2022). With these obstacles to safety in mind, darknet markets should struggle to stay afloat; yet they are thriving with dozens of identified active markets in existence (Décary-Hétu & Morselli, 2011).

Cybercriminals have made darknet markets successful through several means including, but not limited to, structuring the market in such a way that they can develop a system of trust (Yip et al., 2013), maintaining logistical operations to avoid law enforcement (Kamphausen & Werse, 2019), reducing drug market violence through virtual transactions, communicating through asynchronous connections (Aldridge, 2019), and managing self-regulatory support systems to address marketplace discord (Morselli et al., 2017). In other words, cybercriminals employ a series of techniques to avoid being caught by law enforcement or victimized by adversaries. Moreover, when law enforcement officers do successfully seize a market, market participants quickly adapt through mass migration to new platforms (Ouellet et al., 2022).

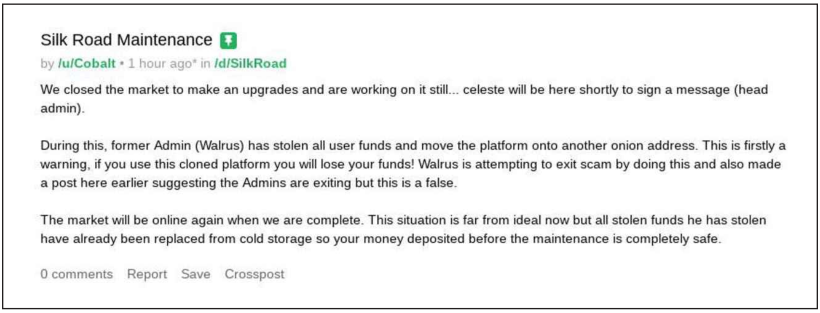
In the context of darknet market supply and demand, the most crucial of these factors is a system of trust (Kim & Ahn, 2007). A prominent method used to establish reputability is a vendor rating system, which is similar to the rating systems present on legitimate e-commerce websites (e.g., Amazon and eBay) (Décary-Hétu & Dupont, 2013). Vendors are rated based on their past transaction history. Those who have completed more successful transactions receive higher scoring reviews. Buyers, as would be expected, choose top-rated vendors and avoid those with lower ratings, even if it means paying higher prices (Duxbury & Haynie, 2018). Recent studies have shown that being a reputable darknet vendor is associated with returning customers

(Décary-Hétu & Quessy-Doré, 2017) and greater monetary gain (Nurmi et al., 2017). Moreover, darknet market administrators also serve a crucial role in upholding a secure milieu of trustworthiness (Kamphausen & Werse, 2019). These administrators often create and maintain escrow systems to increase the likelihood of successful transactions between customers and vendors. Moreover, they also serve as mediators by managing conflict between customers and vendors (Morselli et al., 2017).

However, trusting a third party to manage funds can also create risks for those using darknet markets. Darknet market administrators have been accused of running exit scams: shutting down markets and keeping cryptocurrencies stored in escrow accounts (sometimes worth millions of dollars) (Van Buskirk et al., 2017). In fact, the closure of darknet markets occurs more frequently from inside jobs than from law enforcement operations (Branwen, 2013). Moreover, such behaviors (or the perception of such behaviors) from darknet market administrators can also inadvertently risk "lemonizing" the market in which they are overseeing. Essentially, "lemonization" of a market is an economic phenomenon incited by the state of uncertainty over the quality of a product or legitimacy of the market (see Akerlof, 1978; Reuter & Caulkins, 2004). In the context of underground economies online, lemonization can emerge through slanderous gossip against customers, vendors, or market administrators (Franklin et al., 2007). Scholars have theorized how means of slander appear to be particularly relevant in the context of darknet markets. For example, Hutchings and Holt (2017) posit that gossip can create distrust among buyers and sellers, disrupting market operations. Gossip surrounding darknet market operations may be initiated through a variety of channels, both formal and informal. Law enforcement may deliver official warnings via popular news outlets or social media. Customers may leave negative reviews about vendors on the market, or vendors may complain about administrators over forums dedicated to the market. One form of gossip that may be particularly relevant to disruption is gossip delivered by an official administrator about the safety of users operating on the market they oversee. Since market administrators oversee operations, it is plausible their messages are viewed as credible sources of information. To date, no known study has investigated if and how credible sources of gossip lemonize markets and incite risk avoidance behavior.

Current Study

The primary objective of the current study is to develop a better understanding of risk avoidance behavior in a darknet environment. Drawing from the SCP framework, we assess Hutchings and Holt's (2017) notion that darknet



Silk Road Maintenance

by /u/Cobalt • 1 hour ago* in /d/SilkRoad

We closed the market to make an upgrades and are working on it still... celeste will be here shortly to sign a message (head admin).

During this, former Admin (Walrus) has stolen all user funds and move the platform onto another onion address. This is firstly a warning, if you use this cloned platform you will lose your funds! Walrus is attempting to exit scam by doing this and also made a post here earlier suggesting the Admins are exiting but this is a false.

The market will be online again when we are complete. This situation is far from ideal now but all stolen funds he has stolen have already been replaced from cold storage so your money deposited before the maintenance is completely safe.

Figure 1. Message warning Silk Road 3.1 users of potential victimization.
Note. The message was posted by a Silk Road 3.1 administrator to the market's official forum on February 8th, 2019.

markets can be disrupted through means of gossip. Specifically, we investigate whether a gossip message warning darknet market users of potential victimization experiences alters the behavioral patterns of those users, both customers and vendors. The message, as presented in Figure 1, warned users that a former administrator from Silk Road 3.1 was running an exit scam to steal their cryptocurrencies. The message was posted by the administrator on the market's official forum, meaning everyone who accessed the market could view the message.

Applying Jacques and Reynald's (2012) notion that offenders adopt SCP techniques to avoid detection, punishment, and victimization, we believe online offenders adopt risk avoidance strategies when learning they may be victimized in a darknet environment. One way for drug dealers in the physical world to avoid risk is to limit the amount of product they sell (Jacques & Reynald, 2012). For vendors on the darknet, this risk avoidance strategy would result in less product advertisement being posted on the market, limiting the amount potentially lost during an exit scam. Therefore, the first hypothesis is as follows:

> Hypothesis 1—*Darknet market vendors who receive a message warning them of potential* victimization *experiences will reduce the number of posted advertisements.*

In conjunction with Hutchings and Holt's (2017) notion that entire markets can be lemonized through slander, one may suspect that in the face of credible information regarding potential victimization experiences, distrust will ensue, increasing offenders' risk avoidance behavior independent of the accomplice's (or vendor's) reputation. In other words, it is our belief that customers' distrust for the market and its administrators will outweigh the trust bestowed upon reputable vendors forcing a mass migration from the market. Therefore, we posit that customers will make fewer transactions and spend less money (on the lemonized market) with both reputable and non-reputable vendors after receiving a warning message from a credible source. Stated as hypotheses:

> Hypothesis 2 – *Darknet market customers who receive a message warning them of potential* victimization *experiences will reduce the number of transactions made with vendors, independent of the* vendor's *reputations.*
> Hypothesis 3 – *Darknet market customers who receive a message warning them of potential* victimization *experiences will reduce the amount of money spent with vendors, independent of the* vendor's *reputations.*

Data and Methodology

Data for this study were gathered from Silk Road 3.1, a darknet market only accessible through Tor that serves as a platform to sell illegal commodities such as drugs, fraudulent documents, and criminal services. These data were acquired by using a Python scraper built for the sole purpose of gathering data on Silk Road 3.1. This market was scraped on a weekly basis throughout 2019, which allowed for the extraction of all information posted on the market to a local database server hosted at a large southern university in the United States. This data collection protocol was reviewed by the Institutional Review Board (IRB) and approved under Protocol number H19510.

Intervention

The intervention (or stimuli) in this quasi-experimental study was reception of the message about potential victimization experiences on Silk Road 3.1. On February 8th, 2019, a Silk Road 3.1 market administrator posted a message directly to the market's official forum warning users that a former administrator was running an exit scam in attempt to steal their cryptocurrencies. Our research team, while extracting data, identified the message within an hour of its posting, and the message has since received thousands of comments, demonstrating it was both accessible and widely viewed by the target population. The original posting is presented in Figure 1 above. In line with past research (Maimon et al., 2021) we examined behavioral patterns 4 weeks (or month) before and after reception of the message. The month preceding the message was considered the control condition while the month of operation following the message is considered the treatment condition.

Dependent Variables

Risk avoidance behavior is operationalized in two separate manners, one for customers and one for vendors. Regarding vendors, it is operationalized as a reduction in the number of unique product listings advertised on the market the month of operation post intervention compared to the month of operation prior to the intervention. Regarding customers, it is operationalized as a reduction in the amount of money spent and number of transactions made on the market the month of operation post intervention compared to the month prior to the intervention.

Using these scraped data, we were able to determine the total number of unique advertisements posted in the month prior and the month of operation following the intervention. Additionally, we were able to discern the number of transactions made and amount of money spent (converted to USD based on exchange rates at the time of inquiry) with each vendor (on Silk Road 3.1) daily through the summation of each vendors' total number of transactions and the dollar amount of these transactions during the observational period. Lastly, we were able to gather each vendor's rating, which is a score based on the number of successful transactions made. It is important to note that Silk Road 3.1 makes this information publicly available to all registered users of the site; we simply developed a systematic method to automatically extract the information and store it in a structured database.

We gathered information on 80 vendors who were active on Silk Road 3.1 within the 4 weeks of operation before and/or after the intervention. The vendors' ratings ranged from 1 to 5, with the majority of vendors (n = 48) receiving a score of 1. A score of 1 means the vendor has not established a reputation, whereas a score higher than 1 indicates the vendor has established at least some level of reputability. Therefore, for the purpose of this study, any vendor with a rating score greater than 1 is considered a reputable vendor, whereas any vendor with a score of 1 is considered a non-reputable vendor. The reputation variable was dichotomized (0/1) to reflect this distinction.

Analytic Strategy

The quasi-experimental design employed here is known as the "one-group pretest-posttest design" (Campbell & Stanley, 1963, p.47). Since random assignment was not possible, we simply observed the behavioral patterns of Silk Road 3.1 customers and vendors before and after the naturally occurring intervention and conducted seven one-tailed paired samples *t*-tests. We report the mean differences, *t*-test results, and Cohen's effect size *d* for each of the seven models presented. Generally, Cohen's *d* is a measure of difference between groups in terms of standard deviation units. A rule of thumb is that a d=0.2 is considered small, d=0.5 is medium, and d=0.8 is large.

First, we examined the mean difference in the number of advertisements posted by vendors the month of operation before and after the intervention to assess the message's impact on vendors' risk avoidance behavior. Next, we examined mean differences in the number of transactions made and amount of money by customers the month before and month of operation after the message was delivered to determine the message's overall effect on customers' risk avoidance behavior. Lastly, we examined mean differences in the number of transactions made and amount of money spent by customers with both reputable and non-reputable vendors the month of operation before and after the intervention to determine if risk avoidance behavior was employed irrespective of the vendor's reputations. A post hoc power test showed that all seven models had sufficient power to detect at least medium effect size differences.

Results

Table 1 presents the descriptive and inferential findings regarding customer and vendor behavior across the study's timespan. Table 1, Model 1 compares the number of advertisements posted by vendors to Silk Road 3.1 the month of operation before and after the intervention. The average number of unique advertisements posted per day the month of operation prior to the intervention was 6.71 (SD=1.16). In the month of operation following the intervention, the number of unique advertisements fell to a daily average of 4.03 (SD=0.26), resulting in an average difference of 2.68 unique advertisements, which reached conventional levels of statistical significance (t=11.92, $p < .05$). The impact of the difference between the pre- and post-intervention means was large (d=3.19). In support of our first hypothesis, this finding shows that vendors demonstrate risk avoidance behavior by posting fewer advertisements after being confronted with a gossip message warning them of potential victimization experiences.

Furthermore, and as presented in Model 2, the number of transactions made with the 80 vendors in our study ranged from 0 to 14 the month of operation before the intervention, with the average number of transactions being 2.46 (SD=2.59). A sharp reduction occurred the month of operation following the message. Specifically, the number of transactions ranged from 0 to 8, with the average number of transactions being 1.06 (SD=1.88). The mean difference in the number of transactions before and after the intervention was 1.4 and reached conventional levels of statistical significance (t=3.86, $p < .05$). The effect size of the difference was medium (d=0.62).

Table 1. Paired Samples *t*-test Results of Darknet Vendors and Customers' Behavior After Exposure to a Warning Message.

Comparison	*n*	*M*	*M diff.*	*SE*	*t*	*d*
Model 1						
Advertisements before	28	6.71	2.68	0.22	11.92*	3.19
Advertisements after	28	4.03				
Model 2						
Transactions before	80	2.46	1.40	0.36	3.86*	0.62
Transactions after	80	1.06				
Model 3						
Dollars spent before	80	399.26	171.87	96.43	1.78*	0.25
Dollars spent after	80	277.39				
Model 4						
Non-reputable transactions before	48	1.79	0.96	0.41	2.34*	0.51
Non-reputable transaction after	48	0.83				
Model 5						
Reputable transaction before	32	3.47	2.06	0.66	3.13*	0.79
Reputable transaction after	32	1.41				
Model 6						
Non-reputable dollars before	48	244.54	136.56	81.45	1.68*	0.35
Non-reputable dollars after	48	107.98				
Model 7						
Reputable dollars before	32	631.35	224.84	209.76	1.07	0.23
Reputable dollars after	32	406.51				

Note. $^*p < .05$. For column abbreviations: "*n*" is number of observations; "*M*" is mean; "*M* diff." is mean difference; "*SE*" is standard error of the difference; "*t*" is the value of the *t*-test; "*d*" is Cohen's effect size.

Similar trends, as displayed in Model 3, emerge when examining the amount of money spent with vendors before and after the intervention occurred. The amount of money spent with these vendors before the intervention ranged from $0 to $4747 USD, with an average of $399.26 (SD = $796.20) USD spent. The amount of money spent after the intervention ranged from $0 to $3620 USD, with an average of $227.39 (SD = $578) USD spent. The difference in the amount of money spent before and after the posted message was $171.97 USD and is statistically significance (t = 1.78, p < .05, d = 0.25). This difference shows that customers demonstrate risk avoidance behavior by making fewer transactions and spending less money with their vendors after being confronted with a warning message from a credible source, thus garnering initial support for the second and third hypothesis.

In addition to examining overall market trends post message, we also examined whether customers practice risk avoidance behavior independent of their vendor's reputations. In other words, we assessed how the intervention affected the number of transactions and amount of money spent with both reputable and non-reputable vendors. As indicated in Table 1, we found a significant reduction in the number of transactions made with non-reputable (Model 4) and reputable (Model 5) vendors before and after the intervention. Regarding reputable vendors, the average number of transactions declines from 3.47 (SD=3.07) to 1.41 (SD=2.01), resulting in a statistically significant mean difference of 2.05 transactions (t=3.13, p<.05). Note, the effect size of the difference was large (d=0.79). Regarding non-reputable vendors, the average number of transactions declines from 1.79 (SD=1.98) to 0.83 (SD=1.78), resulting in a statistically significant mean difference of 0.96 transactions (t=2.34, p<.05). The effect size of the difference was medium (d=0.51). Although customers reduced the number of transactions made with both reputable and non-reputable vendors, the number of transactions made by customers with reputable vendors was reduced by 59% in comparison to 54% for non-reputable vendors. These findings, in further support of hypothesis two, indicate customers are likely to employ risk avoidance behavior irrespective of their vendor's reputation, but those who are more reputable suffer a slightly greater loss.

Similar patterns emerge when examining the amount of money customers spend. Regarding non-reputable vendors, and as reported in Model 6, customers spent an average of $244.54 USD before and $107.98 USD after the intervention, resulting in a statistically significant mean difference of $136.56 USD *(*t=1.68, p<.05). Regarding reputable vendors, and as presented in Model 7, customers spent an average of $631.35 USD before the intervention compared to $406.51 after the intervention, resulting in a non-significant mean difference of $224.84 USD (t=1.07, p=ns). Although customers reduced the amount of money spent with both non-reputable and reputable vendors, reputable vendors experienced a 36% reduction (which was non-significant) in the amount of money generated in comparison to non-reputable vendors who experienced a 56% reduction. Paralleling the findings above, and providing further support for hypothesis three, this indicates customers are likely to employ risk avoidance behavior irrespective of their vendor's reputation, but in terms of monetary lost, non-reputable vendors take a larger (and statistically significant) financial hit. It should be noted the effect size of the difference for both reputable (d=0.23) and non-reputable vendors (d=0.35) was small.

Discussion

Although a large body of literature has examined how offenders avoid the risks of both police apprehension and victimization from adversaries, prior studies rely almost exclusively on qualitative research designs. Qualitative research is useful in providing preliminary insight into understudied phenomenon but is unable to assess causal assumptions. To our knowledge, the current study is the first examination of offenders' risk avoidance behavior in cyberspace using a quasi-experimental design that supports casual inference. We find, when presented with a credible source's warning about potential victimization experiences, both darknet vendors and customers demonstrate risk avoidance behavior. More simply put, gossip stemming from an informal communication channel prompted vendors to post fewer advertisements, and customers to make fewer transactions and spend less money.

In essence, the study answers the call for rigorous inquiry into cybercriminal behavior using innovative, interdisciplinary methods (Howell & Burruss, 2020). In doing so, we find support for the notion that cybercriminals act with rationality (Howell et al., 2017; Maimon et al., 2021): when confronted with a risk, behavior is altered to avoid personal harm. Additionally, the current study advances the SCP literature by highlighting the importance of a credible source's ability to incite behavioral change through means of gossip. Both Atlas (1990) and Jacques and Reynald (2012) found that offenders reverse engineer traditional situational techniques to avoid sanction in the physical world. Additionally, Dickinson and Wright (2015) established gossip as a relevant informal communication channel that leads offenders to employ risk avoidance techniques. We expand upon these findings by demonstrating that gossip (in the form of a warning message) influences offenders' decision to engage in risk avoidance behavior in a darknet environment.

Policy Implications

In addition to providing important theoretical contributions to the SCP literature, the findings presented in the current study have practical implications as well. It has been well-established that police officers are unable to deal with cybercrime in any systematic way (Burruss et al., 2019). It is also evident through the yearly increase in the rates of cybercrime incidents that the current retroactive approach to cybercrime prevention is ineffective. The current study provides evidence that human-based interventions can be an effective and proactive means in curtailing the commission of criminal events from occurring.

In terms of policy development, the findings presented here demonstrate that lemonization (Hutchings & Holt, 2017) can be successfully utilized to disrupt darknet market operations. We find that if a credible source warns darknet marketplace users of a potential scam, the customers and vendors of such markets will reduce their engagement with the market. Therefore, it stands to reason that those wishing to disrupt a darknet market can do so using various other informal communication channels, if they first infiltrate the online ecosystem and establish credibility among market participants. This approach may prove more effective and less costly than the search and seizure approach currently employed by law enforcement officials (Ladegaard, 2019). However, such activity may also displace users to a different darknet market: instead of simply leaving Market 1, users may begin shopping at Market 2. This could still be advantageous if Market 2 is notably better than Market 1. For example, if Market 1 allows for the selling of deadly substances such as fentanyl but Market 2 does not, displacing users from Market 1 to Market 2 is still beneficial from a public health perspective.

Limitations and Future Research

The study presented here does have notable limitations. As discussed above, we conducted what Campbell and Stanley (1963) refer to as a one-group pretest-posttest design, but with a naturally occurring stimuli. This design does not rule out the possibility of alternative hypotheses to explain the changes in online offending behavior. It is possible, although unlikely, that something else occurred at the same time the darknet market administrator posted the warning message that sparked the behavioral change. In this hypothetical scenario, some alternative event, rather than the warning message, could have altered offenders' risk avoidance behavior. Furthermore, this study has limited external validity. Silk Road 3.1 is a relatively small market. It is possible that general behavior, and risk avoidance behavior more specifically, differ from market to market based on size and other unobserved factors. External validity can be improved through replication. Ideally, future researchers will employ similar research designs using other samples of active online offenders. Lastly, it is possible that customers did not limit the number of transactions made and money spent, but instead made those transactions and spent their money elsewhere. Similarly, it is possible vendors posted advertisements to different markets. Although we were unable to test the notion of displacement in the current study, this too would exemplify risk avoidance behavior supportive of our hypotheses. Future studies should assess the efficacy of disruption on the darknet ecosystem, rather than a singular market operating within the ecosystem (Ouellet et al., 2022).

Conclusion

Although limitations exist, and future research is warranted, one thing is evident: human-based interventions must not be dismissed when developing comprehensive cybersecurity prevention strategies (Howell et al., 2019; Perkins & Howell, 2021). Technological innovation and target hardening will always have a place in cybercrime prevention, but to overlook what does and does not work in a sociological and psychological context regarding those engaged in cybercrime perpetration is a drastic mistake. Given the previous literature and the current study both present evidence that cybercriminals are rational in their decision-making capabilities (Perkins et al., 2022), it is our belief that effective cybersecurity can only be achieved through collaborative, multi-disciplinary efforts examining both the human and technical elements of a cybercrime incident.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Christian Jordan Howell https://orcid.org/0000-0003-4443-5068

George W. Burruss https://orcid.org/0000-0002-1148-7446

Marie Ouellet https://orcid.org/0000-0003-4442-3374

References

Akerlof, G. A. (1978). The market for "lemons": Quality uncertainty and the market mechanism. In P. Diamond & M. Rothschild (Eds.), *Uncertainty in Economics* (1st ed., pp. 235–251). New York, USA: Academic Press. https://doi.org/hp8b

Aldridge, J. (2019). Does online anonymity boost illegal market trading? *Media, Culture & Society*, *41*(4), 578–583. https://doi.org/gmzdz8

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, *41*, 101–109. https://doi.org/f9x2mw

Atlas, R. (1990, October 8–12). "Offensible Space"— Law and Order Obstruction through Environmental Design. In *Proceedings of the Human Factors Society Annual Meeting* (Vol. 34, No. 7, pp. 570–574). Los Angeles, CA: SAGE Publications. https://doi.org/fxztrx

Becker, G. S. (1968). Crime and punishment: An economic approach. In N. G. Fielding, A. Clarke, & R. Witt (Eds.), *The economic dimensions of crime* (1st ed., pp. 13–68). Palgrave Macmillan. https://doi.org/gf8sw5

Bergeron, A., Décary-Hétu, D., & Ouellet, M. (2022). Conflict and victimization in online drug markets. *Victims & Offenders*, *17*(3), 350–371. https://doi.org/hp8d

Branwen, G. (2013). *Darknet market mortality risks*. Retrieved August 24, 2020, from https://www.gwern.net/DNM-survival

Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing: An International Journal*, *43*(1), 105–119. https://doi.org/grs8

Campbell, D. T., & Stanley, J. C. (1963). *Experimental and quasi-experimental designs for research* (1st ed.). Chicago, IL: Rand McNAlly & Company.

Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *British Journal of Criminology*, *20*(2), 136–147. https://www.jstor.org/stable/23636692

Clarke, R. V. G. (1995). Situational crime prevention. *Crime and Justice*, 1*9*, 91–150. https://doi.org/dfkhw8

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*, 41–96.

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime*, *14*(2-3), 175–196. https://doi.org/gprdgv

Décary-Hétu, D., & Morselli, C. (2011). Gang Presence in Social Network Sites. *International Journal of Cyber Criminology*, *5*(2), 876–890.

Décary-Hétu, D., & Quessy-Doré, O. (2017). Are repeat buyers in cryptomarkets loyal customers? Repeat business between dyads of cryptomarket vendors and users. *American Behavioral Scientist*, *61*(11), 1341–1357. https://doi.org/gckwmn

Dickinson, T., & Wright, R. (2015). Gossip, decision-making and deterrence in drug markets. *The British Journal of Criminology*, *55*(6), 1263–1281. https://doi.org/f7zj8q

Duxbury, S. W., & Haynie, D. L. (2018). Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks*, *52*(2018), 238–250. https://doi.org/gdj7p8

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007, October 31–November 2). An inquiry into the nature and causes of the wealth of internet miscreants [Paper Presentation]. In proceedings of the 14th *ACM conference on Computer and communications security* (pp. 375–388). United States of America. https://doi.org/b6qfmm

Holt, T. J., Blevins, K. R., & Kuhns, J. B. (2008). Examining the displacement practices of johns with on-line data. *Criminal Justice Journal*, *36*(6), 522–528. https://doi.org/dvrdjv

Hovland, C. I., & Weiss, W. (1951). The influence of source credibility on communication effectiveness. *Public Opinion Quarterly*, *15*(4), 635–650. https://doi.org/fs3zww

Howell, C. J. (2021). *Self-protection in Cyberspace: Assessing the processual relationship between thoughtfully reflective decision making, protection motivation theory, cyber hygiene, and victimization*. (Publication No. 28410121) [Doctoral dissertation, University of South Florida –Tampa]. ProQuest Dissertations Publishing. https://doi.org/hp8p

Howell, C. J., & Burruss, G. W. (2020). Datasets for analysis of cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The palgrave handbook of international cybercrime and cyberdeviance* (1st ed., pp. 207–219). London, UK: Palgrave Macmillan. https://doi.org/hp8q

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), 536–550. https://doi.org/grtx

Howell, C. J., Maimon, D., Cochran, J. K., Jones, H. M., & Powers, R. A. (2017). System trespasser behavior after exposure to warning messages at a Chinese computer network: An examination. *International Journal of Cyber Criminology*, *11*(1), 63–77. https://doi.org/grwd

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime*, *18*(1), 11–30. https://doi.org/hp8t

Jacobs, B. A. (1993). Undercover deception clues: A case of restrictive deterrence. *Criminology*, *31*(2), 281–299. https://doi.org/bp4sbr

Jacobs, B. A., & Wright, R. (2010). Bounded rationality, retaliation, and the spread of urban violence. *Journal of Interpersonal Violence*, *25*(10), 1739–1766. https://doi.org/cht7rv

Jacques, S., & Reynald, D. M. (2012). The offenders' perspective on prevention: Guarding against victimization and law enforcement. *Journal of Research in Crime and Delinquency*, *49*(2), 269–294. https://doi.org/dfsxmh

Jeffery, C. R. (1971). *Crime prevention through environmental design* (1st ed.). Beverly Hills, CA: SAGE Publications.

Johnson, B. D., & Natarajan, M. (1995). Strategies to avoid arrest: Crack sellers' response to intensified policing. *American Journal of Police*, *14*(3/4), 49–69. https://doi.org/bkx7dk

Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy*, *73*, 281–287. https://doi.org/gnmkvj

Kim, M. S., & Ahn, J. H. (2007). Management of trust in the e-marketplace: The role of the buyer's experience in building trust. *Journal of Information Technology*, *22*(2), 119–132. https://doi.org/b243zm

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, *63*, 113–121. https://doi.org/gnqxdt

Maimon, D., Howell, C. J., & Burruss, G. W. (2021). Restrictive deterrence and the scope of hackers' reoffending: Findings from two randomized field trials. *Computers in Human Behavior*, *125*, 106943. https://doi.org/grvc

Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs* (1st ed.). London, UK: Palgrave Pivot. https://doi.org/hp8v

Moeller, K., Copes, H., & Hochstetler, A. (2016). Advancing restrictive deterrence: A qualitative meta-synthesis. *Journal of Criminal Justice*, *46*(2016), 82–93. https://doi.org/f8z24z

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict management in illicit drug cryptomarkets. *International Criminal Justice Review*, *27*(4), 237–254. https://doi.org/ghf4g5

Newman, O. (1972). *Defensible space: Crime Prevention Through Urban Design* (1st ed.). New York, NY: Macmillan Publishing.

Nurmi, J., Kaskela, T., Perälä, J., & Oksanen, A. (2017). Seller's reputation and capacity on the illicit drug markets: 11-month study on the Finnish version of the Silk Road. *Drug and Alcohol Dependence*, *178*(2017), 201–207. https://doi.org/gbxgjr

Ouellet, M., Maimon, D., Howell, J. C., & Wu, Y. (2022). The network of online stolen data markets: How vendor flows connect digital marketplaces. *The British Journal of Criminology*. https://doi.org/hp8w

Perkins, R. C., & Howell, C. J. (2021). Honeypots for cybercrime research. In A. Lavorgna & T. J. Holt (Eds.), *Researching Cybercrimes: Methodologies, Ethics, and Critical Apporaches* (1st ed., pp. 233–261). London, UK: Palgrave Macmillan.

Perkins, R. C., Howell, C. J., Dodge, C. E., Burruss, G. W., & Maimon, D. (2022). Malicious spam distribution: A routine activities approach. *Deviant Behavior*, *43*(2), 196–212. https://doi.org/grvw

Reuter, P., & Caulkins, J. P. (2004). Illegal 'lemons': Price dispersion in cocaine and heroin markets. *Bulletin on Narcotics*, *56*(1-2), 141–165. https://www.unodc.org/pdf/bulletin/bulletin_2004_01_01_1_Art6.pdf

Sutherland, E. H. (1937). The professional thief. *The Journal of Criminal Law and Criminology*, *28*(2), 161–163. https://www.jstor.org/stable/1136895

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., & Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence*, *173*(2016), 159–162. https://doi.org/f95bch

Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C., & Gajewski, F. (2006). Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology*, *44*(3), 549–592. https://doi.org/fvb24c

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, *26*(4), 716–745. https://doi.org/fbwhmg

Wright, R. T., & Decker, S. H. (1996). *Burglars on the job: Streetlife and residential break-ins.* Boston, MA: Northeastern University Press.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516–539. https://doi.org/gm477c

Author Biographies

Christian Jordan Howell is an Assistant Professor in Criminology at the University of South Florida. He earned both his doctorate and master's in criminology from the University of South Florida in 2021 and 2016, respectively. His work focuses on the human factor of cybercrime. He employs advanced computer science techniques to gather threat intelligence, which is then used to test social scientific theory, build profiles of active cyber-offenders, plot criminal trajectories, and disrupt the illicit ecosystem enabling cybercrime incidents.

David Maimon is an Associate Professor of Criminal Justice and Criminology at Georgia State University. He received his doctorate in Sociology from the Ohio State University in 2009. Prior to joining Georgia State University ranks, David held a professor position at the University of Maryland. David's research interests include theories of human behaviors, cyber-enabled and cyber-dependent crimes and experimental research methods. His research interests include theories of human behaviors, cyber-enabled and cyber-dependent crimes and experimental research methods.

Robert C. Perkins is a Doctoral Student in the Department of Criminal Justice and Criminology at Georgia State University as well as a graduate research assistant for the Evidence-Based Cybersecurity Research Group. His studies cover cybercrimes and other forms of technologically-facilitated antisocial behaviors. In particular, his research addresses the sociological aspects of cybersecurity and offender-decision making in online environments.

George W. Burruss is an Associate Professor in the Department of Criminology at the University of South Florida and the Editor-in-Chief of the Journal of Crime and Justice. He graduated from the University of Missouri St. Louis in Criminology and Criminal Justice. His research focuses criminal justice organizations and cybercrime.

Yubao Wu is an Assistant Professor in the Department of Computer Science at Georgia State University. His research interests include evidence-based cybersecurity, big data analytics, data mining, databases, and artificial intelligence. His research aims at collecting open-source intelligence from the cybercriminals' public online behavioral data such as ads, chats, and financial transactions.