Individual information security, user behaviour and cyber victimisation:

An empirical study of social networking users

George Saridakis[a], Vladlena Benson[a], Jean-Noel Ezingeard[b], Hemamali Tennakoon[a]

a. Kingston Business School, Kingston University, London, UK,
email:{v.benson, h.tennakoon, g.saridakis}@kingston.ac.uk

b. Manchester Metropolitan University, Manchester, UK,
email:jn.ezingeard@mmu.ac.uk

Abstract

While extant literature on privacy in social networks is plentiful, issues pertaining to information security remain largely unexplored. This paper empirically examines the relationship between online victimisation and users' activity and perceptions of personal information security on social networking services (SNS). Based on a survey of active users, we explore how behavioural patterns on social networks, personal characteristics and technical efficacy of users impact the risk of facing online victimisation. Our results suggest that users with high-risk propensity are more likely to become victims of cybercrime, whereas those with high perceptions of their ability to control information shared on SNS are less likely to become victims. The study shows that there is a negative and statistically significant association between multipurpose dominant SNS (e.g. Facebook, Google+) usage and victimisation. However, activity on the SNS for knowledge exchange (e.g. LinkedIn, Blogger) has a positive and statistically significant association with online victimisation. Our results have implications for practice as they inform the social media industry that protection of individual information security on SNS cannot be left entirely to the user. The importance of user awareness in the context of social technologies plays an important role in preventing victimisation, and social networking services should provide adequate controls to protect personal information.

Keywords: Social media, cyber threats, personal information privacy, information security, cybercrime victimisation, social networking services.

Introduction

Recent trends in information and communication technologies have taken the rates of personal information sharing, storage and processing to an unprecedented level (Conger et al., 2012). This is largely due to the popularity of social networking services (SNS). Social networks enable data accumulation on a previously unimaginable scale, yielding both benefits and undesirable consequences for their users. Amongst such inadvertent outcomes of social networking use are breaches of personal information security, which have become repeatedly reported in the press. Personal and security sensitive information losses resulting from cybercrime, including online identity theft or usurpation (Al-Daraiseh et al., 2014; Reyns, & Henson, 2015), financial fraud, stalking and blackmail, are on the rise (Gradon, 2013; Guitton, 2013).

However, much of the extant literature dealing with security and privacy is based on studies conducted in corporate environments. These studies emphasise potential economic losses to organisations as a result of online information disclosure (Campbell et al., 2003; Cavusoglu et al., 2004; Rauch, 2001), further adding to the paucity of coverage of negative aspects of technology at the individual level. Legacy interpretations of personal information privacy (e.g. Smith et al., 1996) have treated safeguarding personal information as an individual responsibly of users. Although many social networkers consider themselves technologically savvy and confidently transact online, it has come to light that personal information privacy is not directly linked to the skill level nor to the experience of users (Dinev & Hart, 2004; Mesch, 2009). It is now widely accepted that information privacy is no longer achievable at the individual level. As such, we follow on the research agenda set by Conger et al. (2012) in which they call for further studies into the online behaviour of users, and voice the need for raising public awareness to avoid technology-enabled privacy losses.

Even though SNS facilitate information dissemination and social interactions (Sherchan et al., 2013), there is a side to social networking that most users are unaware of. Sodhi & Sharma (2012) found that information posted on social media sites was used by cyberstalkers to identify potential victims, while a content analysis of Facebook profiles by Shelton & Skalski (2013) found that there is an overrepresentation of negative content. Furthermore, in the context of information systems research, some perceive SNS as a potentially addictive technology (Turel & Serenko, 2012), and therefore a negative phenomenon. Social networkers, especially youth, are vulnerable to cyber harassment, including unwanted sexual solicitation via chat rooms, instant messaging and blogs

(Mitchellet al., 2010; Ybarra & Mitchell, 2008; Wolaket al., 2006; Subrahmanyam & Greenfield, 2004). Online harassment extends to cyberbullying[1] and research indicates that the frequency of Internet usage is related to cyber bullying, i.e. higher usage of the Internet leads to higher risk of cyber bullying victimisation (Mesch, 2009). Recent studies have investigated the scale of information disclosure on social media, which is undesirable or inadvertent in many cases (e.g. Chen & Sharma, 2013), leading to personal information security breaches.

On social networks, cybercrime victimisation[2] is viewed differently, while the attributes of crime –e.g. victims, offenders and safeguards – remain the same as in traditional crime. The Routine Activity Theory (RAT), established by Cohen & Felson (1979), has been successfully applied to explain the macroview of online crime, i.e. how the offender and the victim are brought together in the absence of appropriate safeguards (Mesch, 2009). Based on this theory, criminologists argue that continuous compulsive usage of SNS increases users' risk of exposure to motivated offenders (i.e. cybercriminals). In line with the RAT, repetitive use of SNS increases opportunities for offenders and victims to converge in cyberspace (Reyns, 2013; Reyns et al., 2011). Extant literature shows that while significant research attention has been devoted to exploring positive outcomes of social networking usage, literature on the negative aspects of social technology is relatively lean. This study bridges this gap in literature and establishes the link between information security, the SNS usage and its effects on online victimisation.

In this study we have investigated four important areas. Firstly, we examine whether high usage of social media increases the risk of online victimisation. Based on the premise of RAT, it becomes easier for criminals to find potential victims on social networks. Furthermore, users who are more active on SNS create more opportunities for offenders to locate them as victims (Reyns et al., 2011). As such, the frequency of SNS usage should increase the risk of cybercrime victimisation. Secondly, we look at 'guardianship' –another component of RAT (Reyns et al., 2011) –which, in the case of social networks, represents information security measures. We study the guardianship of information in terms of perceived control individuals have over their personal information. We are interested to find out whether users with a higher perception of control over the security and privacy of their

[1]Cyberbullying is defined as the use of e-mails, instant messaging and Websites to inflict repeated harm wilfully on a person (see Patchin & Hinduja, 2006).

[2]Definitions of crime victimisation refer to being the subject of a criminal deed leading to personal harm, loss or injury (Cronje & Zietsman, 2009). The difference in the definition of cybercrime victimisation from the definition of general victimisation is contextual. Thus, cybercrime victimisation means 'personal harm, loss or injury due to actions of cyber-criminals or online perpetrators' (Bougaardt & Kyobe, 2011:63).

information on social networking sites are less likely to be victimised online. Thirdly, we examine the relationship between technological competency of individuals and online victimisation. Past research suggests that the technical efficacy of users is positively related to trust in technology (Connolly & Bannister, 2006), but the applicability of this conclusion with regards to social networking remains unclear.

Finally, in information systems and security research, the treatments of risk and risk analysis have been established among the pillars of security literature (Dhillon & Backhouse, 2001). In this study, we focus on the concepts of risk perception and risk propensity. While risk perception is a psychological status, risk propensity is an action state that determines the amount of risk an individual is willing to take. Cases (2002) argues that risk propensity depends on sources of risk and identifies the Internet as a source of cyber risk. Social networking sites such as Facebook, Twitter and LinkedIn fall into the category of online sources of risk due to their Internet-based nature. We verify the above propositions using data collected in a survey of 514 social media users and offer a categorisation of SNS based on the content sharing purpose guided by the principal component factor model to account for structure. The article is organised as follows. After discussing the different categories of social networks, we review extant literature on the subject of online information security and privacy, setting forward the research hypotheses. The following section discusses the research design and methodology. These are followed by the data analysis and a presentation of our findings. The last section discusses the results of the study, and their implications for theory and practice.

Categories of Social Networking Services

While the usage patterns of social networks attracted research attention, the frequency of logins, time spent on and other engagement metrics (Hoffman & Fodor, 2010) collectively do not provide an accurate account of social activity online. The duration of leisure use of social networks is likely to exceed the one for business or professional uses. It is also possible to surmise that users on professional SNS are more vigilant about their personal information than on leisure networks of trusted friends and family members. Therefore it is necessary to distinguish between the purpose and the nature of uses of social networks and apply this categorisation in the context of online victimisation (Stuzman et al., 2013).

Individuals use social networks to communicate and keep in contact with family and friends, while other networks have a specific business and professional orientation. With the fast changing landscape of social technologies, challenges have emerged in the academic

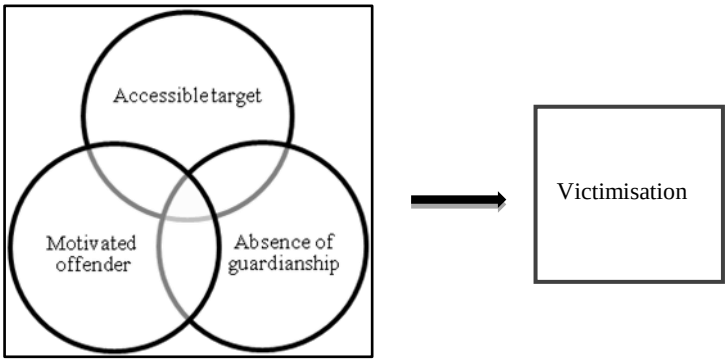
attempts to categorise social networks. Previous research by Junco (2012) confirms that popular SNS such as Facebook are often used for reasons other than to socialise. As many principal networks have blurred the lines of personal versus professional use, the typology of social networks has had to be reassessed. This paper offers a categorisation of social media based on classifications used by Hoffman & Fodor (2010), Kaplan & Haenlein (2010) and Xiang and Gretzel (2010), and also uses a principal component factor model to detect structure. Hence, *multipurpose dominant social networking services* include Facebook, Skype, Google+ and YouTube, which all have a common feature: they allow users to share and access content as well as interact on a personal basis. They are the most dominant platforms in the marketplace. The second category includes social media mainly used for narrow purposes (*narrow purpose social networking services*), specifically World of Warcraft, Second Life and MySpace. These sites focus on users interacting virtually around narrow interests (for example, music interests or gaming). Only a small set of these SNS' functionality is used, hence the term 'narrow purpose'. With regards to the personal purposes of this SNS type, it was found that virtual social worlds, such as Second Life, have a high social presence and a high self-disclosure rate, while virtual game worlds such as World of Warcraft have a high social presence and low self-disclosure (Kaplan & Haenlein, 2010). These 'niche' networks have fewer users than the multipurpose dominant SNS. Finally, *knowledge-exchange purpose social networking services*, including Twitter, LinkedIn, Blogger and Flickr, allow users to share ideas and content.

Online Victimisation and Traditional Crime Theories

Researchers argue that the use of social networking sites is associated with many forms of online victimisation (Ybarra & Mitchell, 2008). Cohen & Felson (1979) developed the routine activity theory (RAT), which has been successfully applied to explain different types of victimisation, including online victimisation (Reyns et al., 2011; Marcum, 2008). The theory suggests that for a crime to take place, certain conditions should be fulfilled (see Figure 1). These conditions include convergence of a victim and a motivated offender; a criminal not only capable, but also willing to commit a crime; in the absence of guardianship to prevent the crime (Cohen & Felson, 1979; Pedneault & Beauregard, 2013). Based on the Routine Activity Theory (RAT), scholars argue that exposure to victimisation depends on an individual's lifestyle and routine daily activities (Mesch, 2009). For online crimes, RAT takes on a new meaning when one considers victimisation in terms of creating an 'opportunity' for offenders to find their online victims, and the enablement of 'guardianship'. Victimisation in

cyberspace takes a broad range of forms, including online consumer fraud (Pratt et al., 2010; Van Wilsem, 2013), cyber stalking, harassment (Nhan et al., 2009; Pedneault & Beauregard, 2013; Pittaro, 2007), among others. For these types of victimisation, an offender and a multitude of targets are brought together in cyberspace, where the opportunity for online victimisation is deemed greater than in the physical world (Reyns et al., 2011).

Figure 1. Elements of the Routine Activity Theory (Cohen & Felson, 1979)



As for guardianship, the questions of who should safeguard and what they should protect are a subject of an ongoing debate. While some argue that online guardianship should be measured in terms of the availability of firewalls and security software (Choi, 2008; Holt & Bossler, 2009), others suggest that guardianship should be exercised by individuals in terms of the control over their online information (Reyns et al., 2011). According to Dhillon & Backhouse (2001), 'security can be achieved by analysing the behaviour of all elements in the system' (p.138). Security controls in the context of social networking have received mixed views. Current media coverage provides a rich account of constant personal data leaks by SNS providers, and unsuccessful attempts by individuals to find who is responsible for ensuring personal information security on SNS. While users view SNS as the responsible agent in ensuring security, SNS imply that the security breaches are caused by individual user behaviour (see Stuzman et al., 2013).

Relevant theories which help explain online behaviour, e.g. the theory of reasoned action (TRA) and theory of planned behaviour (TPB), have been used as a method for examining individuals' decisions when performing specific behaviours (Burak et al., 2013,), and these have informed the theoretical framework of this study. Specifically, TRA and TPB (Fishbein & Ajzen, 1975; Ajzen & Fishbein, 1980; Ajzen, 1985, 1988)posit that beliefs about outcomes of behaviours, beliefs about resources and perceived beliefs of referent individuals are antecedents of attitudes and intentions of behaviour (Burak et al., 2013). TRA and TPB

have been successfully applied in e-commerce to explain consumers' online behaviour (Pavlou & Chai, 2002). TRA addresses individual motivational factors and their link to specific behaviour, and shows the relationship between attitudes, intentions and behaviours (Montano & Kasprzyk, 2008). Its extension – TPB – includes perceptions of behavioural control as an additional predictor of intentions and behaviour (Madden et al., 1992). Users' behaviour towards protective information technology has been explained through the extension of TPB in Dinev et al.(2009). Their model described the formation of behaviour intentions in response to cyber-attacks and other negative technologies. Dinev et al. (2009) show how technology awareness takes a central stage in determining users' behavioural intentions and attitudes. In our study, we were interested in exploring the behaviour of individual users on social networking sites. Through the lens of TRA and TRB, we hypothesise that users' perception of security, control over information and risk can influence their attitudes, intentions and behaviours on social networking sites.

Hypotheses Development

A continuous increase of social activity online and higher usage of ICT have served as antecedents of cybercrime victimisation through simplifying the options of reaching and exposing intended targets (Festl & Quandt, 2013). There is a growing body of research on cybercrime victimisation; however, there is a definite lack of validated measures which specifically examine victimisation in relation to SNS (Landoll et al., 2013). Some have associated victimisation with higher usage of social media through the application of RAT. For instance, Reyns et al. (2011) argue that higher usage leads to more exposure to offenders, and therefore leads to higher likelihood of online victimisation. Usage of SNS has been measured in terms of the number of SNS profiles per individual, and the purpose and frequency of usage (Tynes & Mitchell, 2013).We have adopted a similar approach in this research by incorporating two methods of measuring SNS usage (and thus exposure to victimisation): 1) SNS accounts owned by respondents; and 2) amount of time spent on SNS.

We therefore propose to test the following hypothesis:

H1: *High social media usage has a direct positive impact on the risk of user online victimisation (i.e. user becoming a victim of cybercrime).*

Foxman & Kilcoyne (1993) found that individuals habitually assess the value of their personal information and the amount of control they have over it. This assessment over the control of information is termed 'perceived ability to control submitted information' (Dinev & Hart, 2004, p.419). Moor (1997) and Tavani (2000) suggest that privacy is best understood by the control or restrictions one has over information about oneself. Many websites, including e-commerce, offer users some control over information by giving them an option to opt out (Chadwick, 2001), thereby controlling the actions of the online vendor (Malhotra et al., 2004; Sheehan & Hoy, 2000). Control over information also relates to the principle of guardianship in the RAT. For SNS, control over information has been measured in terms of how users control privacy settings to limit third-party access to their SNS accounts, and how they use profile tracker programmes to see who views their profiles (Reyns et al., 2011). If users perceive they have a reasonable level of control over their information on SNS, and they use SNS security options, then their SNS information is better safeguarded from cybercriminals and there will be fewer opportunities for victimisation. Based on this argument, we derive our second hypothesis:

H2: *High perception of control over information maintained by social media has a negative impact on the risk of user victimisation.*

Significant research attention has been paid to preventative measures against cybercrime. Control over personal information has been identified as one such measure, but researchers were interested in how user characteristics (e.g. technical efficacy) influence online behaviour (e.g. Burns & Roberts, 2013). Some argue that the technical efficacy of SNS users may be one reason why users take a defensive stance against cybercrime. According to Hsia et al. (2014:53), the origins of computer self-efficacy go back to the research on locus of control (Rotter, 1966; Bandura, 1997; Zimmerman, 2000) and it is strongly associated with 'perceived control'. Anderson and Agarwal (2010) argue that technical efficacy is an individual's understanding of their personal competencies required to ensure security. George (2002) refers to it as the 'computer skills' necessary to operate a computer system and software packages; while Lee and Turban (2001) define efficacy as 'an operator's understanding of the underlying characteristics and processes that govern the system's behaviour' (p.4). We are interested in testing whether the possession of better IT skills

measured using self-reported scores[3] – or higher technical efficacy – affects victimisation rates. Hence, we propose the following hypothesis:

H3: *Possession of better ICT skills has a direct negative effect on the risk of user victimisation.*

Many theorists (e.g. Crowe & Horn, 1967; Joffe, 2003; Kaplan & Garrick, 1981; Kasperson et al., 1988; March & Shapira, 1987; Renn,1998; Renn & Rohrmann, 2000; Trimpop,1994) associate risk with 'outcomes' or 'consequences' of 'cost and benefits', 'gains and losses', 'damages' and 'physical, social or financial harm'. In this research, 'risk' of cybercrime victimisation refers to the likelihood of an individual experiencing physical, social or financial harm as a result of cyber threat. Such risks could range from financial loss due to theft of personal information via SNS to physical or psychological damage caused by social cyberstalking or bullying (Cases, 2002; Dowling & Staelin, 1994; Hutchings, 2013). When people are faced with the risk of loss, they tend to assess how serious the threat actually is, which is referred to as 'risk perception' (Joffe, 2003). Crime literature suggests that 'when people believe that they will become a future victim of a nominated offence, they can in fact transpire to become so' (Chadee et al., 2007, p.2). If so, does this imply that the low risk perception of SNS users impacts their vulnerability cybercrimes, i.e. victimisation? We propose to test the following hypothesis to answer this question:

H4: *Low risk perception has a direct positive effect on the risk of user victimisation.*

Information security is often said to be contingent on education, training and awareness programmes (Whitman, 2003), which should increase risk awareness. This is because risk assessment, and therefore risk management, is intertwined with social amplification and relationships (Kasperson et al., 2003). Risk propensity is referred to as the willingness to assume risk (Luhmann, 1988; Mayer et al., 1995; Rousseau et al., 1998; Sheppard & Sherman, 1998) or an individuals' current tendency to take or avoid risks (Sitkin & Pablo, 1995, p.4). In decision-making, this is seen as the action stage that follows the decision to take or avoid risk (Trimpop, 1994). According to the theories of reasoned action

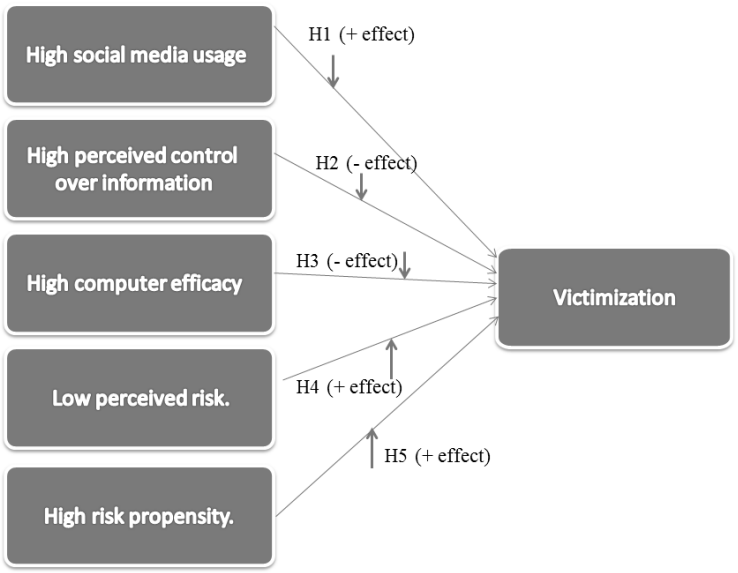
[3] We acknowledge, however, that an objective measure of computer skills may be a better alternative to self-reported measure as applied here. For example, one can argue that some respondents may under-estimate their skills level and some others may be overly confident. However, this study relies on self-reported data of computer skills.

and planned behaviour, this is the result of attitudes and perceptions influencing individual actions or behaviour (Liu et al., 2005). In SNS, individuals engage in risk-taking behaviour, such as communicating online with strangers and sharing personal information, which could increase the likelihood of their victimisation (Whittle et al., 2012). Hence:

H5: *High risk propensity has a direct positive effect on the risk of user victimisation.*

Figure 2 represents the proposed research model, and contains the theoretical constructs representing user behaviour on social media, perceptions of information security attributes and victimisation, along with the hypothesised causal associations between the constructs. Validated measures for behaviour online and information security constructs have been applied, along with the new constructs specific to social media.

Figure 2. Social media behaviour and risk of cybercrime victimisation
(Hypotheses and expected associations)



Data and Empirical Methodology

Sampling and Design

The research population consists of online social media users. Since there are no existing sampling frames to sample this population, purposeful (non-probability) sampling or volunteer panels of Internet users are employed to collect data for this study. In reference to the sample size, Krejcie & Morgan (1970) and Isaac & Michael (1981) recommend a sample

of approximately 400 respondents for a population of 100,000 plus. Duffy (2002) argues that if Internet samples are unrestricted, anyone who comes across the survey could complete it (also known as 'self-selection'), and such a sample may not be representative. However, research findings indicate that participants from self-selected samples provide clearer, more complete responses than participants who are not self-selected volunteers (Gosling & Vazire, 2004).This view is further confirmed by others (e.g. Pettit, 2002; Walsh et al., 1992). In fact, it is believed that self-selection in Web surveys is favoured over interception (e.g. randomly selecting visitors to a website by displaying a message) or using college subject pools (Marsden & Wright, 2010).

To overcome the issue of under-representation, a Web-based questionnaire was developed using Qualtrics software, and then administered to the target sample through Web postings (e.g. on popular SNS like Facebook, LinkedIn, Twitter, etc.) and through personal contacts. This increased the representativeness of the sample (Bhutta, 2012). The survey was only accessible to either members of a particular group (e.g. LinkedIn specialised groups, such as specialist cybercrime forensics groups, academics having profiles on Method Space) or posted on personal websites that can only be accessed by contacts of the site owner (e.g. the researcher's Facebook, LinkedIn and Twitter pages; The Web Experiment List). In the survey invitation, a criterion was imposed to eliminate any non-social media users who might come across the survey's bypassing restrictions. The criteria specify that only those using social media sites are eligible to take part in the survey. Further filtering is conducted by analysing responses to questions in the first section of the questionnaire (e.g. what are the SNS the respondents are currently using, and how often do they use them). Over 700 individuals responded to the survey, but after the data purification procedure the number of usable respondents was 514.

Measures

The survey asked respondents whether they have been a victim of cybercrime, providing them with a number of options to describe the nature of victimisation. The options included 'I have never been a victim of cyber-crime'; 'Spam'; 'Fraud (e.g. bank fraud, identity theft)'; 'Offensive content'; 'Harassment (e.g. cyber-stalking, cyber-bullying)'; and any other type of victimisation not mentioned above. Hence, we can construct the dependent binary indicator variable ($vsns_i$), which takes the value of one if the individual has been victim of cybercrime

(66.53%)[4], and the value of zero if the individual has not experienced any form of victimisation (33.47%).[5]

Social media usage is measured by frequency analysis, whereby respondents indicated their usage (or non-usage) of SNS (Twitter, LinkedIn, MySpace, Google+, YouTube, Blogger, Skype, Flickr, SecondLife, World of Warcraft and Facebook), and how often each SNS is used (Scale: 'Never';'Registered but do not use';'Open all the time';'Several times a day';'Once or twice per day';'Every 2–3 days';'Once a week'; and 'Less than once a week'). We recode the variable to range from one to eight, where one means *no use* and eight means *open all time*. The fast-paced nature of social media technologies explains the challenges in academic attempts to categorise social networks; however, this paper uses a principal component factor model.[6] The first factor loads most highly on *multipurpose dominant social networking services* like Facebook, Skype, Google+ and YouTube ($msns_i$). A common feature of these sites is that they allow users to share and access content as well as interact on a personal basis. They are dominant platforms in the marketplace. The second factor includes social media mainly used for narrow purposes (*narrow purpose social networking services*), specifically World of Warcraft, Second Life and MySpace ($nsns_i$). The common feature of these sites is that they focus on users interacting virtually around narrow interests (for

[4] Since most of users in our sample report being a victim of spam (55.38%) – and only a small proportion of individuals report being a victim of fraud, offensive content harassment or other type - we use a broader category of known online victimisation. Existing research has also shown that definitions of types of crimes can be at odds with what users really experience emotionally (Dredge et al., 2014) and therefore an aggregate measure of victimisation is likely to capture a wider cross-section of concerns of being a victim of cybercrime. Also, it can deal with the measurement error issue within the process of aggregation and reflect more accurately underlying victimization trends. Overall the data shows that most of the active users of Youtube, Facebook, Skype and Linkedin have been victims of the cyber crimes considered in this study (with an average around 77%).

[5] Data limitations, however, do not allow us to measure victimisation in terms of repetition and severity. Also, some users may not know that they have been victims of cyber crime, especially for crimes such as fraud. However, by generating an overall measure of victimisation this problem may be limited since an individual who has been a victim of fraud also reported being a victim of other types of cybercrime (for example nearly 60% of those reported being a victim of fraud have also reported being a victim of spam). Hence, it is likely that those who are not aware of being a victim of fraud are aware and reported being a victim of a different type of cybercrime (e.g. spam) and thus is included in the victimization variable.

[6] Our classification of social media was derived by combining the classification used by Hoffman & Fodor (2010), Kaplan & Haenlein (2010) and Xiang & Gretzel (2010). The first finding can be supported to some extent by previous research by Junco (2012), who found that SNS such as Facebook is often used for reasons other than to socialise. This confirms the fact that SNS similar to Facebook can be safely categorised as 'dual purpose', but we cannot support the argument that dual purpose SNS are more significant than any of the other forms. With regards to SNS used for personal purposes, it was found that virtual social worlds such as Second Life have high social presence and a high self-disclosure rate, while virtual game worlds such as World of Warcraft have high social presence and low self-disclosure (Kaplan & Haenlein, 2010). This would indicate that the second category (SNS for personal use) may include further subcategories and, depending on the nature of personal usage, may rank differently compared to other SNS. SNS used for sharing are seen as a means of interaction, and whether users wish to interact or not may depend on the functional objective of the social media platform (for instance, the objects of sociality on Flickr are pictures; Kietzmann et al., 2011, p.245). This may account for the low factor loading for this category of SNS.

example, music in the case of MySpace). These networks are much more 'niche', with far fewer users than the multipurpose dominant social networking sites. The final factor describes *knowledge-exchange purpose social networking services*, including Twitter, LinkedIn, Blogger and Flickr ($ksns_i$). The common feature of these sites is that they allow users to share ideas and content.

The variable *perceived control over personal information* is measured with four items, capturing ability to control access, and information released, used and provided (cpi_i). The responses varied from strongly disagree (1) to strongly agree (7) (mean = 3.318; Cronbach's alpha = 0.893).[7] The variable *technical-efficacy* (te_i) is measured with four items, which asked respondents if they feel confident working with a personal computer, understanding terms and troubleshooting problems (mean = 5.930; Cronbach's alpha = 0.917) through a seven-point scale (1 = strongly disagree, 7 = strongly agree).[8] The variable *risk-perception* ($rper_i$) is measured using four seven-point scale questions (1 = strongly disagree;7 = strongly agree) that assessed how risky it is to is to provide information to SNS, as well as associated losses and problems (mean = 4.792; Cronbach's alpha = 0.912). Finally, *risk propensity* ($rpro_i$) is measured using a seven-point scale (1 = strongly disagree; 7 = strongly agree), and is measured with five items asking respondents about their willingness to take and accept risks (mean = 2.827; Cronbach's alpha = 0.793). A full list of scales is given in the Appendix. Although not discussed here, we also account for the effects of the various individual variables such as age, gender, occupational status and qualification. For instance, results from a 2012 survey suggest that Facebook is more appealing to adult women aged 18–29, while Pinterest (a recent addition to SNS landscape and not considered in the present study) is popular among adult women, under 50 years of age, with some college education (Duggan & Brenner, 2012).

Statistical Model

Given the nature of our data, we use a probit model to examine the probability of a discrete event (see Greene, 2000) such as being a victim of cybercrime. The explanatory variables can either be dichotomous, ordinal or continuous. We define a latent variable, *vsns**, that represents the propensity of an individual to be a victim of cybercrime. This drives the

[7] Since our study is cross-sectional, changes in perceptions over time cannot be observed. For example, perceptions may change if an individual experience victimisation. However, this issue goes beyond the scope of this paper.

[8] To check for common method bias between 'concept of control' and 'technical efficacy' variable, we implement the Harman's single factor test. A single factor, however, accounts only for 41% of the variance in the model suggesting that common method bias is not a concern here (see Podsakoff et al., 2003).

observed binary indicator of whether an individual has experienced victimisation, *vsns*, through the following measurement equation:

$$vsns_i^* = bX_i + u_i \quad (1)$$

$$vsns_i = \begin{cases} 1 & \text{if } vsns_i^* > 0 \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

where X_i is a row vector of explanatory variables ($msns_i$, $nsns_i$, $ksns_i$, cpi_i, te_i, $rper_i$, $rpro_i$) and *b* is the vector of corresponding coefficients estimated my maximum likelihood methods. We use the variance inflation factor (*ivf*) approach to test for multicollinearity (i.e. there is a perfect linear relationship among the predictors, see Wooldridge, 2000, pp. 95-97). The *vif* values are low - with an average value of 1.08 - suggesting that multicollinearity is not an issue in our estimation approach. The estimation of equation (1) as a probit model provides us with direct measures of the impact of the explanatory variables used in this study on the likelihood of being a victim of cybercrime.[9] Finally, we report marginal effects (for an average individual) to show the change in probability when the independent variable increases by one unit (see Bartus, 2005).

Empirical Findings

The results are presented in Table 1. Model 1 includes the three categories of social media usage as explanatory variables. Model 2 adds the other key explanatory variables. Model 3 presents a reduced form of the model where the *narrow purpose social networking services* variable is excluded from the specification. Finally, Model 4 examines whether the associations are robust when accounting for various individual characteristics. **Hypothesis 1** suggests that high social media usage has a direct positive impact on the risk of user

[9] We also carried out a path analysis. In this model, we assume that risk propensity, perceived risk, technical efficacy and perceived control affect SNS usage, and SNS usage along with the other variables affect whether or not the user experience victimization. In this model, the coefficients of the multipurpose and knowledge-exchange purpose SNS usage are found to be -0.045 ($p<0.05$) and 0.077 ($p<0.01$), respectively. The coefficient of narrow purpose SNS usage is found to be statistically insignificant providing further support to the findings reported in Table 1. Similar to probit estimates, perceived control is found to be statistically significant with estimated coefficient of -0.041 ($p<0.01$). Finally, when the model excludes narrow purpose SNS usage, we also find positive and significant effect of the risk propensity variable (coeff.=0.024, $p<0.1$). Hence, the results are consistent with the one reported by using a probit specification.

victimisation. In fact, intensive usage of the Internet has been viewed as an expansion of the possibilities of perpetration and victimisation, as it simplifies the options of reaching and exposing the intended targets (Festl & Quandt, 2013). Similarly, Reyns et al. (2011) suggest that higher usage leads to more exposure to offenders, and therefore increases the risk of becoming a victim of cybercrime. Usage of SNS has been expressed as the number of SNS profiles per individual, plus the purpose and frequency of usage (Tynes & Mitchell, 2013). Model 1, however, shows that there is a negative and statistically significant association between multipurpose dominant social media usage ($msns_i$) and victimisation (M.E.=-0.057, $p < 0.01$), but a positive and statistically significant association between knowledge-exchange purpose social media usage ($ksns_i$) and being a victim of cybercrime (M.E.=0.091,$p< 0.01$). Additionally, we find no association between narrow purpose social media usage ($nsns_i$) and victimisation. The results remain robust across different specifications (Models 2–4).[10] Furthermore, when we aggregate the social media usage categories to create an index of overall social media usage, we find that the coefficient of this variable is statistically insignificant. Perhaps the two opposite effects of the dual purpose and the sharing purpose of social media usage cancel each other out. Thus, hypothesis 1 is partially supported.

Although the difference between groups of social media is perplexing at first, it is possible to explain it on three levels. Firstly, multipurpose dominant social media sites have significantly revamped their security protocols in the past few years. Most have introduced some form of two-step identification, unusual device or location verification. However, the data used in this study do not allow us to determine the exact time of victimisation which may not overlap with the above changes in security. Secondly, because of their dominance in the marketplace, these sites have also been subjected to much more media interest, which would have raised risk awareness. Increased awareness means that even if the sites in questions now make it easier for users to divulge personal information by default, the trends show that users are in fact disclosing less and less on a broadcast basis (Stutzman et al., 2013). Thirdly, in the case of knowledge exchange sites, successful networking often relies

[10] Dividing SNS into three groups, we find that there are a substantial number of respondents (nearly 45%) in the "knowledge-exchange purpose social networking services" that do not use this SNS platform. For the "multipurpose dominant social networking services" and "narrow purpose social networking services" only 6% and 3% reported no use of these SNS platforms, respectively. Hence, we focus on the former category and test whether there is a significant difference between the treated (i.e. users) and control (i.e. non-users) groups. We construct a dichotomous variable, which takes the value of 1 if the responder has used this SNS platform and 0 otherwise. We then follow a propensity score matching estimator proposed by Becker and Ichino (2002) and estimate the average treatment effect of the treated using the stratification method. The results suggest that the average change in the probability of being a victim is 0.112 for individuals who use the "knowledge-exchange purpose social networking services". The results are robust even when different matching methods are used. This finding is in line with the results presented in Table 1.

on the disclosure of significant amounts of personal information, whether in the form of blogs (Blogger), career information (LinkedIn) or personal pictures (Flickr). RAT suggests that the risk of victimisation grows as a result of the 'opportunity' offered to criminals being exacerbated by the fact that knowledge-exchange requires a wide broadcast of information for SNS to be successful. The fact that narrow purpose social media use does not increase the risks of victimisation would again support this hypothesis. Such sites do not require their users to broadcast so much information indiscriminately in order for users to fulfil their goals.

Hypothesis 2 suggests that a high perception of control over information maintained by social media (cpi_i) has a negative impact on the risk of user victimisation. The results presented in Table 1 provide support of this hypothesis (M.E.=-0.041, p<0.01). Vast amounts of personal data are held by social media sites, and how much control users may exercise over their information has been a point of much debate in recent years. Dinev & Hart (2004) describe an individual's ability to stay in charge of information disclosure as the perceived ability to control submitted information. Information privacy, according to Moor (1997) and Tavani (2000), is linked to the control or restrictions users have over their personal information. Social networking sites generally provide control over privacy settings to restrict outside access to individual user accounts, and use profile tracker programmes to see who views their profiles (Reyns et al., 2011). Control over personal information is also reflected in the principle of guardianship in the RAT. When users perceive having control over their information posted on social media, they may be less likely to become victims of cybercrime.

Our model examines whether individuals with better computer skills and higher technical efficacy (te_i) are better protected from threats of cybercrime. This premise is expressed in **hypothesis 3.** The proliferation of technologies into every aspect of personal and professional activity has possibly led to the increased importance of technological efficacy for individuals. Our findings, however, suggest that there is a positive and statistically insignificant relationship between higher technical efficacy and victimisation. The positive coefficient may be explained, for example, by personal perceptions of individual skills, leading to behaviour which increases the risk of becoming a victim of cybercrime.

Hypothesis 4 and **hypothesis 5** suggest a link between perceived risk and victimisation and risk propensity and victimisation, respectively. Risk perception has been associated by theorists with 'consequences',' losses', 'damages' and 'social and financial harm' (Crowe & Horn,1967; Joffe, 2003; Kaplan & Garrick, 1981; Kasperson et al., 1988; March & Shapira, 1987; Renn, 1998; Renn & Rohrmann, 2000; Trimpop, 1994). Risk-taking or avoidance has been strongly linked to individual attitudes and perceptions (see Liu et al., 2005; Trimpop,

1994), including the premise of TRA and TPB. Risk propensity refers to the willingness to assume risk (Luhmann, 1988; Mayer et al., 1995; Rousseau et al., 1998; Sheppard & Sherman, 1998). Consequently, risky behaviour may increase the likelihood of user victimisation (Whittle et al., 2012). Risk-taking in the context of social media manifests itself in user behaviour involving, for example, communicating with strangers' online and sharing personal information with malicious illegal parties (fourth parties in the extended personal information privacy model of Conger et al., 2012). The consequences of risk-taking behaviour range from financial loss due to theft of personal identities via SNS to physical or psychological damage caused by cyberstalking or bullying (Cases, 2002; Dowling & Staelin, 1994; Hutchings, 2013). Our results, however, show that risk propensity ($rpro_i$) is positively related to cybercrime victimisation (M.E.=0.026, $p<0.10$) supporting hypothesis 5; however, they also show that risk perceptions ($rper_i$) have an insignificant effect, thus rejecting hypothesis 4.

Implications for Policy and Practice

The findings of the study provide three important practical implications. Firstly, the results show that social networking usage has an impact on online victimisation, but the sign, significance and magnitude of the effect depend on the network type. Specifically, high usage of narrow purpose SNS (typically services that support groups with specific interests) and multipurpose SNS that are dominant in the social media sphere (such as Facebook) do not increase the likelihood of becoming a victim of cybercrime. In cases of multipurpose dominant social media, the probability actually decreases. However, high usage of SNS for knowledge-exchange purposes is found to increase the likelihood of victimisation. This is perhaps due to the fact that sharing purpose SNS expose more sensitive information that can be used by potential criminals. Secondly, cybercrime can be mitigated by increasing service security controls on social media sites, and by improving skills of end users to better control the process of personal information disclosure. Finally, awareness of risky user behaviour on social media plays a significant role in reducing cyber victimisation. Awareness of risk has

Table 1: Probit estimates

	Model 1		Model 2		Model 3		Model 4^	
Focal variables	M.E.	S.E.	M.E.	S.E.	M.E.	S.E.	M.E.	S.E.
Multipurpose SNS usage($msns_i$)	-0.057***	0.022	-0.046**	0.023	-0.045**	0.022	-0.049*	0.025
Narrow purpose SNS usage ($nsns_i$)	0.039	0.025	0.031	0.026				
Knowledge-exchange purpose SNS usage ($ksns_i$)	0.091***	0.022	0.085***	0.023	0.083***	0.023	0.083***	0.025
Perceived control (cpi_i)			-0.041***	0.015	-0.042***	0.015	-0.042***	0.015
Technical efficacy (te_i)			0.023	0.017	0.024	0.017	0.026	0.019
Perceived risk ($rper_i$)			-0.027	0.017	-0.026	0.017	-0.025	0.018
Risk propensity ($rpro_i$)			0.023	0.014	0.026*	0.014	0.027*	0.015
Controls	*No*		*No*		*No*		*Yes*	
Log-likelihood	-306.465		-300.307		-301.202		-292.123	
Observation	502		502		502		502	

Notes: ***p < 0.01, **p < 0 .05 and *p < 0.10. Dependent variable: 1= Being a victim of cybercrime; and 0 = otherwise. Marginal effects (M.E.) and robust standard errors (S.E.) are reported. We aggregate the social media usage categories to create an index of overall social media use. We find, however, that the coefficient of this variable is statistically insignificant (M.E.=0.040 and S.E.=0.030). This is possibly is due to the fact that the dual purpose and sharing purpose variables have opposite effects, and they may therefore cancel each other out when an overall measure is considered.

^ Mode 4 estimates equation 1 controlling for various individual characteristics. Specifically, this model finds that individuals aged 29–38 (M.E.=-0.162), 39-49 (M.E.=-0.201) and 49-58 (M.E.=-0.189) are less likely to be victims of cybercrime than individuals aged 18–28. Also, individuals with professional (M.E.=0.19) and technical status(M.E.=0.15) are more likely to be victims than students. We find that there is no gender effect on victimisation. Finally, those with an undergraduate qualification have less probability of being a victim of cybercrime (M.E.=-0.1) than those with a postgraduate qualification (full results are available upon request).We also experiment using an interaction term between control and efficacy but we find no significant statistical association.

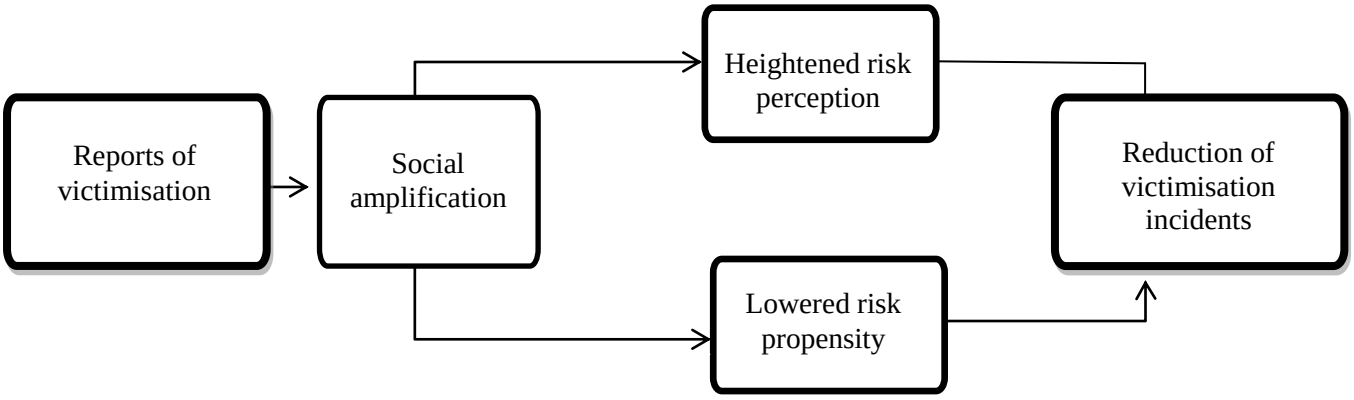
been shown to be an antecedent of the intention to perform security behaviours, both in personal and professional contexts. For this reason, most studies that take into account the social aspects of information security advocate education and awareness programmes (Dutta & McCrohan, 2002; Von Solms, 2001a; 2001b; Warman, 1992; Whitman, 2003). Although information security in social networking is traditionally seen as an individual or personal issue, many businesses, schools, colleges and universities provide some form of educational programme aimed at raising awareness of the risks of cybercrime victimisation. It is clear from the research presented here that much remains to be done, but that effective risk awareness education programmes can help improve risk perceptions.

However, it is questionable whether the awareness education and media involvement in reducing online victimisation is effective across all social levels. For example, some argue that older population are more vulnerable to online frauds due to their accumulated wealth, trusting nature and social isolation (James et al., 2014). Compared to younger population, older victims are less likely to report online victimisation (Pak & Shadel, 2011) and the lack of data on victimisation of senior citizens makes it an arduous task to clearly identify the causes of such victimisation. In terms of awareness education for senior citizens, information may be disseminated through legislatures (as has been done in the US by the introduction, for example, of the Protecting Seniors from Fraud Act in 2000). The need for security education is quite specific to this population cluster and thus requires further research attention.

Beyond education and awareness training through the workplace, schools, colleges and university (among others), the media represents another potential source of information and learning. With the increased media attention to information security and privacy issues, there is a lack of research on how perceptions of risks associated with social media victimisation are amplified by the media. We know from the *social amplification of risk* literature that even with well-documented risks, people's ability to understand, let alone assess, the scale of the danger is much less clear. It is therefore necessary to understand the role that society (notably the media) plays in the amplification (or reduction) of risk (Rosa, 2003). It is likely that as numbers of reports of victimisation increase, so will risk awareness. Our research suggests that this would then result in lower victimisation risks. This is illustrated in Figure 3. Unfortunately, at times there is a tendency to downplay security breaches in the corporate sector, despite evidence that openness and disclosure generally results in a lower likelihood of future breaches (Wang et al., 2013).While, to our knowledge, there has been no studies looking at disclosure (or lack of) of victimisation incidents in a

social media context, there are good reasons to speculate – both from the extant literature and the research presented in this paper – that this would be detrimental to lowering risks.

Figure 3. Social media implications for cybercrime victimisation



This research urges further exploration of the ways to raise user awareness about the negative consequences of social networking activity, and calls for external interventions to enforce privacy and information security measures on social networking sites, which are currently lacking. At the same time, the fact that social amplification may play a role in the reduction of victimisation suggests that social media services should be encouraged (or even compelled) to publish security breaches, as it is likely to increase safer use. In this respect, the results of this study help inform the development of social media user awareness practices, and enhance security mechanisms implemented on social networking platforms. Furthermore, the findings are important to future researchers and scholars who may wish to test similar relationships in different contexts.

Conclusions

While significant research attention has focused on exploring positive outcomes of social networking, the negative aspects of social technology lack academic attention and their implications for SNS industry and users are rarely discussed. The main contribution of this research is in bridging the gap in the current literature exploring the link between user behaviour on social networks and the risk of their online victimisation. We investigated behaviours on social media, such as usage, as well as users' attitudes, for examples their ability to control individual information, technical efficacy, and perceptions of risk and risk propensity, and their association with becoming a victim of cybercrime.

Previous research finds that online victimisation leads to various negative outcomes for the victim. Even when no financial or physical harm is inflicted directly, the negative

impact, in terms of social and emotional outcomes, can be significantly exacerbated by the amount of time spent online (Brown et al., 2014). The findings of this study show that the overall intensity of social media usage alone may not increase the risk of becoming a victim of cybercrime. However, when the effects are considered by the category of SNS, we find that the usage of the dominant multipurpose social media services (such as Facebook) is negatively related to victimisation. On the other hand activity on the knowledge-sharing purpose social media increases individual's chances of becoming a victim of cybercrime. Due to the strong interest of the press in the delinquency linked to the usage of the dominant social media sites, the public has grown wary of their inherent risks, and are now becoming more security conscious. In addition, there is an increasing amount of interest in the role of other users in the protection from victimisation (see, for example, Bastiaensens et al., 2014) and social learning (gaining skills by observing each other's behaviour). It is also possible that intensive users of the dominant multi-purpose social media services have a higher perception of friendship ties on these networks, which might in turn create safer perceived usage environment.

We find no evidence that personal computer efficacy plays an important role in the risk of victimisation. We also find that the opportunity for online victimisation increases with higher risk propensity of users, and not to individual risk perception on social networking users. Importantly, the results show that the need for having and exercising control over personal information on social media is an important aspect which needs the attention of both SNS industry and policymakers to raise awareness, as well asto improve users' skills to control information shared with SNS. Similarly, Hajli & Lin (2014) found a strong link between perceived control and perceived privacy risks, as well as a link between perceived control and information sharing behaviors. However we were able to go one step further: not only do users with high perceived control feel safer and share more - they are also less likely to become a victim of cyber-crime. This is an important finding, indicating that service providers and developers need to take more responsibility in implementing controls for safeguarding social networking users.

There have been many reports of social networks making it 'too difficult' for users to exercise control over their private information, and of calls for this to be changed. Such a discourse is often couched in civil liberty and quasi-human rights terms. In parallel there are calls for SNS to introduce tools (e.g. anti-bullying reporting tools) and automatic security measures (such as dual factor identification requests when users log-in from unknown computers), and give greater control to users (Gradon, 2013; Cassidy et al., 2012; Whittle et

al., 2012). This paper adds to these calls by suggesting that not only do privacy settings, their availability, ease of discovery and ease of use are important from a perceived privacy point of view, but they might be also important in making users more responsible for their personal information, as we have shown that users who perceive high levels of control are less likely to be victimised. Perhaps SNS should be more open about the risks faced by their users and through the application of the social amplification theory proceed to draw users' attention to the responsible online behaviours, while at the same time improving the industry efforts on the automatic prevention and detection techniques to safeguard users.

Limitations and Directions for Future Research

Our study has some limitations. We can only measure victimisation that is known to users. However, since we use an aggregate measure of victimisation this may more closely reflect the underlying trends rather than studying individual cyber-crimes separately. Also, the legal environment is identified as a variable affecting information security, but due to the complex nature of national and international legal frameworks pertaining to information security, it is not included in our research model. For the same reason, economic structure or technological status across countries is not considered when conducting this research. Testing such variables along with information security constructs considered in this study opens up opportunities for future research. Additionally, future survey design and analysis may wish to include questions regarding the frequency of victimisation and investigate how victimisation rates relate to various types of cyber-crimes and to the timeline of victimisation. The data used in this study did not explore the exact times of victimisation which may relate to changes in security settings and SNS countermeasures. Including objective measures of computer skills will also allow direct and potentially interesting comparison with the self-reported data. Lastly, interpretive research is likely to prove very useful in explaining some of the intricate phenomena we have uncovered. It has long been recognised in information security research that an in-depth understanding of user behaviours and motivations can be gained through qualitative research such as discourse analysis (Bowen-Schrire et al., 2004). Furthermore**,** even though our data is gathered from the larger population of social media users on the Internet, the sample size is comparatively smaller compared to the billions of worldwide social media users and refers to a single time period. A longitudinal and larger scale study, for example, could provide additional insight into whether the effects of social networking usage on victimisation differ across crime categories and how perceptions of

security, risk and control adjust after victimisation. Finally, future research should incorporate a control group (non-SNS users) in the design. Therefore, our results should be interpreted with caution, but should still stimulate future empirical work in the field.

References

Ajzen, I. (1985) From intentions to actions: a theory of planned behaviour. In: *Action Control: From Cognition to Behaviour*, Kuhl, J.& Beckman, J.(eds), pp. 11–39. Springer-Verlag, Berlin.

Ajzen, I. (1988) *Attitudes, Personality, and Behaviour*. Dorsey Press, Chicago, IL.

Ajzen, I. & Fishbein, M. (1980) *Understanding Attitudes and Predicting Social Behaviour*. Prentice-Hall, Englewood Cliffs, NJ.

Al-Daraiseh, A. A., Al-Joudi, A. S., Al-Gahtani, H. B., & Al-Qahtani, M. S. (2014) Social Networks' Benefits, Privacy, and Identity Theft: KSA Case Study. Social Networks, **5**(12), 129-143.

Anderson, C.L. & Agarwal, R. (2010) Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, **34**, 613–643.

Bandura, A. (1997) Self-efficacy. New York: Freeman.

Bartus, T. (2005) Estimation of marginal effects using margeff. *Stata Journal*, **5**, 309-329.

Bastiaensens, S., Vandebosch, H., Poels, K., Van Cleemput, K., DeSmet, A. & De Bourdeaudhuij, I. (2014) Cyberbullying on social network sites. An experimental study into bystanders' behavioural intentions to help the victim or reinforce the bully. *Computers in Human Behavior*, 31, 259-271.

Bhutta, C.B. (2012) Not by the book: Facebook as a sampling frame. *Sociological Methods and Research*, **41**, 57–88.

Bougaardt, G. and Kyobe, M. (2011) Investigating the factors inhibiting SMEs from recognising and measuring losses from cybercrime in South Africa. (eds.) Grant, K. In *Proceedings of the 2nd International Conference on Information Management and Evaluation*, Academic Publishing International Limited, UK.

Bowen-Schrire, M., Reid, B, Ezingeard J.-N. & Birchall, D. (2004) Identity management and power in the discourse of information security managers. Proceedings of *6th International Conference on Organizational Discourse International Centre for Research in Organizational Discourse, Strategy and Change (ICRODSC)*. Amsterdam, The Netherlands.

Brown, C. F., Demaray, M. K. & Secord, S. M. (2014) Cyber victimization in middle school and relations to social emotional outcomes. *Computers in Human Behavior*, 35, 12-21.

Burak, L.J., Rosenthal, M. & Richardson, K. (2013) Examining attitudes, beliefs, and intentions regarding the use of exercise as punishment in physical education and sport: an application of the theory of reasoned action. *Journal of Applied Social Psychology*, **43**, 1436–1445.

Burns, S. & Roberts, L. (2013) Applying the theory of planned behaviour to predicting online safety behaviour.*Crime Prevention & Community Safety*, **15**, 48–64.

Campbell, K., Gordon, L.A., Loeb, M.P. & Zhou, L. (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, **11**,431–448.

Cases, A.-S. (2002) Perceived risk and risk-reduction strategies in Internet shopping. *International Review of Retail, Distribution and Consumer Research*, **12**, 375–394.

Cassidy, W., Brown, K. & Jackson, M. (2012) "Making Kind Cool": Parents' Suggestions for Preventing Cyber Bullying and Fostering Cyber Kindness. *Journal of Educational Computing Research*, **46**(4), 415-436.

Cavusoglu, H., Mishra,B. & Raghunathan,S. (2004) The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce*, **9**,69–104.

Chadee, D., Austen, L. & Ditton, J. (2007) The relationship between likelihood and fear of criminal victimisation: evaluating risk sensitivity as a mediating concept. Available at: http://shura.shu.ac.uk/603/ [Accessed 22 October 2013].

Chadwick, S. A. (2001) Communicating trust in e-commerce interactions. *Management Communication Quarterly*, **14**,4, 653-658.

Chang, H.H. & Chen, S.W. (2008) The impact of online store environment cues on purchase intention. *Online Information Review*, **32**, 818–841.

Chen, R. & Sharma, S.K. (2013) Self-disclosure at social networking sites: an exploration through relational capital. *Information Systems Frontiers*, **15**, 269–278.

Choi, K. (2008)Computer crime victimisation and integrated theory: an empirical assessment. *International Journal of Cyber Criminology*,**2**, 308–333.

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

Conger, S., Pratt, J.H. & Loch, K. (2012) Personal information privacy and emerging technologies. *Information Systems Journal*, **23**, 401–407.

Connolly, R. & Bannister, F. (2006) Factors influencing Irish consumers' trust in Internet shopping. *Journal of Information Technology*, **22**, 102–118.

Cronje, S. & Zietsman, J.M. (2009) Criminology. FET College Series, Pearson Publishers.

Crowe, R.M. & Horn, R.C. (1967) The meaning of risk. *The Journal of Risk and Insurance*, **3**, 459–474.

Dhillon, G. & Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, **11**, 127–153.

Dinev, T., Goo, J., Hu, Q. & Nam, K. (2009) User behaviour towards protective information technologies: the roel of national cultural differences. *Information Systems Journal*, **19**, 391–412.

Dinev, T. & Hart, P. (2004) Internet privacy concerns and their antecedentsmeasurement validity and a regression model. *Behaviour & Information Technology*, **23**, 413–422.

Dowling, G.R. & Staelin, R. (1994) A model of perceived risk and intended risk-handling activity. *The Journal of Consumer Research*, **21**, 119–134.

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014). Cyberbullying in social networking sites: An adolescent victim's perspective. *Computers in Human Behavior*, **36**, 13-20.

Duffy, M.E. (2002) Methodological issues in web-based research. *Journal of Nursing Scholarship*, **34**, 83–88.

Duggan, M. & Brenner, J. (2012) The demographics of social media users – 2012. Pew Research Center Internet & American Life Project. Available at: http://www.lateledipenelope.it/public/513cbff2daf54.pdf [Accessed 31 October 2013].

Dutta, A. & McCrohan, K. (2002) Management's role in information security in a cyber economy. *California Management Review*, **45**(1), 67–87.

Festl, R. & Quandt, T. (2013) Social relations and cyber bullying: the influence of individual and structural attributes on victimization and perpetration via the Internet. *Human Communication Research*, **39**, 101–126.

Fishbein, M. & Ajzen, I. (1975) *Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA.

Foxman, E.R. & Kilcoyne, P. (1993)Information technology, marketing practice, and consumer privacy: ethical issues. *Journal of Public Policy and Marketing*,**12**, 106–119.

George, J.F. (2002) Influences on the intent to make Internet purchases. *Internet Research*, **12**, 165–180.

Gosling, S.D. & Vazire, S. (2004) Should we trust Web-based studies?:acomprehensive analysis of six preconceptions about Internet questionnaires. *American Psychologist*, **59**, 93–104.

Gradon, K. (2013) Crime science and the Internet battlefield: securing the analog world from digital crime. *Security & Privacy*, **11**, 93–95.

Greene, W. H. (2000) Econometric Analysis, Fourth Edition, Prentice Hall International Editions.

Guitton, C. (2013) Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security*, **22**, 21–35.

Hajli, N. & Lin, X. (2014) Exploring the Security of Information Sharing on SocialNetworking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics.* (forthcoming). DOI: 10.1007/s10551-014-2346-x

Hoffman, D.L. & Fodor, M. (2010) Can you measure the ROI of your social media marketing? *MIT Sloan Management Review*, **52**, 41–49.

Holt, T.J. & Bossler, A.M. (2009) Examining the applicability of lifestyle-routine activity theory for cybercrime victimisation. *Deviant Behaviour*, **30**, 1–25.

Hutchings, A. (2013) Hacking and fraud: qualitative analysis of online offending and victimization. In: *Global Criminology: Crime and Victimization in a Globalized Era*, Jaishankar, K. & Ronel, N. (eds), pp. 93–114. CRC Press, Boca Raton, FL.

Hsia, J. W., Chang, C. C., & Tseng, A. H. (2014) Effects of individuals' locus of control and computer self-efficacy on their e-learning acceptance in high-tech companies. *Behaviour & Information Technology*, **33**(1), 51-64.

Isaac, S. & Michael, W.B. (1981) *Handbook in Research and Evaluation*. EdITS Publishers, San Diego, CA.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014) Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, **26**(2), 107-122.

Joffe, H. (2003) Risk: from perception to social representation. *British Journal of Social Psychology*, **42**, 55–73.

Junco, R. (2012) Too much face and not enough books: the relationship between multiple indices of Facebook use and academic performance. *Computers in Human Behaviour*, **28**, 187–198.

Kaplan, A.M. & Haenlein, M. (2010) Users of the world, unite! The challenges and opportunities of social media. *Business Horizons,* **53**, 59–68.

Kaplan, S. & Garrick, B.J. (1981) On the quantitative definition of risk. *Risk Analysis*,**1**,11–27.

Kasperson, J.X., Kasperson, R.E., Pidgeon, N. & Slovic, P. (2003) *The Social Amplification of Risk: Assessing Fifteen Years of Research and Theory*. Cambridge University Press, Cambridge, UK.

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson,J.X. & Ratick,S.(1988) The socialamplification of risk: a conceptual framework. *Risk Analysis*,**8**, 177–187.

Kietzmann, J.H., Hermkens,K., McCarthy,I.P. & Silvestre, B.S. (2011) Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, **54**, 241–251.

Krejcie, R.V. & Morgan, D.W. (1970) Determining sample size for research activities. *Educational and Psychological Measurement,* **30**, 607–610.

Landoll, R.R., La Greca, A.M. & Lai, B.S. (2013) Aversive peer experiences on social networking sites: development of the social networking-peer experiences questionnaire (SN-PEQ). *Journal of Research on Adolescence*, **23**, 695–705.

Lee, M.K.O. & Turban, E. (2001)A trust model for consumer Internet shopping. *International Journal of Electronic Commerce*, **6**, 75–91.

Liu, C., Marchewka, J.T., Lu, J. & Yu, C.S. (2005) Beyond concern – a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, **42**(2), 289–304.

Luhmann, N. (1988) Familiarity, confidence, trust: problems and alternatives. In: *Trust: Making and Breaking Cooperative Relations*, Gambetta, D.G. (ed.), pp. 94–107. Blackwell, New York, NY.

Madden, T.J., Ellen, P.S. & Ajzen, I. (1992)A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin*,**18**, 3–9.

Malhotra,N.K., Kim,S.S. &Agarwal,J.(2004) Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, **15**, 336–355.

March, J.G. & Shapira, Z. (1987) Managerial perspectives on risk and risk taking. *Management Science*, **33**, 1404–1418.

Marcum, C. D. (2008) Identifying Potential Factors of Adolescent Online Victimization, *International Journal of Cyber Criminology*, 2(2): 346–367.

Marsden, P.V. & Wright, J.D. (2010) *Handbook of Survey Research*, 2ndedn. Emerald Group Publishing, UK.

Mayer,R.C., Davis,J.H. & Schoorman, F.D.(1995) An integrative model of organizational trust. *Academy of Management Review*,**20**, 709–734.

Mesch, G. S. (2009) Parental mediation, online activities, and cyberbullying. *Cyber Psychology & Behavior*, **12**(4), 387-393.

Montano, D.E. & Kasprzyk, D. (2008) Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health Behavior and Health Education: Theory, Research, and Practice*, **4**, 67–95.

Moor, J.H. (1997) Towards a theory of privacy in the information age. *Computers and Society*, **27**, 27–32.

Nhan, J., Kinkade, P. & Burns, R. (2009) Finding a pot of gold at the end of an Internet rainbow: further examination of fraudulent email solicitation. *International Journal of Cyber Criminology*, **3**, 452–475.

Pavlou, P.A. & Chai, L. (2002) What drives electronic commerce across cultures? A cross-cultural empirical investigation of the theory of planned behavior. *Journal of Electronic Commerce Research*, **3**, 240–253.

Pedneault, A. & Beauregard, E. (2013)Routine activities and time use: a latent profile approach to sexual offenders' lifestyles. *Sexual Abuse: A Journal of Research and Treatment*, **26**, 1–24.

Pettit, F.A. (2002)A comparison of World Wide Web and pencil personality questionnaires. *Behaviour Research Methods, Instruments, & Computers*, **34**, 50–54.

Pittaro, M.L. (2007) Cyberstalking: an analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, **1**, 180–197.

Podsakoff, P. M., & MacKenzie, S. B. (1994). An examination of the psychometric properties and nomological validity of some revised and reduced substitutes for leadership scales. *Journal of Applied Psychology*, 79, 702-713.

Pratt, T.C., Holtfreter, K. & Reisig, M.D. (2010) Routine online activity and Internet fraud targeting: extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, **47**, 267–296.

Rauch, J.E. (2001)Business and social networks in international trade. *Journal of Economic Literature*, **39**, 1177–1203.

Renn,O.(1998)The role of risk perception for risk management. *Reliability Engineering & System Safety*,**59**,49–62.

Renn, O. & Rohrmann, B. (2000) *Cross-cultural Risk Perception: A Survey of Empirical Studies*. Kluwer Academic Publishers, USA.

Reyns, B. W., & Henson, B. (2015) The Thief With a Thousand Faces and the Victim With None Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology*, 1-21.

Reyns, B.W. (2013) Online routines and identity theft victimisation: further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*,**50**, 216–238.

Reyns, B.W., Henson, B. & Fisher, B.S. (2011) Being pursued online: applying cyberlifestyle-routine activities theory to cyberstalking victimisation. *Criminal Justice and Behaviour*,**38**, 1149–1169.

Rosa, E.A. (2003) The logical structure of the social amplification of risk framework (SARF): metatheoretical foundations and policy implications. In:*The Social Amplification of Risk*, Pidgeon, N., Kasperson, R.E. &Slovic, P. (eds), Cambridge University Press, Cambridge, UK, 47-79.

Rotter, J.B. (1966) Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs*, **80**, 1, 1–28.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. & Camerer, C. (1998) Not so different after all: a cross-discipline view of trust. *Academy of Management Review*, **23**, 393–404.

Sam, H.K., Othman, A.E.A. & Nordin, Z.S. (2005) Computer self-efficacy, computer anxiety, and attitudes toward the Internet: a study among undergraduates in Unimas. *Educational Technology & Society*, **8**, 205–219.

Sheehan, K.B. & Hoy, M.G. (2000) Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, **19**, 62–73.

Shelton, A.K. & Skalski, P. (2013) Blinded by the light: illuminating the dark side of social network use through content analysis. *Computers in Human Behavior*.doi:http://dx.doi.org/10.1016/j.chb.2013.08.017

Sheppard,B.H. & Sherman, D.M. (1998) The grammars of trust: a model and general implications. *Academy of Management Review*, **23**, 422–437.

Sherchan, W., Nepal, S. & Paris, C. (2013) A survey of trust in social networks. *ACM Computing Surveys (CSUR)*, **45**(4),1–46.

Sitkin, S.B. & Pablo, A.L. (1995) Reconceptualizing the determinants of risk behaviour. *Academy of Management Review*, **17**,9–38.

Smith, H., Milberg, S. & Burke, S. (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*,**20**, 167–196.

Sodhi, J.S. & Sharma, S. (2012) Conceptualizing of social networking sites. *International Journal of Computer Science*, **9**(1), 422–428.

Stutzman, F., Grossy, R. & Acquistiz, A. (2013) Silent listeners: the evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*,**4**(2), 7–41.

Tavani, H.T. (2000) Privacy and the Internet. Available at: http://www.bc.edu/bc_org/avp/law/st_org/iptf/commentary/content/2000041901.html[Accessed 24 April 2013].

Trimpop, R.(1994) *The Psychology of Risk Taking Behaviour*. ElsevierScience, The Netherlands.

Turel, O. & Serenko, A. (2012) The benefits and dangers of enjoyment with social networking websites. *European Journal of Information Systems*, **21**, 512–528.

Tynes, B.M. & Mitchell, K.J. (2013) Black youth beyond the digital divide: age and gender differences in Internet use, communication patterns, and victimization experiences. *Journal of Black Psychology*, **May**, 1–17. doi: 10.1177/0095798413487555

Von Solms, B. (2001a) Corporate governance and information security. *Computers & Security*, **20**(3), 215–218.

Von Solms, B. (2001b) Information security: a multidimensional discipline. *Computers & Security*, **20**(6), 504–508.

Van Wilsem, J. (2013) Bought it, but never got it: assessing risk factors for online consumer fraud victimization. *European Sociological Review*,**29**(2),168–178.

Walsh, J.P., Kiesler, S., Sproull, L.S. & Hesse, B.W. (1992) Self-selected and randomly selected respondents in computer network survey. *Public Opinion Quarterly*, **56**,241–244.

Wang, T., Kannan, K. & Ulmer, J. (2013)The association between the disclosure and the realization of information security risk factors. *Information Systems Research*,**24**(2), 201–218.

Warman, A.R. (1992)Organizational computer security policy: the reality.*European Journal of Information Systems*, **1**(5), 305–310.

Whitman, M.E. (2003) Enemy at the gate: threats to information security. *Communications of the ACM*, **46**(8), 91–95.

Whittle, H., Hamilton-Giachritsis, C., Beech, A. & Collings, G. (2012)A review of online grooming: characteristics and concerns. *Aggression and Violent Behavior*, **18(**1),62–70.

Xiang, Z. & Gretzel, U. (2010) Role of social media in online travel information search. *Tourism Management*, **31**, 179–188.

Xu, H., Dinev, T., Smith, H.J. & Hart, P. (2008) Examining the formation of individual's privacy concerns: toward an integrative view. Proceedings of the *29th International Conference on Information Systems (ICIS)*, Paris.

Zimmerman, B.J. (2000) Self-efficacy: an essential motive to learn. *Contemporary Educational Psychology*, 25, 82–91.

Appendix. Scale items used as independent variable measures

Construct	Measurement scale in original study	Original Question	Question adopted for this study	Source
Control over personal information (cpi_i)	Strongly disagree to strongly agree (seven points)	1. I believe I have control over who can get access to my personal information collected by these websites. 2. I think I have control over what personal information is released by these websites. 3. I believe I have control over how personal information is used by these websites. 4. I believe I can control my personal information provided to these websites.	1. I believe I have control over who can get access to my personal information collected by SNS. 2. I think I have control over what personal information is released by SNS. 3. I believe I have control over how personal information is used by SNS. 4. I believe I can control my personal information provided to SNS.	Xu et al, 2008
Technical efficacy (te_i)	Strongly disagree to strongly agree (five points)	1. I feel confident working on a personal computer. 2. I feel confident understanding terms/ words relating to computer hardware. 3. I feel confident understanding terms/words relating to computer software. 4. I feel confident troubleshooting computer problems.	1. I feel confident working on a personal computer. 2. I feel confident understanding terms/ words relating to computer hardware. 3. I feel confident understanding terms/words relating to computer software. 4. I feel confident troubleshooting computer problems.	Sam et al., 2005
Risk perception ($rper_i$)	Strongly disagree to strongly agree (seven points)	1. In general, it would be risky to give (information) to online companies. 2. There would be high potential for loss associated with giving (information) to online firms. 3. There would be too much uncertainty associated with giving (information) to online firms. 4. Providing online firms with (information) would involve many unexpected problems.	1. In general, it would be risky to give (information) to SNS 2. There would be high potential for loss associated with giving (information) to SNS. 3. There would be too much uncertainty associated with giving (information) to SNS. 4. Providing SNS with (information) would involve many unexpected problems.	Malhotra et al., 2004
Risk propensity ($rpro_i$)	Strongly disagree to strongly agree (number of scale points not reported)	1. I am willing to take substantial risks to do online shopping. 2. I am willing to accept some risk of losing money if online shopping is likely to involve an insignificant amount of risk.	1. I am willing to take substantial risks to do online shopping. 2. I am willing to accept some risk of losing money if online shopping is likely to involve an insignificant amount of risk. 3. I am willing to accept some risk to my personal information if online shopping is likely to involve an insignificant amount of risk. 4. I am more comfortable using a familiar SNS than something I am not sure about. 5. I am cautious when trying new SNS.	Chang & Chen, 2008