The Results of Criminal Activity on Social Networking Sites - User Behaviour Leading to Victimisation

INTRODUCTION

Social networking sites have become the mainstream communication medium for individuals, especially young people (Holt and Bossler, 2014), and businesses (Culnan. et al., 2010). At present there are approximately 4.17 billion internet users worldwide, thus demonstrating a sustained growth from the year 2015 by a quarter. Of these, 3.4 billion are active social media users with a similar proportion of mobile internet users (3.7 billion) according to Statista (2018). However, with the continuous loss of control over personal information that is exposed online, individuals and businesses present easy targets for non-technical attacks ranging from spear-fishing to whaling leading to serious cyber victimisation (McAlaney et al., 2018). Cybersecurity professionals agree that this security depends on people more than on technical controls and countermeasures. Recent reviews of cyber security express that no industry sector is invulnerable to cyber-attacks and that the public sector tops the list for targeted security incidents (Benson, 2017). This is largely attributed to the weaker cyber security mind-set of employees. On the other hand, the financial sector, year on year, experiences the highest volume of cyber breaches. These are predominantly aimed at financial gain or espionage. What is common among these rather different sectors is that the attack vector by cyber criminals starts with social engineering. The weakest link in the security chain is still the human element. Irrespective of the market segment, the losses are huge contributing to the current global cost of cybercrime estimation of approximately $600 billion (McAffee, 2018).

Unsurprisingly, the human behaviour in an online context has been addressed by researchers for some time. The cybersecurity industry, policymakers, law enforcement agencies and public as well as private sector organisations are yet to realise the factors affecting the risk of online victimisation and the impact on individuals and businesses (Taylor et al., 2010). In order to improve cybersecurity practices, there is a need for a discussion acknowledging that cybersecurity is inherently a complex socio-technical system.

This chapter presents an overview of emerging issues in the psychology of human behaviour and the evolving nature of cyber threats. Theories of crime and empirical studies on user victimisation as seen on social networks are reviewed. The chapter reflects on the role of social engineering as the entry point of many sophisticated attacks and highlights the relevance of the human element as the starting point of implementing cyber security programmes in organisations as well as securing individual online behaviour. Specifically, the criminological theories of crime (i.e. self-control and rational choice theories) are discussed. For example, Cohen and Felson (1979) argue that crime will occur when there is a motivated offender, a suitable target/potential victim and the absence of guardians capable of preventing violation. The latter can be in the form of physical guardianship (e.g. antivirus) or personal guardianship (e.g. computer skills). In addition, Gottfredson and Hirschi (1990) suggest that crime and victimisation are associated with low levels of self-control. We then turn to empirical studies that have examined the user behaviour on social networking sites leading to victimisation (e.g. Hansen et al., 2017; Saridakis et al., 2016; Benson et al., 2015a-c). Issues associated with the emerging trends in human behaviour research and ethics are presented for further discussion. The chapter concludes with a set of open research questions warranting immediate academic attention to avoid the exponential growth of future information breaches.

~~BACKGROUND: SOCIAL PLATFORMS~~

Research suggests that the frequency of internet usage shares a positive association with cyberbullying and victimisation (Mesch, 2009). However, in modern times, most individuals, public organizations and private ones are heavily dependent on the usage of the internet to carry out their daily business activities and communications, therefore, limiting internet use is not a plausible solution to the problem of being a victim of cybercrime. Thus, there is a need for examining the roots of the problem, which starts with people and the psychology behind human behaviour that triggers cybercriminal activities. To this end, a number of theories have been developed to explain the psychology behind criminal activities. The routine activity theory (RAT) proposed by Cohen and Felson (1979), for example, suggest that crime is contingent on the following three components: exposure to a motivated offender, a suitable target and the lack or absence of capable guardians to prevent the violations. Furthermore, Cohen and Felson (1979) describe the suitability of a target as their attractiveness to the motivated offender as well as their availability for the crime. Therefore, if there is a situation where all three components of the RAT are present, then a crime is likely to occur.

According to Marcum el al. (2010), crime is not a random event, instead it follows a consistent pattern where the three components of the RAT are required. Eck and Clarke (2003) propose that the RAT can be expanded for cybercrimes where the offender and target do not necessarily share the same physical space but can share the same cyberspace such as the internet or any shared network.

In the context of cybercrime, the motivated offender is someone who is not only capable of committing the cybercrime but is also willing to commit it because he/she is motivated by personal gain such as identity theft, phishing, espionage, unfair investment information, bank fraud, someone's personal information or even revenge. The suitable target can be an individual or an organization who possesses the online information from which the motivated offender can gain. Finally, the guardian can be in the form of a software guardianship (e.g. antivirus or firewall), personal guardianship (e.g. computer skills or cybercrime awareness) and even physical guardianship such as a capable cybercrime unit or security personnel who can protect the parameters of an organization from intruders seeking to gain access to their network server.

Marcum et al. (2010) derive an explanation for the online victimisation of youths (generation Z) using the RAT by suggesting that the great length of time spent on social networking sites increases their exposure to a motivated offender. Also the types of information that they provide on these social networking sites (i.e., age, relationship status, daily activities, and pictures) make them suitable targets for online victimisation. Furthermore, the unsecure location in which the internet is being used by youths combined with their personal and parents' lack of expertise in cyber technology or internet security provides the third component of the RAT, which is the lack of capable guardianship.

While we reason that prior experience of online victimisation by individuals on social networking sites increases their probability of noticing online security features and increasing their guardianship, a study by Benson et al. (2015b) finds otherwise. Benson at al. (2015b) find that there is no connection between these two factors and suggest that this can be explained through an individual's perception of the utility obtained from social networking sites for entertainment, socializing and other activities which is higher than the risk of online victimisation to them.

Another major theory that is used to explain crime and victimisation is the General Theory of Crime (GTC), proposed by Gottfredson and Hirschi (1990) which suggests that the principal causal agent of all crimes and victimisation is low self-control. There are six elements associated with low levels of self-control which are: lack of future orientation, temper/anger, lack of diligence, self-centredness, preference for risk taking and a preference for physical over mental task (Piquero et al., 2005). Individuals with low self-control are more likely to get angered easily than their counterparts who have high self-control and a similar statement can be made about each of the six elements associated with low self-control. According to Gottfredson and Hirschi (1990) there is a lot of shared personal and social characteristics between victims and offenders. Piquero et al. (2005) suggest that offenders of crimes are more likely to be victims of crime compared to non-offenders. The six elements of low self-control can be used to explain cybercrime offenders and cybercrime victimisations.

Individuals who demonstrate the first element, which is a lack future orientation, can influence victimisation because they do not consider the long-term consequences of their actions neither do they take precautionary measures to protect the image of their online identities nor to protect their private and personal information from being stolen and shared on the internet. On the other hand, offenders of cybercrime demonstrate a lack of future orientation by failing to consider the illegality of the cybercrimes which they are committing and the long-term consequences if caught, which can possibly include jail sentences and permanent criminal records.

The second element, anger/temper, can result in individuals expressing these emotions on social networking sites which may include politics and other topics that can potentially elicit counter-controlling responses by other individuals who may be offended and thus respond through a cyber-bullying attack. Some cybercrimes such as cyber-bullying and cyber-harassment are as a result of offenders who hold anger for other individuals or firms and therefore seek revenge through cyberattacks.

The third element, lack of diligence, can increase victimisation since an individual who lacks tenacity is less likely to take precautionary measures against cyberattacks such as the installation of an antivirus or firewall and the assurance that it is updated regularly.

Offenders who engage in cybercrimes such as phishing, espionage, bank fraud and the theft of personal information for financial gain exhibit a lack of diligence by choosing to commit cybercrime in order to generate income instead of a legal job. The fourth element, self-centredness, relates to victimisation. Since self-centered individuals are more likely to ignore the advice or request of others and show concern only for their own situation, this can create a lack of awareness of current cybercrime activities and preventative measures. Offenders demonstrate self-centredness through their lack of care for their victims' emotional trauma or financial struggle that can arise from cybercrimes. The fifth element, preference for risk taking, increases victimisation since individuals who are risk takers may visit more risky websites, purchase at untrusted retailers for lower prices and even skip security checks, thus increasing their probability of being attacked. Offenders of cybercrime are also risk takers since the act of committing these crimes exposes them to the consequential risk of being caught. The final element of low self-control can influence victimisation since in non-cybercrimes we can argue that individuals who prefer physical tasks over mental ones are more likely to respond physically when faced with a hostile situation rather than use cognitive skills to arrive at a solution which is similar for offenders. This final element of low self-control is the only one that may not support cybercrime since the offenders of this must have the mental capacity required to commit such an act. According to Schreck (1999) vulnerability to victimisation is a by-product of the psychological appearances of low self-control.

Another theory that describes the psychology of human behavioural influence on crime is known as the rational choice theory (RCT). This theory explains that an offender will violate the law after rationally considering personal factors (i.e., the need for money, family, dependents, revenge, consequence and entertainment) and situational factors (i.e., how well the target is guarded and the competence of the local police service). Therefore, if an offender rationalises that the consequential risk of the crime does not outweigh the reward gained from committing this crime, then the offender will commit the crime (Seigel, 2006). In the context of cybercrime, an offender will commit an act such as cyber-bullying, cyber-harassment, identity theft, espionage and even theft of personal and banking information if the satisfaction obtained through committing any of these cybercrimes is greater than the probability of getting caught by officials in addition to the dissatisfaction felt as a result of the consequences. The rational choice theory can explain how the high number of cybercrimes worldwide, due to the low probability of being caught, may be because of a lack of efficiency, competence and training of local police officials in handling cybercrime incidents. There exist very few studies which used the RCT to explain cybercrime activities, therefore more research is needed in this area.

Finally, there also exist the deviant place theory (DPT) that is used to explain victimisation. According to this theory, individuals who have higher exposure to dangerous places have a higher probability of being a victim of a crime (Siegal, 2006). Therefore, this theory suggests that individuals should avoid dangerous places (e.g. crime hotpots) to lower their probability of being victimised. This theory can be expanded to include cyberspace and not just a physical space. Therefore, in the context of cybercrime, individuals who are exposed to dangerous cyberspace such as unsecure websites and unsecure internet networks, are more likely to be victims of a cybercrime. This theory is closely related to the RAT since the exposure to a dangerous place used in the deviant place theory is similar to the concept of the convergence of the motivated offender and a suitable target used in the routine activity theory.

FOCUS OF THE ARTICLE: LINKING CRIME THEORIES AND EMPIRICAL EVIDENCE

Cyber threats lead to two types of crime (McAlaney et al., 2018). On one hand, the internet technology is used to assist existing offences. Such cyber-enabled crime includes e.g. fraud. The first vector of attacks is often established through the social media, where the offender researchers the victim profiles and/or gets in touch with them. Therefore social media serves as an assistive technology to cyber-enabled crime. On the other hand, cyber-dependent crime exists owing to the opportunities offered by the internet technology. Both hacking and malware distribution are examples of cyber-enabled crime. These crimes are often perpetrated and spread via social platforms, making social networks enablers of convergence of the motivated offender and a suitable target (Saridakis et al., 2015)

There are numerous studies worldwide that have adopted some of these theories of criminology to address the issues surrounding crime, and these theories have been expanded to be used in the analysis of cybercrime in recent times. One such example is a study by James et al. (2014) which suggests that older individuals are more likely to be targets for cybercrimes due to accumulated wealth, social unfamiliarity and trusting nature. This is consistent with the RAT since the older an individual is, the more suitable a target he/she becomes for a motivated offender due to the lack of guardianship. More young adults use the internet and more frequently than older adults, in fact 89% of young adults between the ages of 18-29 uses the internet for social media (Pew Research, 2015). This age group is very similar to the age group of university students. This group also manifests the preferences for conducting the commercial and business activities in purely online mode, making themselves the prime targets for criminal activities within cyberspace. A study by Benson et al. (2015c) finds that university students are less likely to be victims of cybercrimes as compared to non-university students. This can be explained using the Gottfredson and Hirschi (1990) GTC, since university students are generally more future oriented and thus have a higher level of self-control as compared to non-university students. Alternatively, this can also be explained using the RAT since universities' internet servers are very secure and therefore increase the guardianship to prevent cybercrimes.

Research by Marcum et al. (2010) shows that a higher exposure to motivated offenders combined with allowing personal information to be accessible online, results in a higher probability of online victimisation among college and high school students. Furthermore, a study done by Marcum et al. (2010) shows that communication with strangers online and provision of online contacts with personal or private information are the most significant predictors of cyber victimisation. This study is consistent with the RAT and since this activity merges the motivated offender with the suitable target, it is also consistent with the GTC as sharing of private information with strangers is a risky activity associated with lower levels of self-control. Also, it is consistent with the DPT since spending time on social networks with strangers increases your exposure to victimisation in a dangerous place (cyberspace).

The RAT describes the importance of guardianship in the fight against crime and as a preventative measure against victimisation. One form of guardianship in the context of cyberspace is security software. However, the UK Government's National Cyber Security Tracker revealed that only 44 percent of the internet users in the UK installed a security system such as an antivirus software, 37 percent updated these software regularly and furthermore, only 57 percent ensured that a website was secure before purchasing from that website (Home Office 2013, as cited in Williams, 2015). Williams (2015) finds that there is a negative relationship between software guardianship (e.g. antivirus and firewall) and identity theft victimisation and his research quantifies this negative relationship by saying that a reduction in software guardianship by one point will result in an increase in identity theft victimisation by 1.32 times. Additionally, a study on child online safety by Tennakoon et al. (2018) finds that self-employed parents are more likely to monitor their children's internet activities compared to parents who work in the private sector. Hill and Duncan (1987) suggest the "absent mother" hypothesis, which argues that when a mother works away from home it affects her child's behaviour and development since her ability to supervise and socialise with her child is restricted and limited. McLanahan (1985) propose a similar explanation for absent fathers. Therefore, self-employed parents provide extra guardianship through monitoring of their children’s internet usage, which explains the increased guardianship that would result in a lower risk of children being victims of cybercrimes, according to the routine activity theory. Furthermore, Tennakoon et al. (2018) find that self-employed parents use online technology more frequently and are more aware of possible threats online such as cybercrimes, therefore this increases their capabilities as guardians to protect their children from cyberattacks.

Cybercrime includes identity theft and online banking information fraud. A study by Williams (2015) finds that individuals who sell goods online have a victimisation rate that is 1.56 times higher than those who do not sell goods online. Another study by Pratt et al. (2010) finds that the routine of online shopping at online stores and spending time online are significant predictors of cybercrime. These two factors are more significant than the age and education of consumers. Therefore, it can be reasoned that the act of selling, auctioning or buying goods online is a risky routine activity that will increase the likelihood of being victimised in cyberspace, which is consistent with the theories discussed above.

Moreover, research shows that increased usage of social networking sites tends to increase the probability of convergence between motivated offenders and suitable victims in cyberspace (Reyns et al., 2011). Interestingly, however, Saridakis et al. (2016) find that individuals who have a higher usage of dominant multipurpose social media sites (e.g. Facebook and Google+) are less likely to be victims of cybercrimes. However, the study also finds that individuals who have higher usage of knowledge-sharing through social media (e.g. LinkedIn, Twitter and Blogger) are more likely to become victims of cybercrime. These findings could be explained through the psychology of human behavior since the public mindfulness of the inherent risk associated with dominant social media sites may cause them to take additional precautions compared to the perceived level of trust and safety associated with knowledge-sharing social media sites where they may take less precautionary or safety measures. Furthermore, Saridakis et al. (2016) show that higher computer skills and greater technological efficacy is positively but statistically insignificantly related to victimisation. The researchers argue that the positive relationship could be due to the individual perception of their superior computer skills resulting in an increased risk-taking behaviour that exposes them to higher probabilities of victimisation. This finding is consistent with Gottfredson and Hirschi’s GTC since this can be viewed as a preference for risk-taking behaviour, which is an element of low self-control, therefore this characteristic increases the individual likelihood of being victimised.

CONCLUSIONS

There are several theories outlined in this chapter, which include, the RAT, the GTC, the DPT and the RCT, all of which attempt to address the phenomenon of human behaviour that leads us to commit an act of crime. The desired approach to crime should not be merely to catch the offenders of crime but to prevent the occurrence of a crime by addressing and removing the stimuli that encourage or allow it to happen. All these theories of crime have been modified and extended to include the new age of cyber-crime especially in the financial sector and among all individuals using social networking sites.

To gain better insights in addressing evolving challenges of the digital world, cybersecurity increasingly relies on advances in research done on human behaviour. Whilst technology may often form the core of cyber-attacks, these incidents are instigated by and responded to by people. Researchers believe that social networking sites are important tools that promote social exchange since social interaction plays a vital role in education (Vollum, 2014, as cited in Benson, 2015c). Therefore, strategies should be developed to allow the continued use of social networking sites without the fear of cyberattacks and thus creating a safe-space in cyberspace to promote social interactions. Researchers also need to address the issue of privacy since privacy on social networking sites is not only an individual issue but also an organizational and institutional one that involves data sharing actors (Benson et al., 2015a). The number of registered social network users and the amount of time spent on social network increase every year. In addition, the commercial value of personal information on social networking sites is on the rise (Benson et al., 2015a) having a tangible contribution to the digital economy. Therefore, with this growing rate of technology and increased dependence on the internet for social networking sites and other essential functions, our risk of losses due to cybercrime is continuously increasing.

Strategies to be used in the protection against cyberattacks can be intelligently developed and delivered by the government awareness programmes, public places and on television to raise awareness of cybercrime. For example, a study by Marcum et al. (2010) suggests that youths lower their probability of online victimisation by communicating only with people whom they know on social networking sites, and not giving personal information to people that they do not know. Furthermore, by gaining a better understanding of the human aspect of cybercrime through psychology, we can develop better mitigation strategies for cybercrimes. This area of human element exploration has a big impact on the future of computing. As such, the younger generation is driving the commercialisation of social media platforms. Therefore, gaining a better understanding of their behavioural traits, intentions and acquisition of safe usage patterns are imperative for the prevention of criminal exploitation of the young user of social networking sites.

RESEARCH QUESTIONS OPEN FOR FURTHER DISCUSSION

This chapter ends with a series of questions warranting future research to explore. These include:

- Should strategies be adopted based on the target age group, as different age groups have different online skills and use the internet for different purposes?
- Do geographical location, technological literacy and culture play a role in determining the types of cybercrime activities?
- Does the risk of losses due to cybercrime activities outweigh the efficiency benefit of implementing the emergent digital technology offerings?
- Can a connection between suicide incidents, mental-illness, cyber-bullying or identity theft cases be established by researchers?
- Governments have placed significant emphasis on privacy regulation. Should they continue to regulate the privacy controls of social networking sites or leave it up to the owners of the social networking sites to prioritise data comercialisation over individual privacy?

This is the time when academic attention is so valued, having the potential to mitigate future cyberattacks, as well as minimise their impact on individuals who are yet to realise their full potential in business and enter the workforce. In order to take control of online victimisation, the relevant stakeholders, including policy makers and

SNS vendors, need to have sufficient control and public awareness to support a safer online future for the younger generation.

KEY TERMS AND DEFINITIONS

Cyberattack: A cyberattack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation.

Cybercrime: A cybercrime is any criminal activity that involves a computer a networked device or a network.

Cyber security: Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

Cyber-victimisation: Cyber-victimisation refers to the process in which others are victimised through the use of information and communication technologies.

Cyber security skills: Cyber security skills are those skills associated with ensuring the security of information technology (IT-generally referring to information storage and integrity) and operational technology (OT-referring to systems that control physical devices).

Risky online behaviour: A risky online behaviour is an action that can potentially leave one exposed to a variety of dangers, putting individual and possibly organisational internet security at risk.

Social network: A social network is an online communication platform that is used for creating relationships with other people who share an interest, background or real relationship.

REFERENCES

Benson, V. (2017). *The State of Global Cyber Security: Highlights and Key Findings*. LT Inc, London, UK DOI: 10.13140/RG.2.2.22825.49761

Benson, V., Saridakis, G. and Tennakoon, H. (2015a). Information disclosure of social media users: does control over personal information, user awareness and security notices matter? *Information Technology & People*, 28(3):426-441.

Benson, V., Saridakis, G., Tennakoon, H. and Ezingeard, J.N. (2015b). The role of security notices and online consumer behaviour: an empirical study of social networking users. *International Journal of Human-Computer Studies*, 80:36-44.

Benson, V., Saridakis, G. and Tennakoon, H. (2015c). Purpose of social networking use and victimisation: are there any differences between university students and those not in HE? *Computers in Human Behavior*, 51(B):867-872.

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

Culnan, M. J., McHugh, P. J. and Zubillaga, J. I. (2010). How Large U.S. Companies Can Use Twitter and Other Social Media to Gain Business Value, *MIS Quarterly Executive*, 9(4): 243-259.

Eck, J. E. and Clarke, R. V. (2003). Classifying Common Police Problems: A Routine Activity Approach, *Crime Prevention Studies*, 16:7-39.

Gottfredson, M. R. and Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Hansen, J., Saridakis, G. and Benson, V. (2017). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior*, 80:197-206.

Hill, M.S. and Duncan, G.J. (1987). Parental family income and the socioeconomic attainment of children, *Social Science Research*, 16(1):39-73.

Holt, T. J. and Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1):20- 40.

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

Marcum, C. D., Higgins, G. E. and M L. Ricketts. (2010). Potential Factors of Online Victimisation of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior*, 31(5):381-410.

McAffee (2018). Executive Summary: The Economic Impact of Cybercrime-No Slowing Down. McAffee Research 2018. Available at: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

McAlaney, J., Frumkin, L., and Benson, V. (2018). *Psychological and Behavioral Examinations in Cyber Security*. IGI Global, Hershey, PA; USA pp. 334.

McLanahan, S. (1985). Family structure and the reproduction of poverty, *American Journal of Sociology*, 90(4):873-901.

Mesch, G.S. (2009). Parental mediation, online activities, and cyberbullying. *Cyber Psychol. Behav.* 12(4):387-393.

Pew Research (2015). The Demographics of Social Media Users. Internet & Technology. August 2015. Available online at: http://www.pewinternet.org/2015/08/19/the-demographics-of-social-media-users/

Piquero, A. R., Macdonald, J., Dobrin, A., Daigle, L.E. and Cullen, F.T.. (2005). Self-Control, Violent Offending, and Homicide Victimisation: Assessing the General Theory of Crime. *Journal of Quantitative Criminology*, 21(1):55-71.

Pratt, T. C., Holtfreter, K. and 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.

Reyns, B., Henson, B., and Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimisation. *Criminal Justice and Behavior*, 38(11): 1149-1169.

Saridakis, G., Benson, V., Ezingeard, J.-N. and Tennakoon, H. (2016) Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users. *Technological Forecasting and Social Change*, 102:320-330

Schreck, C. J. (1999). Criminal victimisation and low self-control: an extension and test of a general theory of crime. *Justice Quarterly*, 16: 633-654.

Seigel, L., J. (2006). Criminology, 10th Edition. University of Massachusetts, Lowell. Thomson Wadsworth.

Statista (2018). Global digital population as of October 2018 (in millions). Demographics & Use. Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/

Taylor, R. W., Fritsch, E. J., Liederbach, J. and Holt, T. J. (2010). *Digital crime and digital terrorism* (2nd ed.). Upper Saddle River: Pearson Prentice Hall.

Tennakoon, H., Saridakis, G. and Mohammed, A-M. (2018). Child Online Safety and Parental Intervention: A Study of Sri Lankan Internet Users. *Information Technology & People*, 31:770-790.

Williams, Matthew L. (2015). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology*, 56:21-48.