Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs.

Jacqueline M Drew[a]* & Lucy Farrell[b]

[a] School of Criminology and Criminal Justice, Griffith Criminology Institute, Griffith University; [b] School of Criminology and Criminal Justice, Griffith Criminology Institute, Griffith University

ABSTRACT

The prevalence and impact of cyber fraud continues to increase exponentially with new and more innovative methods developed by offenders to target and exploit victims for their own financial reward. Traditional crime reaction methods used by police have proved largely ineffective in this context, with offenders typically located outside of the police jurisdiction of their victims. Given this, some police agencies have begun to adopt a victim focused, crime prevention approach to cyber fraud. The current research explores with a sample of two hundred and eighteen potential cyber fraud victims, the relationship between online victimization risk, knowledge and use of crime prevention strategies. The study found those most at risk of cyber fraud victimization despite accurate perceptions of risk and knowledge of self-protective behaviors in the online environment underutilise online prevention strategies. This research has important implications for police agencies who are designing and delivering cyber fraud education. It provides guidance for the development of effective prevention programs based on practical skills development.

Keywords

Cyber fraud; policing; victimization; crime prevention

Introduction

The use of the internet to engage in traditional activities, such as banking, entertainment, shopping, and even to establish and maintain social relationships is now commonplace (Bossler & Holt, 2009). A report published by the United Nations in 2016 indicated that 84% of the world population live in an area where mobile-broadband is available and 47% actively use the internet (United Nations, 2016).

It is widely acknowledged that the internet has provided increasing opportunities for criminals to commit crimes enabled by the online environment with the creation of new crimes and to perpetrate traditional crimes in new and innovative ways (Australian Government Attorney-General's Department, 2013; Broadhurst, 2006; Clough, 2015; Webster & Drew, 2017). Despite this, there is much still to be learnt about online victimization risk and in turn, online crime prevention (Grabosky, 2001; Reyns, 2010). The dearth of knowledge is particularly evident in the context of policing (Webster & Drew, 2017). Given the significant challenges in addressing crime across international borders, increasingly police will be expected to move away from traditional policing approaches that primarily target the apprehension of offenders (Cross & Blackshaw, 2015; Davidson & Martellozzo, 2008; Hinduja, 2004; Webster & Drew, 2017). As discussed in this paper, the nature of cybercrime necessitates the development of more effective approaches that involve investment in innovative, victim focused education and prevention activities.

The current study explores crime prevention activities of potential victims of online cyber fraud crimes. It is based on the premise that victims are the lynchpin in their own self-protection, and that police agencies can play an important role in reducing the prevalence of cyber fraud by supporting and encouraging potential victims to protect themselves against cyber fraud attacks. However, this approach requires an evidence-based understanding of both knowledge and use of online self-protective crime prevention behaviors that are being employed by online users. To date, little research has examined the translation of knowledge of online crime prevention behaviors into the actual use of online crime prevention strategies (Burns & Roberts, 2013). The current research is interested in exploring whether those most at risk of cyber fraud victimization develop increased knowledge of cyber fraud crime prevention strategies, and given their risk, whether they implement crime prevention strategies in practice. Understanding this translation of knowledge into practice is essential for those, such as police, who need to determine how to best design and allocate their resources to the education and interruption of online cyber fraud victimization and reduce the prevalence of cyber fraud crime.

Cyber Fraud: Definition and Prevalence

Whilst we continue to debate specific definitions of cybercrime, it is generally acknowledged that cybercrime is concentrated in two main categories (Clough, 2015). The first category captures crimes directed at computers or relevant information technologies (crimes that typically only exist in the online world). The second category includes crimes where computers or relevant information technologies are an integral part of the offense itself (this often includes traditional crimes that are facilitated or enhanced by the internet) (Australian Government Attorney-General’s Department, 2013; Clough, 2015; House of Representatives Standing Committee on Communications, 2010).

The current study focuses on cyber fraud as a subset of cybercrime. Cyber fraud can be understood using the two generic categories of cybercrime. Cyber fraud offenses under the first category, crimes directed at computers or other information communications technology (ICTs), includes illegal access, illegal interception, data interference, system interference, misuse of devices and hacking offenses (Australian Government Attorney-General’s Department, 2013). These offenses can be broadly considered as attacks against the hardware of the computer or ICTs. Cyber fraud offenses under the second category, are where computers or ICTs are integral to the offense and typically involve deception for the purpose of obtaining financial advantage (Australian Government Attorney-General's Department, 2013). These include advance fee fraud (e.g. romance scams, inheritance scams, investment scams, and fraudulent financial transactions) and identity theft (Australian Government Attorney-General's Department, 2013).

Turning to prevalence, on an international level cyber fraud is viewed as an extensive and complex crime type (Australian Government Attorney-General's Department, 2013; Council of Europe, 2004; Cybercrime Act 2001). The global growth of cyber fraud demonstrates that it is a new generation of criminality that is fast evolving, with new and sophisticated fraud schemes constantly emerging (Ionescu, Mirea, & Blajan, 2011). Cyber fraud or financial cybercrime began as simple scams and elementary phishing, typically through email, but has since developed into a sophisticated crime type (Ionescu et al., 2011). Cyber fraud offenders may employ highly developed software tools, increasingly well-crafted social engineering and psychological techniques and often group together in either organised or loosely associated cybercrime syndicates to enhance reach and efficiency (Broadhurst, 2006; Ionescu et al., 2011).

Whilst current research acknowledges that official published statistics surrounding cybercrime offenses are likely to be grossly underestimated due to significant underreporting, the statistics that are available, including victimization surveys show significant growth in cybercrime across the world (Cross, Smith & Richards, 2014; House of Representatives Standing Committee on Communications, 2010; Webster & Drew, 2017). Recently in the UK, cybercrime was for the first time included in the Crime Survey for England and Wales. The results indicated that fraud (online) and computer misuse are now the most commonly experienced offenses, overtaking traditional crimes such as burglary and theft of vehicles

(Office of National Statistics, 2017). The economic impact of online crime is also significant. Victim losses collated by the US Internet Crime Complaint Center (IC3) in 2016 totalled US$1.33 billion. In Australia, it has been conservatively estimated to be as high as AU$2 billion annually (Australian Government Attorney-General's Department, 2013). For cyber fraud and online financial scams alone, the Australian Consumer and Competition Commission (ACCC) (2016) estimated annual losses exceeding AU$300 million, a conservative estimate given this only captures reported victimization data.

Cyber fraud offenses have an immense impact on victims, even though the offender and victim typically never come into contact with each other in the physical world (Webster & Drew, 2017). This impact is undoubtedly financial, however the emotional and psychological impact for victims is also enormous (Australian Government Attorney-General's Department, 2013; Button, Lewis & Tapley, 2014; Cross et al., 2014; Webster & Drew, 2017). Further, users who fall victim to online scams are often repeatedly targeted thus experiencing high levels of re-victimization (Cross et al., 2014).

Given the growth in cyber fraud, there is, in turn, increasing need to focus on self-protective behaviors for both those who have already experienced cyber fraud victimization and those who are at risk. The following discussion explores why one of the most promising approaches to cyber fraud reduction involves more effective victim education. It is argued that victims need to be educated on how to best enact behaviors that minimise their suitability and vulnerability as crime targets (House of Representatives Standing Committee on Communications, 2010). Self-protective measures will be explored in this paper as a means of better understanding how to educate potential victims on how to recognise and reduce target suitability, focusing on the role of an individual in reducing their own risk of victimization.

Theoretical Applications to Online Fraud Victimization and Self-Protective Behaviors

Theoretical frameworks that can be employed to understand self-protective behaviors in the cyber fraud context include routine activities approach and lifestyle exposure theory (Holt & Bossler, 2008; Leukfeldt & Yar, 2016). Crime prevention education can then be developed, employing a situational crime prevention framework.

Routine activities and lifestyle exposure theories provide a theoretical lens through which to understand victimization. They capture determinants and differences in individual risk (lifestyle exposure) and patterns of routine activities that provide opportunities for crime to occur (routine activities) (Cohen and Felson, 1979). A combined approach labelled lifestyle-routine activities theory has been developed and utilized to explore target suitability (Bossler & Holt, 2009; McNeeley, 2015). It has been proposed that target suitability can be conceptualised as a combination of visibility, accessibility, exposure and internet lifestyle of potential victims.

Recent studies have conceptualized visibility within the online context as the extent of information available online about the individual (van Wilsem, 2011). The concept of visibility in the online world relates to the extent of publicly available information (such as date of birth, residential address, contact details) provided on the internet that may enhance an individual's suitability as a target (van Wilsem, 2011). Accessibility in the online environment has been defined as holes and gaps in online users' security measures, for example, those that expose them to malware infection or information theft (Leukfeldt, 2014). Accessibility is impacted by behaviors such as installation of virus protection software, using high privacy settings on Facebook profiles and using a secure home wireless network with a password. These strategies all attempt to protect the data stored on the computer and personal information online. The element of exposure in the online environment is defined as the amount of time an individual spends online in close proximity of motivated offenders (Leukfeldt, 2014). The current study conceptualizes exposure as the amount of time an individual spends on the internet, defining the internet itself as a potentially high risk environment. Internet lifestyle can be seen as a determinant of exposure, as it explores the activities of an individual in high risk environments and situations that increase their exposure to motivated offenders (Leukfeldt, 2014). Low risk online activities include emailing and targeted browsing while high risk online activities would include active participation in online chatrooms, online gaming, and social networking sites (Leukfeldt, 2014). High risk online activities increase an individual's exposure to motivated offenders online.

Using a lifestyle-routine activities approach, we can employ the concepts of visibility, accessibility, exposure and internet lifestyle to define the types of self-protective behaviors that need to be employed by potential victims to reduce their vulnerability as a target, in particular, how potential victims can 'harden' themselves against attacks. Target hardening measures were established in Clarke's (1980) situational crime prevention framework. Situational crime prevention techniques aim to limit the opportunities of motivated offenders to reach their targets (Reyns, 2010). A study by Reyns (2010) explored the application of the 25 situational crime prevention techniques to reduce cyberstalking victimization. Results indicated that by taking a victim focus to cybercrime prevention, particularly target hardening strategies, there was potential to reduce victimization risk.

Of relevance to this study, as discussed previously, cyber fraud offenses fall under two broad categories. As such, target suitability and, in turn, target hardening need to be cognizant of the need for strategies that combat crimes directed at computers or ICTs and crimes where computers or ICTs are an integral part of the offense (Australian Government Attorney-General's Department, 2013).

Potential target hardening measures in the case of attacks against the computer system itself relevant to cyber fraud offenses involve the implementation of physical barriers or *hard* crime prevention measures. These include installation of virus software, firewalls, and password protection. This study conceptualises hard crime prevention measures as those self-protective behaviors that provide physical, digital barriers between the target and the offender.

Potential target hardening measures in relation to cyber fraud offenses that use the computer as an integral part of the offense acknowledge the role of the victim in their own victimization (Wortley, 1998). Target hardening or self-protective strategies in relation to this category of cyber fraud can be conceptualised as behavioral barriers or *soft* crime prevention measures. In the online world, soft crime prevention measures are conceptualised as self-protective behaviors that require ongoing behavioral action by the online user to reduce contact with potential offenders. Online soft crime prevention measures include reducing the information published on online social networking sites, opting into additional privacy settings in online forums and chat rooms, not accepting online social networking requests unless the individual is known to the victim and not replying to emails from an unknown or untrustworthy sender.

The approach taken in this study to separate hard and soft crime prevention knowledge and use of online self-protective strategies is an important contribution of this research. Whilst the differentiation between physical barriers and behavioral barriers have been discussed, few studies have operationalised online crime prevention in this way.

Designing Crime Prevention Education: Police and Victims

As highlighted earlier, traditional law enforcement strategies that focus on apprehending the offender are challenging and have proven largely ineffective when attempting to reduce cyber fraud victimization (Button et al., 2011; Cross, 2016; Webster & Drew, 2017). Often police do not know about cyber fraud crimes, as many victims do not report victimization (Holt & Bossler, 2014; Wall, 2007; Whitty & Buchanan, 2012) due to feelings of shame or embarrassment (Webster & Drew, 2017). New online cybercrime reporting systems, such as ACORN in Australia (see https://www.acorn.gov.au), have seemingly increased reporting rates but this does not overcome the inherent difficulties faced in policing cybercrime. Identifying offenders is difficult, as the internet provides high levels of anonymity with offenders actively masking their identities (Drew & Webster, 2017) and even when police are able to identify the offender, they typically face transnational jurisdictional difficulties with the apprehension of offenders requiring international cooperation (Cross, 2016). Cybercrime investigation is resource intensive and the adequacy of investment of police resources remains largely inadequate (Davis, 2012; Webster & Drew, 2017).

It is evident that, in order to reduce cyber fraud victimization, a victim-centric focus to crime prevention is a viable option. It is perhaps for this reason that recent policing strategies have started to take a preventive approach to reduce cyber fraud victimization (Cross, 2016; Cross & Blackshaw, 2015; Webster & Drew, 2017). Unfortunately, to date there has been very little research into the effectiveness of education campaigns available to the public (Cross & Kelly, 2016; House of Representatives Standing Committee on Communications, 2010). If police start to more heavily invest in their role of proactive victim identification and victim prevention education they need further guidance on how best to design interventions.

To provide police (and also others who may be involved in prevention of cyber fraud victimization) with an evidence base on which to develop crime prevention initiatives and programs, this study firstly addresses the issue of whether potential victims are aware of their actual victimization risk. An individual's knowledge of actual risk is an important factor when identifying why or why not self-protective measures are implemented. If an individual does not know they are at risk they may not implement self-protective measures and are therefore vulnerable to victimization attempts (Buchanan et al., 2007). This relationship needs further exploration for two reasons. First, more generalized studies of crime prevention have often failed to establish a link between perception of risk and use of self-protective behaviors (Radar, May & Goodrum, 2007), and, second, this relationship has not been adequately explored in the cyber fraud context.

Education campaigns must provide the knowledge and skills that are needed to engage in online protective behaviors (Burns & Roberts, 2013; Martin and Rice, 2011). As such, this study examines whether those most at risk of victimization have developed increased knowledge of crime prevention strategies to 'target harden' themselves against cyber fraud attempts. In turn, this study explores whether this knowledge is associated with a proportionate level of use of self-protective behaviors and strategies by those at higher risk of cyber fraud victimization.

Intuitively, it would be expected that those who have an accurate perception of their online victimization risk would develop commensurate levels of knowledge *and* strategies required to protect themselves online. However, this relationship has not to date been empirically tested. This is crucial for the design of crime prevention programs in the cyber context. Does knowledge translation to skills implementation need to be an articulated focus of cyber fraud prevention programs and particularly linked to relative levels of actual victimization risk?

Method

Sample and Procedure

The sampling strategy used in the current study was snowball sampling. The sample group targeted for participation in the current study were online users aged 18 years and over, specifically those who use social networking sites. An online questionnaire was developed and distributed using Qualtrics survey software. Facebook was used as the sampling site. The first wave of surveying, involved sharing the link to the online questionnaire via Facebook profiles of the researchers. As such this was a convenience sample given it involved sending the survey link to all those in the friends list of each of the two researchers conducting this research. The second wave of surveying involved posting a message on Facebook to the friends list of the researchers. This message encouraged those initially contacted by the researchers to share the online survey link with their Facebook friend lists. This expanded the participant recruitment group by reaching out to the friends' lists of the initial group directly contacted by the researchers. A final sample of 218 participants was obtained.

Measures

The online questionnaire was developed by operationalising key theoretical concepts of routine activities approach, lifestyle exposure theory and situational crime prevention. The questionnaire was pilot tested with a police detective working within the State police fraud and cybercrime specialist unit and two academics in the field. The online questionnaire measured a broad range of variables, but for the purpose of this study the variables of actual victimization, perceived victimization, knowledge of hard and soft crime prevention measures, and actual use of hard and soft crime prevention measures will be discussed.

Perception of victimization risk

Participants were asked to report their perceived likelihood of victimization risk in relation to a list of common online crime types identified in the ACCC (2014) scam report using a 5-item Likert scale, with 1 (very unlikely) to 5 (very likely) (α=.837). These crime types included such crimes as phishing and identity theft, advance fee fraud, shopping scams and hacking. The responses to these questions were combined to give an overall sum score of perceived victimization risk. Scores ranged from 8 to 38. Higher scores indicated higher levels of perceived victimization risk.

Actual victimization risk

An actual victimization risk score for participants was created through the combination of sub-scales based around the variables derived from lifestyle exposure theory, including visibility, accessibility, exposure and internet lifestyle. Visibility was conceptualised as individuals who provide extensive amounts of information online about themselves, particularly personal details (α=.763). Participants answered a question indicative of visibility. For example, "What information from the list below is available about you online?" Accessibility was conceptualized as the ease with which information (as measured through visibility) could be obtained online. Participants were asked, referring to information they listed in availability of information about them online, "how easy it would be for someone to gain access to this information about you?" Exposure was measured primarily in respect to the amount of time spent online. Internet lifestyle was measured by examining types of online activities. Riskier activities included online chatrooms/forums, online gaming, social networking sites and online dating sites with less risky activities including emailing, targeted website browsing, banking and work and study activities. With the exception of time spent online (exposure), all questions used a 5-item Likert scale response set, with 1 (very unlikely) to 5 (very likely). For exposure, respondents were asked to report the number of days a week that they access the internet, with responses ranging from every day (7 days a week) to 1-2 days a week. Responses to this question were collapsed into 1-2 days (1), 3-4 days (2), and 5-7 days (3). Mean scores were calculated across the 4 sub-scales to create three groups: low (1 to 1.99), medium (2 to 2.99) and high (3 to 5).

Crime Prevention

The crime prevention knowledge and use questions were developed using an educational guide produced by the Australian government, "Protecting Yourself Online, What Everyone Needs to Know" (Australian Government Attorney-General's Department, 2011). The key self-protective measures that online users should use when participating in online activities were identified (Australian Government Attorney-General's Department, 2011).

Knowledge of crime prevention measures

Participants were asked to answer 15 questions using a 5-item Likert scale, rating their knowledge and competency in relation to online crime prevention strategies from 1 (No competency) to 5 (High competency) (α=.939). Participants were asked in relation to a series of knowledge questions, "How would you rate your knowledge of how to use the following measures to protect yourself online?" An overall sum score was produced by combining participant responses to the 15 questions. A higher score indicated greater levels of knowledge of how to use online crime prevention measures. An overall mean knowledge score was constructed by dividing the overall sum score by the number of questions (15). Further, a sum score were created for the six questions indicative of the sub-scale hard crime prevention measures knowledge by combining the scores for each of the six questions. Scores ranged from 6 to 30. A mean score was created by dividing the sum score by the number of questions (six). A sum score was also created for the nine questions indicative of the sub-scale soft crime prevention measures knowledge by combining the scores for each of the nine questions. Scores ranged from 9 to 45. A mean score was created by dividing the sum score by the number of questions (nine).

Use of crime prevention measures.

Participants were asked to answer 23 questions using a 5-item Likert scale, rating how true the statements were in relation to their use of crime prevention measures online with 1 being never true and 5 being always true (α=.734). Participants were asked, "Please rate how true the following statements are regarding your online behaviour?" Eleven questions were reverse coded as they were asking about negative online behaviors. An overall sum score was then calculated based on participant responses to the 23 questions, with higher scores indicating greater use of self-protective measures. A mean overall use of crime prevention measures sum score was calculated by dividing the overall use sum score by the number of questions (23). Further a sum score was created for the 10 questions indicative of hard crime prevention use. A mean score was then calculated by dividing the sum score by the number of questions (10). A sum score was also created for the 13 questions indicative of soft crime prevention use. A mean score was then calculated by dividing the sum score by the number of questions (13).

Results

The study included 219 participants, with one participant subsequently excluded as they were under 18 years of age. Of the participant group, 54.1% were between 18 and 24 years of age, 23.4% were between 25 and 44 years of age and 22.5% of the sample were aged 45 years or older. The final sample included 77.1% females and 22.9% males, with the majority of the participants having completed post Year 12 qualifications (60.1%). Of the sample, 46.3% indicated that they spent 8 hours or more per week on the internet and 97.7% accessed the internet 5 or more days per week. Access to internet was mostly undertaken using smartphones (94%) and personal laptops (72%). Online activities that were undertaken by respondents, at least once a week, included emailing (95%), social networking (95%) targeted website browsing (91%), banking (88%), work or study (86%), shopping (56%), chatrooms (18%) and online gaming (17%).

Of the sample group, 64.7% indicated that they had previously been a victim of some type of cyber fraud crime. Survey respondents were presented with a list of crime types and their definitions. They were asked to indicate whether they had been a victim or not of each of the crime types listed. The top three cyber fraud crimes identified were advance fee fraud (upfront payment for goods or services that you did not receive, 82.6%); lottery scams (received an unexpected email, phone call, or mail stating you have won a large amount of money, 47.2%) and shopping scams (purchased goods online that were not what they said they were, 22.5%).

Actual victimization and perceived victimization risk

A one-way between-groups analysis of variance was conducted to explore whether there were differences in perceived victimization risk across actual victimization risk groups. Actual victimization risk included three categories (high, moderate, and low). Statistically significant differences across groups were found at the $p<0.05$ level, $F(2, 215) = 3.513$, $p=.032$ (see Table 1).

Table 1. Insert here.

Post hoc comparisons using the Bonferroni test indicated that there were statistically significant differences between those in the low actual victimization risk group (M=1.97, SD=0.68) and those in the high actual victimization risk group (M=2.67, SD=0.74). Those in the high actual victimization risk perceived that they were more likely to be victimised ($p=0.37$).

Actual victimization risk and Knowledge and Use of Crime Prevention Strategies

A one-way between-groups analysis of variance was conducted to explore differences in both knowledge of crime prevention strategies and use of crime prevention strategies across actual victimization risk groups. Actual victimization risk included three categories (high, moderate, and low). For knowledge of crime prevention strategies, no statistically significant differences were found across groups, $F(2, 215) = 0.18$, $p=.838$. For use of crime prevention strategies statistically significant differences were found at the $p<0.001$ level, $F(2, 215) = 10.390$, $p=.000$ (see Table 2).

Table 2. Insert here.

Post hoc comparisons using the Bonferroni test indicated statistically significant differences between all three groups in respect to use of crime prevention strategies. Those in the high actual victimization group (M=3.13, SD=0.54) reported less use of crime prevention strategies than those in both the moderate (M=3.66, SD=0.49, p=0.001) and low (M=3.94, SD=0.41, p=0.000) actual victimization groups. And, those in the moderate actual victimization group reported less use of crime prevention measures than those in the low actual victimization group (p=0.051).

Actual Victimization Risk and Use of Hard and Soft Crime Prevention Strategies

Given the statistically significant finding between groups regarding the use of crime prevention strategies, a one-way between-groups analysis of variance was conducted to examine differences across actual victimization risk groups and use of hard and soft crime prevention strategies. For use of hard crime prevention strategies, differences across groups were not statistically significant, *F*(2, 215) = 2.927, p=.056. For use of soft crime prevention strategies statistically significant differences were found at the p<0.001 level, *F*(2, 215) = 15.955, p=.000 (see Table 3).

Table 3. Insert here.

For use of soft crime prevention strategies, post hoc comparisons using the Bonferroni test indicated statistically significant differences across all three groups. Those in the high actual victimization group (M=3.08, SD=0.53) reported less use of soft crime prevention strategies than those in both the moderate (M=3.74, SD=0.50, p=0.000) and low (M=4.10, SD=0.40, p=0.000) actual victimization groups. And, those in the moderate actual victimization group reported less use of soft crime prevention measures than those in the low actual victimization group (p=0.007).

Discussion

A key purpose of this study was to gain a better understanding of self-protective and crime prevention knowledge and behaviors of potential victims of cyber fraud in light of their victimization risk. This research provides police and others involved in cyber fraud prevention with a better understanding of self-protective and crime prevention behaviors of potential victims of cyber fraud. This study contributes to an evidence base on which more effective, focused and tailored crime prevention programs can be developed and delivered. The findings of this research are relevant to police and other relevant stakeholders (including the broader information and communications technology sector) who embrace the mandate that victim-focused prevention activities is a clear and important priority for combatting cybercrime.

A simplistic question is whether knowledge directly translates into practice. Does knowledge of online self-protective, crime prevention result in the commensurate level of use of crime prevention strategies that target harden the potential victim against cyber fraud attacks? This question is, however, somewhat limiting. It is argued in the current research, we need a more detailed understanding of the interplay between risk, knowledge and use of self-protective strategies. This will allow for improved evidence-based curriculum design of cyber fraud crime prevention education by understanding where the ‘gaps’ are and who would gain most benefit from engaging in crime prevention programs. While cybercrime education should be available for all, resources are scarce, particularly the resources of police in the crime prevention space. It is important for police to design effective educational programs but it is also essential that they are able to determine who is most ‘at risk,’ as they need to be prioritised.

This study found that potential cyber fraud victims have an accurate understanding of their cyber fraud victimization risk. Those in the high risk victimization group perceived they were at greater risk compared to those in the low victimization risk group. This is interesting, given that research on other crime types have often found that individuals do not hold accurate perceptions of risk and tend to overestimate their level of risk relative to actual risk (Ambrey, Fleming & Manning, 2014; Indermaur and Roberts 2005).

This finding is also important, as understanding personal risk to crime may be influential in whether or not the individual perceives a need to increase knowledge and use crime prevention strategies to better protect themselves. If an individual does not know they are at risk they may not seek to gain knowledge or implement self-protective measures leaving them even more vulnerable to victimization attempts (Buchanan et al., 2007). This has not to date been extensively studied within the cybercrime context. This research provides confirmation that victims of cyber fraud are both aware of and are able to identify accurately their relative risk online.

The current study examined whether those most at risk of victimization have developed increased knowledge of crime prevention strategies to 'target harden' themselves against cyber fraud attempts. In turn, this study explored whether actual use of self-protective strategies in the online environment is proportionate with victimization risk. Those at heightened victimization risk did not, despite their awareness of their increased risk, develop greater levels of knowledge about cyber fraud prevention. The mean knowledge score indicated that all groups rated themselves competent or moderately competent in knowledge of cyber fraud prevention strategies. Of perhaps even more concern, was the finding that those most at risk were comparatively, least likely to use online self-protective, crime prevention behaviors. Given that all victimization groups had similar levels of knowledge, it would be expected that those most at risk would have at least similar levels of use to the other groups.

Research conducted in different contexts may shed some light on these findings. Research examining the relationship between financial literacy and fraud victimization is one example. It was found that those who are most knowledgeable are most likely to become fraud victims (NASD, 2006). The researchers interpreted this as the 'knowing-doing' gap (NASD, 2006). This may be related to over-confidence in their knowledge and ability to identify fraudulent offers and/or the development of strong knowledge but not the practical strategies by which to identify or deflect fraud attacks (Drew & Cross, 2013; NASD, 2006; Pfeffer & Sutton, 1999). A study by Gamble, Boyle, Yu and Bennett (2013) found that overconfidence in financial knowledge was a significant predictor of victimization. This issue of differences in technical versus behavioral strategies of crime prevention is discussed later with reference to soft crime knowledge and use. At a general level, this finding indicates that more effort is needed in assisting those at higher risk of victimization. Victims need to be able to identify their risk, understand the strategies that are needed in order to combat how they are being profiled as 'suitable' targets in cyber space and have the technological capabilities to implement prevention measures. These steps may assist potential victims more accurately perceive risk, increase knowledge and in turn, increase use of self-protective behaviors to prevent online victimization.

The aim of this research was to gain a better understanding of knowledge and use of online self-protective strategies of victims, in light of their actual and perceived victimization risk. It was undertaken to inform the development and implementation of crime prevention education. A number of important conclusions regarding crime prevention education by police agencies can be made.

The first relates to the content of cyber fraud crime prevention education. The current study provides evidence to suggest that practical implementation of cyber fraud prevention strategies needs to be an articulated focus of program curriculum. Of particular importance is the difference that was found between hard and soft crime prevention strategy use, with those at highest risk using the least soft crime prevention strategies.

By studying hard and soft knowledge and use separately this study has provided an important contribution to the literature on cyber fraud prevention. These findings indicate that cyber fraud prevention education needs to ensure that the less technical behavioral strategies, those that are perhaps more difficult to navigate, need to be prioritised. Alternatively, in the case of phishing, which requires soft crime prevention knowledge and skill, one needs to undertake a number of active and deliberate decisions in order to deflect an attack. Development of maximally effective cyber fraud prevention education will need to address the complexity of interactions and associated fraud risks when online. This is not to suggest that educational efforts surrounding cyber fraud crimes that target the computer or other ICT's should be abandoned, but it is suggested that an increased focus be placed on crime prevention education that targets prevention of cyber fraud crimes that use the computer as an integral part of the offense.

The results of this study indicate that cyber fraud prevention education provided by police is likely to have a meaningful impact on cybercrime. The findings of this study indicate that those most at risk are also most vulnerable to victimization. This constitutes a multiplier effect in that it is likely to accelerate increases in cyber fraud if not addressed. By prioritising crime prevention education for those most at risk, police agencies will potentially be able to make a real impact relevant to their traditional performance measures, that is, a reduction in crime rates and, also, meet the objectives of crime prevention. Given that traditional law enforcement approaches to combatting crime, primarily the apprehension of offenders, is often ineffective with this crime type, this research suggests that the effectiveness of police can be directly enhanced by their involvement and participation in cybercrime prevention initiatives.

Whilst the findings of the current study have provided important and valuable insights, the limitations of the study are acknowledged. The sample used was a convenience sample that employed snowball sampling strategy. The generalisability of these findings should be tested on a larger and more representative sample. The study focused on cyber fraud crime only, further research should examine whether similar results are found for other types of cybercrime. Importantly, future research exploring the specific reasons or factors why knowledge is not driving the actual use of self-protective strategies in the online environment is needed. This is crucial for the ongoing design of crime prevention programs in the cyber context.

Conclusion

In conclusion, this study has provided an important contribution to our understanding of the relationships between actual and perceived online victimization risk and the knowledge and use of self-protective, crime prevention behaviors of potential victims of cyber fraud. Based on the findings of this research it is argued that a victim-centric policing approach should be seen as a viable and preferred alternative to policing cyber fraud given the nature of these crimes. Police agencies should feel justified in investing in the development and provision of cyber fraud crime prevention education given the positive and impactful outcomes that are likely to be achieved.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Jacqueline Drew is a Senior Lecturer in the School of Criminology and Criminal Justice and a member of the Griffith Criminology Institute, Griffith University. She trained as an organisational psychologist and has worked as a practitioner and researcher across a number of police agencies. Her research interests include cyber fraud and white collar crime (particularly, advance fee fraud and financial fraud and regulation) and leadership and performance management.

Lucy Farrell is a member of the Australian Federal Police working in digital forensic examination. She graduated in 2015 with First Class Honours in Criminology and Criminal Justice from the School of Criminology and Criminal Justice, Griffith University. She holds a double degree in Criminology and Criminal Justice and Forensic Science.

References

Ambrey, C.L., Fleming, C.M. & Manning, M. (2014). Perception or reality, what matters most when it comes to crime in your neighbourhood? *Social Indicators Research, 119,* 877-896.

Australian Consumer and Competition Commission (ACCC). (2016). *Targeting scams: Report of the ACCC on scam activity 2016.* Retrieved from https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2016

Australian Government Attorney-General's Department. (2011). *Protecting Yourself Online, What Everyone Need to Know*. Retrieved from https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/PDF%20-%20Protecting%20Yourself%20Online%20-%20Second%20Edition%20-%20Booklet.pdf

Australian Government Attorney-General's Department. (2013). *National plan to combat cybercrime.* Retrieved from http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management, 29(2),* 408-433.

Burns & Roberts (2013). Applying the theory of planned behavior to predicting online safety behavior. *Crime Prevention and Community Safety, 15(1),* 48-64.

Button, M., Lewis, C. & Tapley, J. (2014). Not a victimless crime: the impact of fraud on individual victims and their families. *Security Journal 27(1)*, 36–54.

Clarke, R. V. (1980). "Situational" crime prevention: theory and practice. *British Journal of Criminology, 20*(2), 136 – 147.

Clough, J. (2015). *Principles of cybercrime* (2nd ed.). Cambridge: Cambridge University Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rates trends: a routine activity approach. *American Sociological Review, 44*(4), 588-608.

Council of Europe. (2004). *Convention on Cybercrime*. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Cross, C. (2016). Using financial intelligence to target online fraud victimization: Applying a tertiary prevention perspective. *Criminal Justice Studies, 29(2),* 124-145.

Cross, C. & Blackshaw, D. (2015). Improving police responses to online fraud. *Policing: A Journal of Policy and Practice, 9(2),* 119-128.

Cross, C. & Kelly, M. (2016). The problem of "white noise": Examining current prevention approaches to online fraud. *Journal of Financial Crime, 23(4),* 806-814.

Cross, C. Smith R. & Richards, K. (2014). Challenges of responding to online fraud victimization in Australia. *Trends and Issues in Crime and Criminal Justice, 474,* 1-6.

Cybercrime Act 2001 (Cth) (Austlli.)

Davidson, J.C. & Martellozzo, E. (2008). Protecting vulnerable young people in cyberspace from sexual abuse: Raising awareness and responding globally. *Police Practice and Research: An International Journal, 9(4),* 277-289.

Davis, J.T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management, 35(2),* 272-284.

Drew, J.M. & Cross, C. (2013). Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes. *Journal of Financial Services Marketing, 18(3),* 188-198.

Gamble, K., Boyle, P., Yu, L. and Bennett, D. (2012) *Aging, financial literacy and fraud.* Social Science Research Network. Retrieved from http://ssrn.com/abstract=2165564

Grabosky, P. N. (2001).Virtual criminality: Old wine in new bottles? *Social and Legal Studies*, *10*(2), 243-249.

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management, 27(3)*, 341-357.

Holt, T. & Bossler, A.M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30,* 1-25.

Hot, T. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior,* 35, 20-40.

House of Representatives Standing Committee on Communications. (2010). Hackers, fraudsters and botnets: Tackling the problem of cybercrime. *The Report of the Inquiry into Cyber Crime.* The Parliament of the Commonwealth of Australia. Retrieved from http://www.aph.gov.au/parliamentary_Business/Committees/House_of_Representatives_Committees?url=coms/cybercrime/report.htm

Indermaur, D., & Roberts, L. (2005). *Perceptions of crime and justice. Australian social attitudes: the first report.* Sydney: University of New South Wales Press.

Ionescu, L. Mirea, V. & Blajan, A. Fraud, corruption and cyber crime in a global digital network. *Economics, Management and Financial Markets, 6(2),* 373-380.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking, 17(8),* 551-555.

Leukfeldt, E.R. & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37(3),* 263-280.

Martin, N. and Rice, J. (2010) Building better Government IT: Understanding community beliefs and attitudes towards smart card technologies. *Behavior and Information Technology 29 (4)*, 433–444.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice, 31*(1), 30-52.

NASD Investor Education Foundation. (2006). *Investor fraud study: Final report.* Retrieved from http://www.sec.gov/news/press/extra/seniors/nasdfraudstudy051206.pdf, accessed 25 January 2013.

Office of National Statistics (2017). *Crime survey for England and Wales*. Retrieved from http://www.crimesurvey.co.uk/

Pfeffer, J., & Sutton, R. (1999). Knowing "what" to do is not enough: turning knowledge into action. *California Management Review, 42(1),* 83-108.

Radar, N.E., May, D.C. & Goodrum, S. (2007). An empirical assessment of the "threat of victimization": Considering fear of crime, perceived risk, avoidance, and defensive behaviors. *Sociological Spectrum, 27(5),* 475-505.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety, 12*(2), 99-118.

United Nations. (2016). *The state of broadband: Broadband catalyzing sustainable development.* Broadband Commission for Sustainable Development. Retrieved from http://www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf

US Internet Crime Complaint Center. (2016). *Internet crime report.* Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115-127.

Wall, D.S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research: An International Journal, 8(2),* 183-205.

Webster, J. & Drew, J.M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science and Management, 19(1),* 39-53.

Whitty, M. & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior and Social Networking, 15(3),* 181–183.

Wortley, R. (1998). A two-stage model of situational crime prevention. *Studies on Crime and Crime Prevention, 7,* 173-188.

Table 1. Summary of One-Way Analysis of Variance of Actual Victimization Risk and Perceived Risk of Victimization (N=218).

Source	*df*	*SS*	*MS*	*F*	*p*
Between Groups	2	4.031	2.016	3.513	.032*
Within Groups	215	123.341	.574		
Total	217	127.372			

*Significant p<0.05

Table 2. Summary of One-Way Analysis of Variance of Actual Victimization Risk and Knowledge and Use of Crime Prevention Strategies (N=218).

Source	*df*	*SS*	*MS*	*F*	*p*
Knowledge					
Between Groups	2	0.254	0.127	0.176	.838
Within Groups	215	154.632	.719		
Total	217	154.886			
Use					
Between Groups	2	4.926	2.463	10.390	.000*
Within Groups	215	50.970	.237		
Total	217	55.897			

*Significant p<0.001

Table 3. Summary of One-Way Analysis of Variance of Actual Victimization Risk and Use of Hard and Soft Crime Prevention Strategies (N=218).

Source	*df*	*SS*	*MS*	*F*	*p*
Hard Use					
Between Groups	2	2.206	1.103	2.927	.056
Within Groups	215	81.008	.377		
Total	217	83.213			
Soft Use					
Between Groups	2	7.767	3.883	15.955	.000*
Within Groups	215	52.330			
Total	217	60.096			

*Significant p<0.001