The online stolen data market: Disruption and intervention approaches

Alice Hutchings[a] & Thomas J. Holt[b]

[a]Computer Laboratory, University of Cambridge, Cambridge, UK, +44 1223 763660, alice.hutchings@cl.cam.ac.uk; [b]School of Criminal Justice, Michigan State University, East Lansing, USA, +1 517-353-9563, holtt@msu.edu

This paper brings a new taxonomy and collation of intervention and disruption methods that can be applied to the online stolen data market. These online marketplaces are used to buy and sell identity and financial information, as well as the products and services that enable this economy. This paper combines research findings from computer science with criminology to provide a multidisciplinary approach to crimes committed with the use of technology.

Keywords: online black market; stolen data; crime prevention; intervention and disruption; underground economy

Introduction

Over the last two decades, research has identified a range of offenses that are enabled through computer technology and the Internet.[1] For example, communication systems streamline the solicitation process of the sex trade,[2] increase the available number of targets for fraud,[3] and engender stalking and threatening communications that can directly affect victims at any time of the day.[4] At the same time, technology has also facilitated forms of offending that would not otherwise exist, including computer hacking where actors compromise existing boundaries of ownership to gain access to sensitive information and affect data.[5]

The threat posed by unauthorised access should not be underestimated, especially given the economic harm caused by the misuse of personal information, including credit and debit card account numbers. Sensitive data now resides in various electronic databases on-line that can be remotely accessed and compromised by hackers.[6] Numerous sensitive databases are compromised every year,[7] some of which lead to losses of millions of credit cards or personal data.[8]

The substantial quantity of information obtained by hackers and attackers have led to the growth of on-line markets where cybercriminals can sell stolen data to others.[9] Research suggests actors engage one another via Internet Relay Chat (IRC) or Russian-language web-based forums, although a small proportion also operate in English.[10] These markets facilitate the sale of credit card numbers and personally identifiable information, as well as resources to facilitate various cybercrimes.[11] The sales process is driven by advertisements posted by sellers describing the products they have to offer, their pricing structures, contact information, and any rules regarding the transaction process. In turn, buyers contact the seller, negotiate the terms of sale, send money directly to the seller, and wait for their products to be delivered.[12]

Estimates on the scope of harm caused by stolen data market operations suggests they may cause millions of dollars in losses to individual victims and corporations, as well as enabling various forms of cybercrime across the globe.[13] Limited research has given recommendations on methods to disrupt markets or affect their operations.[14] There is, however, virtually no criminological research considering these strategies or the ways that they may be practically applied by law enforcement agencies, consumers, policy makers, and commercial organisations. This study addresses this gap through an analysis of the various disruption and intervention methods that have been proposed and implemented by academics, industry, and policy-makers alike.

The current focus to disrupt online marketplaces centres on investigation and prosecution of key players.[15] In 2004, Shadowcrew, a stolen data marketplace, was targeted by law enforcement using a police informant. Following this operation, FBI agents infiltrated the DarkMarket forum, culminating in the agency running the server and hosting the communication.[16] In 2012, international efforts involving seven countries resulted in three arrests and 36 websites being shut down.[17] Such a takedown of stolen data markets involves substantive high profile investigative resources, which, in the long term, may have a limited disruption effect on the larger underground economy for information.[18] Thus, there is some tension with the law enforcement approach of targeting high value, small volume type offences, which seemingly ignores small value, but potentially high volume, type crimes.

Previous research on data markets is largely descriptive, documenting the products sold and practices of market actors.[19] While valuable, they do not inform policy-makers as to the most vulnerable points in the process of data sales that may facilitate successful implementation of disruption strategies. This paper extends recent research by Hutchings and Holt,[20] which is the only study to date that has applied a crime script analysis to demonstrate the step-by-step interactions in the stolen data market, how they operate, and the actors involved. Crime scripts are useful in identifying the significant steps in criminal operations that can be targeted for crime prevention.[21]

The crime script that was developed described the preparations to entry, including setting up the necessarily client software and accounts, and taking steps towards anonymity and security. Some actors operate in multiple marketplaces. Marketplaces differ in their openness, the predominant language used, their specialisation in different products or services, and the ways in which they regulate users' behaviours. Some forums provide tutorials and discussions to teach specialised knowledge, both free and for a fee, and some advertisers claim to provide technical support.

Forums provide formal marketplace rules, which are policed by moderators. Sellers of credit card data often set out their own terms, advising the conditions under which their products would be replaced if declined. In addition to learning these formal rules, newcomers are required to learn the jargon and slang that are commonly used. A precondition for sellers is having services, or obtaining and manufacturing products to trade. In some cases, sellers re-sell products or services obtained elsewhere. Data offered for sale are obtained from data breaches, malware, phishing, or skimming credit cards.

Advertisements are placed in accordance with the rules of the forum. Some forums offer a verification process, whereby moderators test a sample of the products offered. Actors on the marketplace are communicative, commenting on threads, initiating and responding to discussion points, and sometimes exchanging information relating to law enforcement activities. Advertisements also include private contact details for the purpose of negotiating and finalising sales. A variety of money transfer providers are used, with payment usually required before delivery, or using an escrow service.

The transfer of stolen data from the seller to the buyer takes place electronically outside of the forum or IRC channel used to sell products. However, physical goods, such as skimmers, are packaged and sent to the purchaser by mail, courier, or in some cases, delivery by hand or local transport. Sellers manage their reputations by seeking positive reviews within their advertising thread so that others can publicly validate the seller reputation. However, negative reviews are also common which may hinder the reputation development of the vendor. Sellers looking to exchange their currency, and to launder their proceeds, can utilise the providers who advertised these services.

This paper contributes to and extends the existing literature by researchers like Hutchings and Holt[22] by considering the types of interventions that can be applied at these points. The intervention strategies discussed are not intended as an exhaustive or complete representation of all current examples employed. Rather, this analysis serves as a convenience sample representing some of the most prominent strategies either previously or actively employed to disrupt data markets. The attention focused on these strategies by academic, industry, and law enforcement sources would suggest they have utility, though there has been no empirical review of their value to date. Thus, this analysis provides an overview of their utility from a situational crime prevention perspective.

The implications of this study for law enforcement across the globe and for computer scientists are considered in detail, with an emphasis on police legitimacy and visibility, along with the potential for offender displacement. These considerations are important for crime prevention generally, and are especially so for online crime, where displacement opportunities increase, along with the opportunities for actions that may not be perceived as legitimate. The paper considers these concepts in turn, before discussing the specific crime prevention strategies applicable to the stolen data market. This latter part has been structured by interventions aimed at the act, actor, and marketplace for stolen data.

Situational crime prevention and disruption initiatives

Situational crime prevention often takes a different focus from that of the criminal justice system; namely, to catch and punish offenders.[23] Levi and Maguire,[24] in relation to organised crime, stated that crime prevention should be aimed at the particular forms of crime, or the 'acts', as well as those who were involved in their commission, or the 'actors'. This approach to crime prevention and disruption is situational in nature, as the aim is to change the environment in which crime occurs. The situational crime prevention approach applies multiple theories. One method is the routine activity approach, which posits that crime reduction can be achieved by increasing the capability of guardians, decreasing the suitability of targets, and decreasing the presence of motivated offenders.[25] On the other hand, rational choice theory[26] suggests that increasing the effort to commit a crime, increasing the perceived likelihood of detection, and reducing the expected benefit, will deter crime. One intervention may have several effects, such as both increasing the effort and reducing the benefits.

We note that situational crime prevention methods go beyond deterrence principles, in that they do not seek to solely deter crime through the threat of punishment. Nevertheless, some of the principles of deterrence are applicable to crime prevention more generally. In particular, Gibbs[27] and Jacobs[28] expanded the concept of deterrence to incorporate restrictive deterrence, which refers to reducing the severity and/or frequency of offending to reduce the risk of punishment. Restrictive deterrence contrasts with absolute deterrence, or the avoidance of the criminal behaviour entirely, due to the threat of punishment.[29] Similarly, we may think of restrictive intervention; that is the reduction in the rate or gravity of offending through crime prevention principles.

Crime script analysis can inform situational crime prevention, and has been used in this way to identify intervention methods in relation to drug manufacturing,[30] child sex offending,[31] and organised crime.[32] Chiu et al.[33] approached this task by breaking down interventions aimed at the offender, the guardians (such as regulators and those that sell precursor chemicals), and the locations where drug laboratories were present, by the script scenes. In contrast, Leclerc et al.[34] outlined prevention strategies by applying the conditions that facilitated or enabled the offence to take place (such as the lack of a suitable guardian and the presence of a vulnerable child), to each scene. Meanwhile, Hancock and Laycock[35] categorised the actions for each scene into whether they related to criminal lifestyles, networking of offenders, or the primary criminal act, and applied the intervention approaches to these. In this paper, we use the points of intervention from Hutchings' and Holts' crime script analysis of online stolen data markets.[36]

Another point to consider when developing intervention strategies is who is responsible for their development and implementation. Cohen and Felson[37] use the term 'capable guardian' to include those that have the potential to discourage offenders, whether they be the owner of the property, law enforcement agencies, regulatory bodies, or any other individual or agency. Levi and Maguire[38], however, refer to 'ownership' of crime prevention problems and focus on entities who can deal with offenses in different ways. Organisations identified by Levi and Maguire[39] include the public sector, including the operational level, such as law enforcement (customs and policing agencies); the strategic level, such as policy development; and regulatory bodies. They point out that transnational crimes also require a transnational approach, including non-government organisations that tackle money laundering and other cross-border offences.

The public sector does not have sole ownership over crime prevention strategies. Additional guardians for the stolen data market would include banks, merchants, and security companies, who provide protective software programs, such as antivirus software or firewalls that minimize the likelihood of malicious software infections or attempts to penetrate the user's system.[40] Similarly, Internet Service Providers and web hosting companies that may knowingly or unknowingly host these forums and markets could be vital in securing evidence and records of connections to sites.[41] As noted by Garland,[42] it is not solely the state's responsibility to prevent or control crime. In relation to frauds and scams, especially those that involve an online element, the state can be particularly limited due to the challenges presented by jurisdiction and anonymity.

Legitimacy

Ensuring that interventions are perceived as legitimate, in that they have public acceptance, is essential to their success. Legitimacy has been found to be just as, if not more, important as deterrence principles in influencing compliance with the law. Surveys by Sunshine and Tyler[43] examined the relationship between compliance with the law and evaluations of the legitimacy of the New York City Police Department, as well as perceived risk of being caught and punished. Perceived legitimacy was found to be a stronger predictor of compliance than risk, although both were significant factors. Laws, policies, and institutions that are seen as overstepping legitimacy potentially lessen overall authority in a state.[44] Authorities need to be perceived as legitimate to gain the trust, support, and cooperation of the public, as well as compliance with the law.[45] In relation to state use of authority, it is important to ask questions relating to whether the state should have the requisite power; whether there is oversight and supervision in the use of that power, such as judicial authorisation through the issuance of warrants; how the state responds to abuses of power; and the level of transparency about the use (and abuse) of power.[46] These questions relate to procedural justice, or the fairness of the processes in which authorities make decisions and exercise their powers.[47]

Other perceptual issues relating to how the public and law enforcement view cybercrime may also be important when considering what countermeasures are appropriate. For example, online black markets are generally not visible to the general public, unless they go looking for them. On the other hand, cybercrime types such as malware and spam may be considered more of a nuisance than a threat due to their comparatively high visibility.[48] The general public may not have much knowledge of how their personal data being stolen relates to how their data are misused. Even murkier to the average person, as well as to law enforcement agencies, may be the knowledge of the intermediary steps between these two nuisances, such as the trade of their personal information in online black markets. To whit, less than 20% of respondents in a sample of state and local law enforcement could accurately define the term carding in relation to cybercrime, and 36% had never heard the term before.[49] If law enforcement do not view this problem as a threat or worthy of investigation, it is likely that they will not support attempts to disrupt these marketplaces.[50]

When developing legitimate intervention methods, there should also be consideration of the effects on the rights and freedoms of the law-abiding majority.[51] For example, intervention methods aimed at anonymity networks such as Tor may adversely affect those who use the services for good, and cause harm to individuals whose identities are made known. In addition, for such international marketplaces, there should be consideration as to the ethical questions about whether legislative protections apply to all, or just those who are citizens of a particular country.

Displacement

While disrupting the scripts involved in the crime commission process may prevent crime, it may also result in displacement to alternative locations, targets, times, methods, offenders or offence type.[52] Research on prostitution in the US, for example, has found that increased patrols lead some clients to seek sex workers in other places in a city, or to move online to decrease the risk of arrest.[53] The introduction of chip and PIN credit cards in the United Kingdom has seen a displacement from card-present, to card-not-present payment fraud.[54] In the context of on-line black markets, an offender may displace from one form of computer-mediated communication to another, such as from IRC to forums. In fact, there is limited evidence that such transitions have already occurred, creating multiple markets concurrently for data and other products[55]. Displacement occurs when the script changes as a result of the intervention method that has been put in place. Therefore, intervention approaches should be evaluated to ensure that they create the intended effects, and are not generating unforeseen or undesirable consequences.

Alternative disruption and intervention opportunities

Disruption and intervention opportunities that are aimed at the act, the actor, and the marketplace are outlined below. The acts that are the subject of intervention are those that relate to the black market economy, such as selling tools to steal data, selling stolen data, and providing drop, cashier, and money laundering services. The actors include those identified in the crime script analysis by Hutchings and Holt,[56] namely sellers, buyers, suppliers, moderators (who maintain order on the forums and apply the rules), administrators (who organise the platforms and the hosting of the actual forums), and teachers (who write tutorials and provide advice). These roles are not mutually exclusive, as one individual may take on multiple roles, such as seller and buyer, or administrator and moderator.

Interventions aimed at the Act

Most data advertised for sale in the marketplaces are stolen from data breaches, using keyloggers, phishing, or by skimming credit cards at the point of sale or at ATMs.[57] Intervention methods aimed at user authentication may reduce the success of keylogging and phishing attacks, and therefore the availability of stolen data (the suitable targets). One example is Pico, which aims to increase the security of user accounts by replacing passwords and PINs with a token-based authentication system.[58] It is proposed that Pico, which is still under development, may also be used as an authentication system for smartcards,[59] therefore such a device may not only protect data from being stolen from individual accounts, but would also protect that data from being used, such as authenticating chip and PIN and card-not-present transactions. It is anticipated that there will be disruption in the market for stolen credit card credentials if there is an increase the effort required for their subsequent use.

In some cases, technical measures are available to safeguard data but are not effectively implemented. For example, a study by Mirante and Cappos[60] into high-profile data breaches found that many organisations did not use best practice when storing user credentials. Data stored in plaintext requires no extra effort on behalf of those with access to the database to obtain credentials including passwords and payment data, and hashed data that have not been salted, by way of adding random data, can be cracked using brute force. By improving the security by which data are stored, transmitted, and used by individual users as well as by the organisations that hold their data, the availability of products to sell is reduced and the effort required to obtain useable stolen data is increased.

Banks use fraud detection methods to identify suspicious transactions on credit cards, or against merchants.[61] Hutchings and Holt[62] identified that actors on the stolen data markets were concerned about fraud detection methods, which reduce the expected benefits. Tutorials are provided on forums providing information about how fraud detection systems work, discussions about gaining employment at target organisations to learn more about them, and advising that using credit card checkers may ultimately be counterproductive as cards may be more likely to be subsequently detected. In addition to suspicious credit card transactions, banks and other financial institutions have the capacity to detect other suspicious transactions, such as those undertaken by money mules or for the purposes of money laundering.

Banks are increasingly proactive in fraud detection among their card-holders, increasing their capability of guardians, by monitoring marketplaces for cards that they have issued. According to The Economist,[63] banks are purchasing credit card credentials to detect those entering the black market. There could potentially also be scope for banks to covertly advertise credit card checkers on black markets, if they are not already doing so, to identify compromised credit cards that are being checked before being sold on.

Merchants may also be guardians for stolen data, particularly as they usually carry the financial burden of card-not-present payment fraud. Merchants may employ their own fraud detection methods, and can also pay for subscription services that allow them to perform additional checks such as address and card verification.[64] In relation to carding, there are often multiple merchants that are targeted: first is the merchant that is used for checking to see if the credit card details are valid; second are the merchants that are subsequently targeted for purchasing goods that the offender exchanges for a monetary benefit. Popular websites, including charities, are used to make small transactions that are unlikely to be detected by fraud detection systems in real time.[65] Card checkers are available as a service, which operate using botnets. Peacock and Friedman[66] argue that if merchants that are targeted for checking credit card services are better able to protect themselves, can help prevent further fraud from taking place.

Peacock and Friedman[67] suggest that merchants utilise anti-automation technology for online credit card transactions to stop botnets automating credit card transactions. This would require offenders to test cards manually, increasing the effort, cost and time involved. Time is one of the crucial elements in this approach, as when cards are tested in batches, by the time the entire batch has been tested, it is more likely that those tested at the beginning will have been caught by fraud detection systems. Anti-automation technologies utilise CAPTCHAs, reputation methods, proof of work problems, and real time polymorphic web content.[68] However, the approach put forward by Peacock and Friedman[69] assumes that credit cards are being sold, and checked, in large batches, which may not always be the case.

The stolen data market economy includes the sale of identification documents.[70] ‘Scanned’ digital forgeries, as well as real and counterfeit documents, such as drivers licences and passports, are advertised for sale. In Australia, the federal government established the Document Verification Service as a countermeasure against fake identity documents. This service allows government agencies, as well as financial and telecommunication organisations, to cross reference government issued documents, such as birth certificates, citizenship certificates, driver licenses, marriage certificates, passports, and visas, to validate their authenticity.[71] While this may be an effective intervention to identify counterfeit identity documents, and increase the perceived likelihood of detection, it does not detect the use of stolen documents, or those where the backend database has been tampered with.

A number of regulatory approaches may also have positive effects in preventing acts associated with the online marketplaces. Those reviewed here include data breach notifications, regulations relating to payment providers, and money laundering regulations. Mandatory data breach notification requirements have been introduced to a number of jurisdictions worldwide, albeit with differing requirements.[72] One of the rationales for data breach notification is that end users are in a position to identify any suspicious activity relating to their accounts or credit histories, and can therefore intervene to reduce subsequent misuse of the data. To empirically assess whether mandatory data breach reporting reduces identity theft, Romanosky, Telang, and Acquisiti[73] compared levels of identity theft reported in states that had data breach notification laws with levels reported in states that did not. Data were sourced from the US Federal Trade Commission's Identity Theft Data Clearinghouse, which collects identity theft complaints from victims, across a period of eight years (2002 to 2009). The study found that, controlling for the extent that data breach notification increases the likelihood of identity theft victimisation being detected and subsequently reported, adoption of data breach disclosure laws reduced identity theft caused by data breaches by a statistically significant amount of 6.1 percent, on average.[74]

Another area for tighter regulation is the payment mechanisms used by actors to purchase goods, receive payments, and to launder the proceeds. There are a multitude of payment providers and digital currencies listed on online black markets for these purposes.[75] There is certainly scope to increase regulations for payment providers so that further steps are taken to minimise their involvement in black markets and reduce expected benefits to offenders. For example, Western Union do not require identification when sending amounts (less than £600); for receiving and sending amounts less than £1999.99, two forms of non-primary identification, such as a utility bill or a confirmation letter from a hotel are accepted.[76] As noted, multiple forms of primary and secondary identification, including drivers licences and passports, are readily available in online black markets.[77] Unlike Western Union, which is based on traditional currencies and therefore more likely to be subject to local regulatory agencies, digital currencies are less likely to be regulated. However, it is noted that two digital currency providers, Liberty Reserve and e-gold, were alleged to facilitate money laundering and online crime, and were shut down amid United States prosecutions.[78]

Money laundering is regulated in many countries, with requirements for banks and other agencies to report transactions that exceed a certain amount, as well as other 'suspicious transactions'. However, such requirements may be circumvented by making transactions appear legitimate,[79] as well as techniques such as 'smurfing', whereby multiple smaller transactions are processed using different identities. Therefore, there is scope for improving money laundering regulations, including reviewing how they apply to digital currencies.

Other ways in which those with ownership of the online black market problem could consider infiltrating the marketplace include advertising as drops, who receive stolen goods; as hammerers, who enter stolen card data; and as mules, to receive stolen goods. This could potentially allow for the recovery of stolen goods, as well as identifying stolen credit card details. While the principal aim of such intervention would be fraud detection, information obtained in such a way could also be used for investigative purposes.

The ownership of some of the strategies referred to above belong to organisations. For example, while individuals are the users of multifactor identification, it is companies that implement these systems. However, end users can also take ownership of crime prevention strategies by detecting fraudulent email messages, unusual computer behaviour that may indicate malware infection, and avoiding low security websites. Individuals may also be recruited into the black market economy using work-from-home scams, to receive carded goods and to participate in money laundering as an unwitting mule. Therefore, interventions aimed towards end users focus on the provision of fraud awareness, as well as tools to block access to malicious emails, websites or software.

Interventions aimed at the Actor

A number of disruption techniques have been proposed to promote distrust within marketplaces, and therefore reduce motivated offenders. Several of these techniques relate to creating the appearance of mistrust between buyers and sellers, referred to as 'lemonising the market'.[80] A lemon market is one in which there is quality uncertainty; therefore those selling quality products are unable to differentiate from sellers with poor quality products, and cannot compete with their low prices.[81] As a result, engaging in the market would increase the effort and cost of crime for buyers, and reduce their expected benefits.

Franklin, et al.[82] suggested that marketplaces can be lemonised using Sybil and slander attacks to create quality uncertainty. A Sybil attack involves the creation of multiple fictitious actors, who generate a positive reputation by undertaking fictitious transactions and providing feedback to one another. When non-fictitious actors request to purchase goods, payment is accepted, however the goods are never received. The fictitious seller will then generate negative feedback for being a ripper, which is argued would generate distrust in the marketplace. Hoe, et al.[83] suggested an extension of the Sybil attack. Named the 'fake peach' attack, in this variation law enforcement engage in actual sales so as to identify and take action on actors purchasing stolen data.

However, there are a number of potential problems with the Sybil and fake peach attacks. One such problem is that the fictitious actors first generate a positive reputation by leaving false feedback. While this may lead to distrust in positive feedback in the long term, Holt, et al.[84] found that sellers with positive feedback had significantly higher advertised prices for dumps, eBay and PayPal credentials, and that 'ripper' forums, which were characterised by high levels of negative feedback, had significantly lower advertised prices. Therefore, the Sybil attack may be advantageous to other sellers on the marketplace due to the positive feedback that is being left on the forums. In addition, there may be legitimacy concerns in relation to accepting payment for goods with either no intention to deliver, or delivering fake data. However, the slander attack may overcome these obstacles.

The slander attack involves leaving false feedback for sellers claiming that they are rippers.[85] This attack increases the effort required by sellers, and decreases their potential profits and benefits. It also increases the perceived risk to buyers that the seller is a ripper, increasing the difficulty inherent in participating in the market. Another variation on the Sybil attack may be to undertake the first action, and flood the marketplace with fictitious actors, but to not complete the remainder of the attack. Therefore, the fictitious advertisers do not generate a positive reputation and, by not replying to those who wish to purchase their products or services, create frustration with the marketplace, and potentially negative feedback. This solves the aforementioned problems of increasing the apparent number of sellers with positive feedback on a marketplace, and no payment exchanges hands. One potential problem with this approach is that a carefully moderated board may ban or blacklist sellers that do not provide data for a check. However, they may not have verified sellers participating in the site or do not have sellers who actively engage in the checking process.[86]

Nevertheless, Herley and Florêncio[87] suggest that, as the online black market is already essentially a lemon market, market participants are themselves conducting Sybil attacks. This could at least be the case in lower tier marketplaces, while higher tier marketplaces would be harder to enter. By disrupting lower-tier markets by lemonising them, it could increase the effort required by both buyers and sellers in gaining entry to the higher tier marketplaces.

The crime script developed by Hutchings and Holt[88] provides additional insights into the marketplace that can lead to further disruption and intervention strategies. Other potential ways to create distrust in the marketplace is to highlight the insecurity of the products and services sold on the marketplace, some of which are used to steal data. The legitimacy of this approach does not need to be questioned, as the security concerns are real. Research has shown that backdoors have been written into phishing kits,[89] which are both sold on the marketplaces and used to obtain stolen data. The backdoor consists of an obfuscated email address, to which the creator of the kit receives the credentials that have been obtained during the phishing attempt.

Similarly, in 2012, Slowloris, a denial of service tool, was found to include the Zeus Trojan.[90] More recently, the trustworthiness of the encryption software TrueCrypt has been questioned after a post appeared on the official website claiming that it was not safe to use.[91] By highlighting real or potential insecurities, they can be leveraged to generate mistrust and increase the perceived risk. An alternative approach, with the appropriate judicial authority and oversight, is to gain control over such backdoor destinations, with the ongoing goal of identifying compromised accounts. These can then be flagged with the account provider, such as the bank or financial institution. By blocking the accounts for subsequent misuse, the benefits for the purchaser of the stolen data can be subsequently decreased.

Additional ways to generate distrust in the market could include fictitious actors making fictitious claims, questioning reputations, providing false information, and promoting distrust in competing marketplaces. Fictitious claims could include that a product has been sent for verification but that the moderator took it and never provided a review, that other actors' accounts have been taken over by law enforcement or competitors, or that card checkers are used to steal credit card credentials. Questioning reputations could include suggesting that positive feedback had been bought or was actually posted by the seller, or questioning the (il)legitimacy of the marketplace administers.

Providing false information could include tutorials for matters in relation to specialist knowledge that frustrates others' efforts, and disseminating information about how to package goods, which actually makes them appear distinctive and easier to identify in transit. In addition to false information, providing real information about law enforcement activities to increase perceived risk could entail publicising arrests and successful prosecutions. Finally, as it would be expected that moderators would remove defaming posts relating to their own marketplaces, it could be claimed that competing marketplaces are not trustworthy.

Prosecuting offenders is another way of disrupting actors on online black marketplaces. The aim of law enforcement operations in this regard would be deterrence, both specific (deterring offenders from re-offending) and general (deterring others from commencing or continuing offending). There is some literature in relation to online offenders that indicate that it is the likelihood of detection that has the greatest deterrent effect, rather than the harshness of the available punishment.[92] In relation to cybercrime, challenges faced by law enforcement include having the necessary resources and powers to investigate complex matters, the time required to conduct cross-jurisdictional investigations and obtain evidence using current procedures, and recruiting, training, and retaining personnel with the appropriate skills.[93] These challenges may influence prosecution rates. Inconsistent laws and police resources also allow offenders to base their operations or select their victims in jurisdictions where they are least likely to be detected or prosecuted.[94] This in turn may have implications on the amount of crime that occurs online if perpetrators believe that they can offend with impunity, and negative effects for the reputation of policing agencies.

Faced with such challenges, there are a number of matters to take into consideration when selecting which offenders to target. First, law enforcement may select a particular marketplace to target, such as the FBI's DarkMarket operation. The second option is to target particular individuals, or groups of individuals who work together, whether they are operating in one or several marketplaces. Anderson[95] proposes randomised enforcement, whereby low value or low volume offenders are just as likely to be prosecuted as more serious offenders. The argument is that by randomly selecting complaints to investigate, it provides the opportunity to identify large-scale frauds that may otherwise escape scrutiny because of the low values involved, or alternatively will have a greater deterrence effect, in that even low-level offenders will see that there is a risk inherent in offending of being detected.

Although there are challenges faced by police, electronic data may be particularly useful for investigative purposes. For example, financial investigation techniques can be effective in detecting the extent of offenders' activities,[96] and transactions using Bitcoin are particularly open to traffic analysis.[97] Further investigative tools being developed include a method to detect associations between actors on online black markets, or users with multiple accounts, using stylometry to identify similarities in writing style.[98]

It is apparent that corruption is one element that enables the black market economy, presumably decreasing the perceived likelihood of detection, as well as the effort required. Hutchings and Holt[99] identified a number of organisational types that were discussed on the forums as either having employees that would assist in the black market economy, such as law enforcement and customs agents, bank employees, and sales staff who operate point of sale terminals (to either skim credit cards, or collude and conduct fraudulent transactions). Other organisations were identified as targets: places to attempt to gain employment as corrupt insiders, so as to access the organisation's systems and data. Conductors on public transport in Russia were also identified as playing a role in transporting plastics locally.[100] Law enforcement have a dual advantage in implementing anti-corruption strategies within their own agencies, as not only may it disrupt the black market economy, but by reducing corruption, and being transparent about the process, there should be positive effects in relation to perceived legitimacy.

McCusker[101] argues that successfully addressing systematic corruption requires a systematic approach. Not only do governments need to recognise and prioritise corruption, but they also require assistance in developing and implementing policy. Some of the specific initiatives that McCusker[102] recommends include establishing an anti-corruption agency, ensuring adequate pay, staff rotation, ensuring staff are not politically appointed, creating disincentives for corruption, removing opportunity, increasing transparency, and addressing cultural issues within the organisation. Smith and Jorna[103] note that, as computer systems are used for communication and the execution of corrupt activities, they can also incorporate measures to prevent and detect corruption, such as internally restricting access to data, or monitoring when and from where computer systems are accessed. Organisations targeted by would-be corrupt insiders may also find that background checks undertaken at the time of recruitment increase their ability to guard their computer systems and processes that would otherwise be valuable in the stolen data economy.

Interventions aimed at the marketplace

Marketplaces may be disrupted through censorship practices, or controlled by law enforcement. Interventions may also include disrupting the infrastructure, including communication, and anonymity systems. Censorship and Internet filtering may reduce marketplace visibility and availability, at least to those under the relevant regime who do not have the prerequisite knowledge to overcome censorship technologies. Murdoch and Anderson[104] outline the various filtering mechanisms available, such as TCP/IP header filtering, TCP/IP content filtering, DNS tampering, and http proxy filtering. These interventions increase the effort required by sellers and buyers to visit online marketplaces.

Alternative disruption interventions that also block access to websites instead increase the effort required by administrations to keep a site running. These include domain deregistration and server takedown.[105] Domain deregistration is possible if the site is registered under the domain of a country that prohibits the hosted content. However, it appears that the operation of online black markets may not be prohibited in all locations. For example, the terms and conditions for .ru (Russian) top level domains refers to deregistration of domain names for phishing pages, botnet control and child exploitation material.[106] Therefore, there is the potential for displacement to top level domains with more lenient abuse provisions. Similarly, server takedown requires that the hosted content be objectionable under the jurisdiction of the physical location of the server.[107]

In relation to censorship, whether that be by Internet filtering, domain deregistration and server takedown, a number of legitimacy concerns may be raised. These include the process by which sites are deemed to be offensive, how the public can be assured that content is not being blocked that should not be, and about freedom of access to information. There are also a number of ways that censorship and filtering may be overcome, including displacement to VPNs and anonymity networks, such as Tor or I2P. Law enforcement may operate VPNs to observe traffic, use an informant, as they did with the Shadowcrew takedown,[108] or obtain logs from VPN providers, as they did with an investigation into the compromise of data held by Sony Pictures.[109] However, talk on the forums indicate that some actors are displacing from VPNs to other systems, such as Tor and botnet-based proxy services, as they no longer trust VPN providers.

Anonymity networks may be used when visiting online black markets. Tor can also be used to hide the location of services, including some online black market forums. Hidden services are then accessed through the Tor network. Some attacks on the Tor network that reveal the location of hidden services have been published.[110] Hidden services themselves may also be attacked, such as by installing drive-by-downloads that reveal details about visitors,[111] and the Firefox browser has reportedly been attacked to target Tor users.[112] Exit nodes may be operated to read unencrypted packets exiting the network,[113] and other attacks against the Tor network have been reported.[114] Again, there are concerns about the legitimacy of attacks against the Tor network, which is also used for legal and pro-social purposes.

The final intervention strategy directed towards marketplaces is law enforcement control of marketplaces for the purposes of investigation and, ultimately, prosecution. This may be achieved directly, as in the DarkMarket example, or through the use of informants, such as the Shadowcrew approach.[115] Although costly, in terms of time and resources, further prosecutions may undo the belief that law enforcement do not, or cannot, act in relation to these offence types. Prosecutions relating to the Silk Road marketplace highlight the importance that law enforcement actions are perceived as legitimate, with allegations that the FBI acted unlawfully when obtaining evidence.[116] Whether or not a court of law agrees with these allegations, or even considers them, does not decrease the online chatter about the proceedings, or necessarily affect the public's perceptions of legitimacy.

Discussion and conclusion

As the problem of cybercrime continues to gain prominence among law enforcement agencies, there is a need to understand how various crimes may be best disrupted and affected. In particular, the economic harm caused by stolen data markets where individuals buy and sell financial information to others around the world cannot be underestimated. This paper investigates and considers the range of recommendations that have been proposed to disrupt both the actors and the markets where information is sold.

The paper demonstrates that law enforcement agencies and other guardians need to evaluate what intervention opportunities are appropriate. Multiple interventions coordinated across different guardians, nationally and internationally, incorporating different bodies (investigative, regulatory, strategic, non-government organisations, and the private sector) that have ownership of the crime prevention problem may reduce duplication of effort, as well as provide a more systematic approach with the greatest disruption effect.

At present, there is virtually no criminological inquiry with respect to evaluations of cybercrime intervention strategies, or prevention programs generally. Such research is, however, pivotal to ensure a technique or strategy is effective, delivering value for money, and that there are no unforeseen or undesirable consequences. There is also need for evaluating perceptions of legitimacy and the fairness of the processes in which decisions are being made, how power is being exercised as well as oversight and supervision of powers.

Considerations relating to legitimacy, the rights of the law-abiding majority, as well as judicial oversight, are relevant to all of the disruption and intervention methods. For example, in relation to the legitimacy of attacks lemonising the market, questions may be raised about targeting individuals who had not been found to have committed a crime by a court of law. Attacks against the infrastructure used to access these places, such as the Tor network, for the purpose of disrupting harmful behaviours (the trade in stolen data) may also be used to target those whose goals are not so nefarious, such as those seeking to avoid censorship, uncovering state wrongdoings, or bringing about positive change within repressive regimes. Mass surveillance and data collection using backdoors and malware may also result in backlash, particularly when the investigative approach is not targeted and where there is no judicial oversight, such as a warrant for surveillance devices and communication interception.

Although varied, the disruption methods outlined in this paper aim to increase the effort, increase the perceived risk, and reduce the benefits for crime. The disruption methods against actors would be easier to undertake in open marketplaces where there is less access control, and therefore the cost of being banned for the disruption activities is not as high. While marketplaces may change their methods and become closed, or those operating on those marketplaces may displace to more closed forums, both of these outcomes increase the required effort for motivated offenders, and may limit the number of actors that participate. It appears that low tier, open marketplaces are already doing well at disrupting their own economies by being known for their rippers. Promoting distrust in these marketplaces may assist with this process.

Though these prospective techniques may be valuable, there is virtually no research empirically assessing the application of these techniques in active markets. Furthermore, there may be additional disruption methods not covered in this paper. As a result, there is a need for substantive evaluation of the utility of market disruption strategies. This can only be achieved through direct coordination with law enforcement agencies and active research pre and post-intervention. Future research exploring these issues with active markets will improve our knowledge of the validity of these strategies and demonstrate avenues for future research on cybercrime.

Funding

This work was supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific under contract number N66001-13-C-0131, to A.H.; and the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice under grant number 2010-IJ-CX-1676, 2010, to T. H. The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

Acknowledgements

The work would not have been possible without the invaluable assistance of Richard Clayton, Ross Anderson, Mike Bond, Ian Goldberg, and Jeunese Payne.

Notes

[1] Brenner, "Fantasy crime"; Holt and Bossler, "An assessment"; and Wall, "Maintaining order and law".

[2] Holt and Blevins, "Examining sex work"; and Sanders "Selling sex".

[3] Burns, Whitworth and Thompson, "Assessment law enforcement preparedness"; and Newman and Clarke, *Superhighway Robbery*.

[4] Bocij, *Cyberstalking: Harassment*; Reyns, Henson and Fisher, "Stalking in the twilight"; and Finn, "Survey of online harassment".

[5] Bachmann, "Deciphering the hacker underground"; Holt, "Subcultural evolution"; and Schell and Dodge, *The hacking of America*.

[6] Franklin et al., "An inquiry"; Holt and Lampke, "Exploring stolen data markets"; Hutchings and Holt, "A crime script analysis"; and Peretti, "Data breaches".

[7] For example, Ponemon Institute, *Cost of Data Breach*.

[8] Higgins, "Target, Neiman Marcus Data"; Pauli, "Oz privacy comish says"; and Seals, "2014 so far".

[9] Franklin et al., "An inquiry"; Holt and Lampke, "Exploring stolen data markets"; Peretti, "Data breaches"; Motoyama et al., "Analysis of underground forums"; and Wehinger, "The dark net".

[10] Wehinger, "The dark net"; and Symantec Corporation, *Internet Security Threat Report*.

[11] Holt and Lampke, "Exploring stolen data markets"; and Peretti, "Data breaches".

[12] Franklin et al., "An inquiry"; and Holt and Lampke, "Exploring stolen data markets".

[13] see Holt, Smirnova and Chua, "Revenues and profits"; Ponemon Institute, *Cost of Data Breach*; Symantec Corporation, *Internet Security Threat Report*.

[14] Franklin et al., "An inquiry"; and Holt and Smirnova, "Examining the Structure, Organization".

[15] For example, Peretti, "Data breaches"; and Poulsen, *Kingpin: the true story*.

16 Glenny, *Darkmarket, Cyberthieves, Cybercops*.

17 Rawlinson, “Websites linked to $500m”.

18 See Peretti, “Data breaches”.

19 Franklin et al., “An inquiry”; Holt and Lampke, "Exploring stolen data markets"; Holt and Smirnova, “Examining the Structure, Organization”; Motoyama et al., "Analysis of underground forums"; Peretti, "Data breaches"; Wehinger, "The dark net."

20 Hutchings and Holt, “A crime script analysis”.

21 Chiu, Leclerc and Townsley, “Crime script analysis of”; Cornish, “Crime as scripts”; Hancock and Laycock, “Organised crime and crime”; Leontiadis and Hutchings, “Scripting the crime”; and Morselli and Roy, “Brokerage qualifications”.

22 Hutchings and Holt, “A crime script analysis”.

23 Cornish, “Procedural analysis of offending”.

24 Levi and Maguire, “Reducing and preventing organized”.

25 Cohen and Felson, “Social change and crime”.

26 Cornish and Clarke, “Understanding crime displacement”.

27 Gibbs, *Crime, Punishment and Deterrence*.

28 Jacobs, “Deterrence and Deterrability”.

29 Gibbs, *Crime, Punishment and Deterrence*.

30 Chiu, Leclerc and Townsley, “Crime script analysis of”.

31 Leclerc, Wortley and Smallbone, “Getting into the script”.

32 Hancock and Laycock, “Organised crime and crime”.

33 Chiu, Leclerc and Townsley, “Crime script analysis of”.

34 Leclerc, Wortley and Smallbone, “Getting into the script”.

35 Hancock and Laycock, “Organised crime and crime”.

36 Hutchings and Holt, “A crime script analysis”.

37 Cohen and Felson, “Social change and crime”.

38 Levi and Maguire, “Reducing and preventing organised”.

39 Levi and Maguire, “Reducing and preventing organised”.

40 Bossler and Holt, “The effect of self-control”; Bossler and Holt, “On-line activities, guardianship”; Holt and Bossler, “An assessment”; Wall, “Maintaining order and law”; and Holt and Bossler, “Examining the applicability”.

41 For example, Peretti, “Data breaches”; and Wall, *Cybercrime: The Transformation”*.

42 Garland, “Limits of the sovereign”.

43 Sunshine and Taylor, “Role of procedural justice”.

44 Grabosky, “Secrecy, transparency and legitimacy”.

45 Tyler, “Enhancing police legitimacy”.

46 Grabosky, “Secrecy, transparency and legitimacy”.

47 Sunshine and Taylor, “Role of procedural justice”.

48 Furnell, *Cybercrime: Vandalizing the Information*; and Holt, Bossler and Fitzgerald, “Examining state and local”.

49 Holt, Bossler and Fitzgerald, “Examining state and local”.

50 See also Wilson, Walsh and Kleuber, “Trafficking in human beings”.

51 Hancock and Laycock, “Organised crime and crime”.

52 Smith, Wolanin and Worthington, *e-Crime Solutions and Crime*.

53 Holt, Blevins and Kuhns, “Examining diffusion and arrest”.

54 Peacock and Friedman, “Automation and disruption”.
55 Herley and Florêncio, “Nobody sells gold”; and Wehinger, “The dark net”.
56 Hutchings and Holt, “A crime script analysis”.
57 Hutchings and Holt, “A crime script analysis”.
58 Stajano, “Pico: no more passwords!”
59 Stajano, “Pico: no more passwords!”
60 Mirante and Cappos, “Understanding password database compromises”.
61 Peacock and Friedman, “Automation and disruption”.
62 Hutchings and Holt, “A crime script analysis”.
63 The Economist, “Banks and fraud”.
64 Peacock and Friedman, “Automation and disruption”.
65 Peacock and Friedman, “Automation and disruption”.
66 Peacock and Friedman, “Automation and disruption”.
67 Peacock and Friedman, “Automation and disruption”.
68 Peacock and Friedman, “Automation and disruption”.
69 Peacock and Friedman, “Automation and disruption”.
70 Hutchings and Holt, “A crime script analysis”.
71 Attorney-General’s Department, “Document Verification Service”.
72 Maurushat, “Data breach notification law”.
73 Romanosky, Telang and Acquisti, “Do data breach disclosure”.
74 Romanosky, Telang and Acquisti, “Do data breach disclosure”.
75 Hutchings and Holt, “A crime script analysis”.
76 Western Union, “What is considered valid”.
77 Franklin et al., “An inquiry”; Holt and Lampke, “Exploring stolen data markets”; Hutchings and Holt, “A crime script analysis”; and Motoyama et al., “Analysis of underground forums”.
78 Samani, Paget and Hart, *Digital Laundry.*
79 Newman and Clarke, *Superhighway Robbery*.
80 Hoe, Kantarcioglu and Bensoussan, “A game theoretical analysis”.
81 Akerlof, “The market for ‘lemons’”.
82 Franklin et al., “An inquiry”.
83 Hoe, Kantarcioglu and Bensoussan, “A game theoretical analysis”.
84 Holt, Chua and Smirnova, “Exploration of the factors”.
85 Franklin et al., “An inquiry”.
86 Holt and Smirnova, “Examining the structure, organization”; and Hutchings and Holt, A crime script analysis”.
87 Herley and Florêncio, “Nobody sells gold”.
88 Hutchings and Holt, “A crime script analysis”.
89 McCalley, Wardman and Warner, “Analysis of back-doored”; and Chu, Holt and Ahn, *Examining the Creation, Distribution*.
90 Bangeman, “Slowloris DDoS tool”.
91 Goodin, “Bombshell TrueCrypt advisory”
92 Hollinger, “Crime by computer”; Hutchings, *Theory and Crime*; and Skinner and Fream, “Social learning theory analysis”.
93 Smith, *Cross-Border Economic Crime*.
94 Smith, *Cross-Border Economic Crime*.
95 Science and Technology Committee, *Personal Internet Security.*
96 Brown et al., *Contribution of Financial Investigation*.
97 Christin, “Traveling the Silk Road”.

98 Afroz et al., “Doppelgänger Finder”.
99 Hutchings and Holt, “A crime script analysis”.
100 Hutchings and Holt, “A crime script analysis”.
101 McCusker, *Review of anti-corruption strategies*.
102 McCusker, *Review of anti-corruption strategies*.
103 Smith and Jorna, “Corrupt misuse of information”.
104 Murdoch and Anderson, “Tools and technology”.
105 Murdoch and Anderson, “Tools and technology”.
106 Coordination Centre for TLD RU, “The terms and conditions”.
107 Murdoch and Anderson, “Tools and technology”.
108 Glenny, *DarkMarket: Cyberthieves, Cybercops.*
109 Martin, “LulzSec hacker exposed”.
110 Biryukov, Pustogarov and Weinmann, “Trawling for Tor hidden”; Christin, “Traveling the Silk Road”; Jansen et al., “The sniper attack”; Murdoch, “Hot or not”; and Øverlier and Syverson, “Locating hidden servers”.
111 Poulsen, “Visit the wrong website”.
112 Schneier, How the NSA attacks”.
113 McCoy et al., “Shining light in dark”.
114 Menn, “Talk on cracking Internet”.
115 Glenny, *DarkMarket: Cyberthieves, Cybercops.*
116 Kravets, “Are the FBI and”; Kravets, “US says it can”; and Krebs, “Silk Road lawyers poke”.

References

Afroz, Sadia, Aylin Caliskan-Islam, Ariel Stolerman, Rachel Greenstadt, and Damon McCoy. "Doppelgänger Finder: Taking Stylometry to the Underground." In *IEEE Symposium on Security and Privacy*. San Jose, 2014.

Akerlof, George A. "The Market for" Lemons": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84, no. 3 (1970): 488-500.

Attorney-General's Department. "Document Verification Service." http://www.dvs.gov.au/Pages/default.aspx

Bachmann, Michael. "Deciphering the Hacker Underground: First Quantitative Insights." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas J Holt and Bernadette H Schell, 105-26. Hershey: Information Science Reference, 2010.

Bangeman, Eric. "Slowloris Ddos Tool Used by Anonymous Hacked to Include Zeus Trojan." http://arstechnica.com/tech-policy/2012/03/slowloris-ddos-tool-used-by-anonymous-hacked-to-include-zeus-trojan/

Biryukov, Alex, Ivan Pustogarov, and R Weinmann. "Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization." Paper presented at the IEEE Symposium on Security and Privacy, San Francisco, May 19-22 2013.

Bocij, Paul. *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Westport: Greenwood Publishing Group, 2004.

Bossler, Adam M, and Thomas J Holt. "The Effect of Self-Control on Victimization in the Cyberworld." *Journal of Criminal Justice* 38, no. 3 (2010): 227-36.

Bossler, Adam M, and Thomas J Holt. "On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory." *International Journal of Cyber Criminology* 3, no. 1 (2009): 400-20.

Brenner, Susan W. "Fantasy Crime: The Role of Criminal Law in Virtual Worlds." *Vanderbilt Journal of Entertainment and Technology Law* 11, no. 1 (2008): 1-97.

Brown, Rick, Emily Evans, Sarah Webb, Simon Holdaway, Geoff Berry, Sylvia Chenery, Brian Gresty, and Mike Jones. *The Contribution of Financial Investigation to Tackling Organised Crime: A Qualitative Study*. London: Home Office, 2012.

Burns, Ronald G., Keith H. Whitworth, and Carol Y. Thompson. "Assessing Law Enforcement Preparedness to Address Internet Fraud." *Journal of Criminal Justice* 32, no. 5 (2004): 477-93.

Chiu, Yi Ning, Benoit Leclerc, and Michael Townsley. "Crime Script Analysis of Drug Manufacturing in Clandestine Laboratories: Implications for Prevention." *British Journal of Criminology* 51, no. 2 (2011): 355-74.

Christin, Nicolas. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." Paper presented at the Proceedings of the 22nd international conference on World Wide Web, 2013.

Chu, Bill, Thomas J. Holt, and Gail Joon Ahn. *Examining the Creation, Distribution and Function of Malware on-Line*. Technical Report for National Institute of Justice. NIJ Grant No. 2007-IJ-CX-0018., 2010.

Cohen, Lawrence E., and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44, no. 4 (1979): 588-608.

Coordination Centre for TLD RU. "The Terms and Conditions of Domain Names Registration in Domains .Ru And .Рф." http://cctld.ru/en/docs/rules.php

Cornish, Derek B. “Crime as scripts”. In *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*. Tallahassee, 1994.

Cornish, Derek B. "The Procedural Analysis of Offending and Its Relevance for Situational Prevention." In *Crime Prevention Studies* edited by Ronald V Clarke, 151-96. Monsey: Criminal Justice Press, 1994.

Cornish, Derek B., and Ronald V. Clarke. "Understanding Crime Displacement: An Application of Rational Choice Theory." *Criminology* 25, no. 4 (1987): 933-47.

Finn, Jerry. "A Survey of Online Harassment at a University Campus." *Journal of Interpersonal violence* 19, no. 4 (2004): 468-83.

Franklin, Jason, Vern Paxson, Adrian Perrig, and Stefan Savage. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." In *ACM Conference on Computer and Communications Security (CCS), 375– 388*, 2007.

Furnell, Steven. *Cybercrime: Vandalizing the Information Society*. London: Pearson Education Limited, 2002.

Garland, David. "The Limits of the Sovereign State." *The British Journal of Sociology* 36, no. 4 (1996): 445-71.

Gibbs, Jack P. *Crime, Punishment and Deterrence*. New York: Elsevier Scientific Publishing Company, Inc, 1975.

Glenny, Misha. *Darkmarket: Cyberthieves, Cybercops and You*. London: The Brodley Head, 2011.

Goodin, Dan. "Bombshell Truecrypt Advisory: Backdoor? Hack? Hoax? None of the Above?" http://arstechnica.com/security/2014/05/bombshell-truecrypt-advisory-backdoor-hack-hoax-none-of-the-above/

Grabosky, Peter. "Secrecy, Transparency and Legitimacy." http://www.india-seminar.com/2014/655/655_peter_grabosky.htm

Hancock, Graham, and Gloria Laycock. "Organised Crime and Crime Scripts: Prospects for Disruption." In *Situational Prevention of Organised Crimes*, edited by Karen Bullock, Ronald V. Clarke and Nick Tilley, 172-92. Devon: Willan Publishing, 2010.

Herley, Cormac, and Dinei Florêncio. "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy." In *Economics of Information Security and Privacy*, edited by Tyler Moore, David Pym and Christos Ioannidis, 33-53: Springer, 2010.

Higgins, K J. "Target, Neiman Marcus Data Breaches Tip of the Iceberg." http://www.darkreading.com/attacks-breaches/target-neiman-marcus-data-breaches-tip-o/240165363

Hoe, SingRu Celine, Murat Kantarcioglu, and Alain Bensoussan. "A Game Theoretical Analysis of Lemonizing Cybercriminal Black Markets." In *Decision and Game Theory for Security*, 60-77: Springer, 2012.

Hollinger, Richard C. "Crime by Computer: Correlates of Software Piracy and Unauthorised Account Access." *Security Journal* 4, no. 1 (1993): 2-12.

Holt, Thomas J, and Kristie R Blevins. "Examining Sex Work from the Client's Perspective: Assessing Johns Using on-Line Data." *Deviant Behavior* 28, no. 4 (2007): 333-54.

Holt, Thomas J, Kristie R Blevins, and Joseph B Kuhns. "Examining Diffusion and Arrest Avoidance Practices among Johns." *Crime & Delinquency* 60, no. 2 (2014): 261-83.

Holt, Thomas J, AM Bossler, and S Fitzgerald. "Examining State and Local Law Enforcement Perceptions of Computer Crime." In *Crime on-Line: Correlates, Causes, and Context*, edited by Thomas J Holt, 221-46. Raleigh: Carolina Academic Press, 2010.

Holt, Thomas J, Yi-Ting Chua, and Olga Smirnova. "An Exploration of the Factors Affecting the Advertised Price for Stolen Data." Paper presented at the eCrime Researchers Summit (eCRS), 2013, 2013.

Holt, Thomas J, and Olga Smirnova. *Examining the Structure, Organization, and Processes of the International Market for Stolen Data*. 2014.

Holt, Thomas J., Olga Smirnova, and Yi Ting Chua. "Exploring and Estimating the Revenues of Profits of Participants in Stolen Data Markets." *Deviant Behavior* 37, no. 4 (2016): 353-367.

Holt, Thomas J. "Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures." *Deviant Behavior* 28, no. 2 (2007): 171-98.

Holt, Thomas J., and Adam M. Bossler. "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behavior* 35, no. 1 (2014): 20-40.

Holt, Thomas J., and Adam M. Bossler. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization." *Deviant Behavior* 30, no. 1 (2009): 1-25.

Holt, Thomas J., and Eric Lampke. "Exploring Stolen Data Markets Online: Products and Market Forces." *Criminal Justice Studies* 23, no. 1 (2010): 33-50.

Hutchings, Alice. "Theory and Crime: Does It Compute?", PhD diss., Griffith University, 2013.

Hutchings, Alice, and Thomas J Holt. "A Crime Script Analysis of the Online Stolen Data Market." *British Journal of Criminology* 55, no. 3 (2015): 596-614.

Jacobs, Bruce A. "Deterrence and Deterrability*." *Criminology* 48, no. 2 (2010): 417-41.

Jansen, Rob, Florian Tschorsch, Aaron Johnson, and Björn Scheuermann. "The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network." Paper presented at the Network and Distributed Systems Security Symposium (NDSS), San Diego, February 23-26 2014.

Kravets, David. "Are the Fbi and 'Weev' Both Hackers?" http://arstechnica.com/tech-policy/2014/09/are-the-fbi-and-the-weev-both-hackers/

Kravets, David. "Us Says It Can Hack into Foreign-Based Servers without Warrants." http://arstechnica.com/tech-policy/2014/10/us-says-it-can-hack-into-foreign-based-servers-without-warrants/

Krebs, Brian. "Silk Road Lawyers Poke Holes in Fbi's Story." http://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story/

Leclerc, Benoit, Richard Wortley, and Stephen Smallbone. "Getting into the Script of Adult Child Sex Offenders and Mapping out Situational Prevention Measures." *Journal of Research in Crime and Delinquency* 48, no. 2 (2011): 209-37.

Leontiadis, Nektarios, and Alice Hutchings. "Scripting the Crime Commission Process in the Illicit Online Prescription Drug Trade." *Journal of Cybersecurity* 1, no. 1 (2015): 81-92.

Levi, Michael, and Mike Maguire. "Reducing and Preventing Organised Crime: An Evidence-Based Critique." *Crime, Law and Social Change* 41, no. 5 (2004): 397-469.

Martin, Adam. "Lulzsec Hacker Exposed by Service He Thought Would Hide Him." http://www.thewire.com/technology/2011/09/lulzsec-hacker-exposed-service-he-thought-would-hide-him/42895/

Maurushat, A. *Data Breach Notification Law across the World from California to Australia. University of New South Wales Law Research Series Paper No. 11.* Sydney: University of New South Wales, 2009.

McCalley, Heather, Brad Wardman, and Gary Warner. "Analysis of Back-Doored Phishing Kits." In *Advances in Digital Forensics Vii*, 155-68: Springer, 2011.

McCoy, Damon, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. "Shining Light in Dark Places: Understanding the Tor Network." Paper presented at the Privacy Enhancing Technologies, Leuven, July 23-25 2008.

McCusker, Rob. *Review of Anti-Corruption Strategies*. Canberra: Australian Institute of Criminology, 2006.

Menn, Joseph. "Talk on Cracking Internet Anonymity Service Tor Withdrawn from Conference." http://www.reuters.com/article/2014/07/21/cybercrime-conference-talk-idUSL2N0PW14320140721

Mirante, Dennis, and Justin Cappos. "Understanding Password Database Compromises." Technical Report TR-CSE-2013-02, Department of Computer Science and Engineering Polytechnic Institute of NYU, 2013.

Morselli, Carlo and Julie Roy. "Brokerage Qualifications in Ringing Operations". *Criminology* 46, no. 1 (2008): 71-98.

Motoyama, Marti, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. "An Analysis of Underground Forums." In *2011 ACM SIGCOMM conference on Internet measurement*, 71-80. Berlin, Germany: ACM, 2011.

Murdoch, Steven J. "Hot or Not: Revealing Hidden Services by Their Clock Skew." Paper presented at the Proceedings of the 13th ACM conference on Computer and Communications Security, Alexandria, October 30-November 3 2006.

Murdoch, Steven J, and Ross Anderson. "Tools and Technology of Internet Filtering." In *Access Denied: The Practice and Policy of Global Internet Filtering*, edited by Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, 57-72. Cambridge: MIT Press, 2008.

Newman, GR, and Ronald V Clarke. *Superhighway Robbery: Preventing E-Commerce Crime*. Devon: Willan Publishing, 2003.

Øverlier, Lasse, and Paul Syverson. "Locating Hidden Servers." Paper presented at the 2006 IEEE Symposium on Security and Privacy, Oakland, 21-24 May 2006.

Pauli, Darren. "Oz Privacy Comish Says Breaches Could Be Double This Year." http://www.theregister.co.uk/2014/10/20/2014_a_bumper_year_for_aussie_breaches/

Peacock, Timothy, and Allan Friedman. "Automation and Disruption in Stolen Payment Card Markets." In *13th Annual Workshop on the Economics of Information Security*. Pennsylvania State University, 2014.

Peretti, Kimberly Kiefer. "Data Breaches: What the Underground World of Carding Reveals." *Santa Clara Computer & High Tech. LJ* 25 (2009): 375-413.

Ponemon Institute. *Cost of Data Breach Study: Global Analysis*. IBM, 2014.

Poulsen, Kevin. *Kingpin: The True Story of Max Butler, the Master Hacker Who Ran a Billion Dollar Cyber Crime Network*. Sydney: Hachette Australia, 2011.

Poulsen, Kevin. "Visit the Wrong Website, and the Fbi Could End up on Your Computer." http://www.wired.com/2014/08/operation_torpedo/

Rawlinson, Kevin. "Websites Linked to £500m Credit Card Fraud Shut Down by Police." http://www.independent.co.uk/news/uk/crime/websites-linked-to-500m-credit-card-fraud-shut-down-by-police-7681808.html

Reyns, Bradford W, Billy Henson, and Bonnie S Fisher. "Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending among College Students." *Deviant Behavior* 33, no. 1 (2012): 1-25.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. "Do Data Breach Disclosure Laws Reduce Identity Theft? (Updated)." *Journal of Policy Analysis and Management* 30, no. 2 (2011): 256-86.

Samani, Raj, François Paget, and Matthew Hart. *Digital Laundry: An Analysis of Online Currencies, and Their Use in Cybercrime*. Santa Clara: McAfee, 2013.

Sanders, Teela. "Selling Sex in the Shadow Economy." *International Journal of Social Economics* 35, no. 10 (2008): 704-16.

Schell, Bernadette H, and John L Dodge. *The Hacking of America: Who's Doing It, Why, and How*. Westport: Greenwood Publishing Group, 2002.

Schneier, Bruce. "How the NSA Attacks Tor/Firefox Users with Quantum and Foxacid." https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

Science and Technology Committee. *Personal Internet Security Volume II: Evidence*. London: House of Lords, 2007.

Seals. "2014 So Far: The Year of the Data Breach." http://www.infosecurity-magazine.com/news/2014-the-year-of-the-data-breach/

Skinner, William F., and Anne M. Fream. "A Social Learning Theory Analysis of Computer Crime among College Students." *Journal of Research in Crime and Delinquency* 34, no. 4 (1997): 495-518.

Smith, Russell G. *Trends & Issues in Crime and Criminal Justice No. 202: Cross-Border Economic Crime: The Agenda for Reform*. Canberra: Australian Institute of Criminology, 2001.

Smith, Russell G., and P Jorna. "Corrupt Misuse of Information and Communication Technologies." In *Handbook of Global Research and Practice in Corruption*, edited by Adam Graycar and R G Smith, 255-81. Cheltenham: Edward Elgar Publishing Limited, 2011.

Smith, Russell G., Nicholas Wolanin, and Glenn Worthington. *Trends & Issues in Crime and Criminal Justice No. 243: E-Crime Solutions and Crime Displacement*. Canberra: Australian Institute of Criminology, 2003.

Stajano, Frank. "Pico: No More Passwords!". Chap. 6 In *Security Protocols XIX*, edited by Bruce Christianson, Bruno Crispo, James Malcolm and Frank Stajano. Lecture Notes in Computer Science, 49-81: Springer Berlin Heidelberg, 2011.

Sunshine, Jason, and Tom R Tyler. "The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing." *Law & Society Review* 37, no. 3 (2003): 513-48.

Symantec Corporation. *Internet Security Threat Report*. Mountain View: Symantec Corporation, 2014.

The Economist. "Banks and Fraud: Hacking Back." http://www.economist.com/news/finance-and-economics/21600148-bankers-go-undercover-catch-bad-guys-hacking-back

Tyler, Tom R. "Enhancing Police Legitimacy." *The Annals of the American Academy of Political and Social Science* 593, no. 1 (2004): 84-99.

Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, 2007.

Wall, David S. "Maintaining Order and Law on the Internet." In *Crime and the Internet*, edited by David S. Wall, 167-83. London: Routledge, 2001.

Wehinger, Frank. "The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services." Paper presented at the Intelligence and Security Informatics Conference (EISIC), 2011 European, 2011.

Western Union. "What Is Considered Valid Identification to Pick up a Money Transfer?" http://www.westernunion.co.uk/gb/faq-send-money-in-person

Wilson, Deborah G, William F Walsh, and Sherilyn Kleuber. "Trafficking in Human Beings: Training and Services among Us Law Enforcement Agencies." *Police Practice and Research* 7, no. 02 (2006): 149-60.