Critical Analysis of Strategies Towards Creating an Adequate Level of Awareness on Cybercrime among the Youth in Gauteng Province

Mmabatho P. Aphane[1,*] and Jacob T. Mofokeng[2]

[1]Department of Police Practice, School of Criminal Justice, University of South Africa, South Africa

[2]Department of Safety and Security Management, Faculty of Humanities, Tshwane University of Technology, South Africa

Abstract: This study aims to determine any measures taken by the South African Police Service (SAPS) to create awareness about cybercrime among the youth in the selected policing areas in the Gauteng province. A qualitative research method was applied using semi-structured interviews to find the views of participants, of measures if any, to create youths' awareness in the area of cybercrime. A total of 37 participants comprised of 29 youths aged between 19 and 35 years, including an additional eight participants from the SAPS Crime Intelligence Unit who agreed to participate. Among these participants, there were 18 females and 19 males. The findings highlighted that there was a lack of awareness on the measures taken by the SAPS in educating the youth about the risks associated with cybercrime. The other challenges highlighted by the SAPS were a lack of capacity, resources, and training to increase the technical skills amongst the SAPS members to work effectively on cybercrime-related challenges, lack of collaboration among role players to respond adequately to cybercrime, and ineffective implementation of cybercrime policies, therefore, there was a lack of cybercrime-related campaigns. Based on the findings, five themes were explored in this study, including a lack of capacity, resources, and training to increase the technical skills amongst the SAPS members to work effectively on cybercrime-related challenges, lack of collaboration among role players to respond adequately to cybercrime and ineffective implementation of cybercrime policies. The recommendations are provided as a potential step towards tailoring education packages and awareness programs to ensure at-risk groups are equipped with actionable mechanisms to protect themselves against cybercrimes.

Keywords: Awareness, cybercrime, cybersecurity, police, youth.

INTRODUCTION

Research indicates that the Internet and rapid deployment of information and communication technologies (ICT) in recent years have compromised historic trends and practices in controlling secure cyberspace (Kritzinger and von Solms 2010, 840; Kortjan and von Solms 2014, 29; Riem 2001, 12). Cyber-attacks are increasing in quantity and Internet advancement has become a socio-technical system of systems (Laplante, Michael and Voas 2009, 63). All aspects of human life are more or less dependent on the Internet. Not only do businesses depend on the Internet for all types of electronic transactions, but more and more home users are also experiencing the immense benefit of the Internet (De Joode 2011, 16; De Lange and von Solms 2011, 14). However, this dependence and use of the Internet brings new and dangerous risks (Fritzvold 2017, 71). Through the use of the Internet, cyberspace is growing at an unprecedented speed.

Although there are numerous benefits that the Internet brings, it also provides opportunities for criminals to commit new crimes and to carry out old crimes in new ways. Although cyber-attack can be defined, there is no generally accepted definition for cybercrime (Ismailova and Muhametjanova 2016, 32). According to the United Nations Office on Drugs and Crime (UNODC) (2013, 2), definitions of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity, and availability of computer data or systems represents the core of cybercrime. Certain definitions are required for the core of cybercrime acts. However, a definition of cybercrime is not as relevant for other purposes, such as defining the scope of specialised investigative and international cooperation powers, which are better to focus on electronic evidence for any crime, rather than a broad, artificial cybercrime construct. However, in general, any crime conducted via the Internet or other computer networks can be classified as a cybercrime (Ismailova and Muhametjanova 2016, 32). Currently, due to developments in IT, many crimes have digital traces. Computerised crime has evolved slowly, so there has been time for the development of countermeasures as well. Illegal activities held over cyberspace are relatively new forms of crime (Ismailova and Muhametjanova 2016, 32).

*Address correspondence to this author at the Department of Police Practice, School of Criminal Justice, University of South Africa, South Africa; Tel: 076 297 9292; Fax: 0866 055 600; E-mail: ampaphane@gmail.com

E-ISSN: 1929-4409/20

While the growth of cybercrime in developing countries is generally phased with the development of IT, in South Africa, as well as in many other countries with similar backgrounds, it suddenly appeared. There were 36.54 million Internet users in South Africa in January 2020. The number of Internet users in South Africa has increased by 1.1 million (+3.1%) between 2019 and 2020. Internet penetration in South Africa stood at 62 percent in January 2020 (Kemp 2020). According to Kemp (2020), there were 22 million social media users in South Africa in January 2020. The number of social media users in South Africa increased by 3.5 million (+19 %) between April 2019 and January 2020. Social media penetration in South Africa stood at 37 percent in January 2020. Despite the high Internet penetration rate in South Africa, youths, especially students in higher education institutions, use the Internet frequently.

However, Internet users are not ready for crimes that are brought about by global networks. Strategies to create adequate levels of awareness on cybercrime among the youths in Gauteng province have never been taken. This increases the risk of becoming a victim for youths in Gauteng province, since most websites are in use, making it important to improve the information security awareness rate among Internet users. This study aims to investigate the views of participants, of any measures used to create youth awareness in the area of cybercrime.

LITERATURE REVIEW

Cybersecurity Awareness

According to South Africa Cyber-Security Academic Alliance (SACSAA) (2014, np), the rising number of youth and teenagers are either engaging in cybercrime or becoming victims due to a lack of awareness regarding the dangers or risks associated with the use of the Internet. The inherent linkage of cyberspace exposes all of its constituents to a failure of their most vulnerable elements. Effective cybersecurity cannot be reached by technological measures alone as modern cyber-attacks could bypass all defence layers by exploiting the human factors through techniques such as social engineering. For this article, awareness among the youths refers to ongoing and planned measures, which may potentially be of an educational, behavioural, or disseminative nature. Cybersecurity awareness and education are central to any attempt to secure cyber space. Since cybersecurity is a global issue, every country must have a clearly defined plan for instilling cybersecurity knowledge in all sections of society (Kortjan and von Solms 2013, 289; Dlamini and Modise 2013, 1). As in many other educational domains, the most evident place to begin helping the youth to protect themselves against cybercrime is in the schools (Dlamini and Modise 2013, 1). Furthermore, because cybercrime is a criminal act, some of the strongest lines of defence against it are the police departments and law enforcement agencies.

Cybersecurity awareness is an enabler for increasing cybersecurity defence and capabilities (SACSAA 2014; De Lange and von Solms, 2011, 14). Fritzvold (2017, 71) concurs that alert security culture is an important preventative measure and can mitigate cyber risk. Lack of security awareness is ranked as the number one factor that prevents defence against cyber threats. An effective way of reducing risk is to have continuous efforts to raise awareness, motivate, and increase the understanding of security and risk. Education, learning, and simulation will ensure knowledge of how to respond, what to look for and why is it important. Cyberspace, cyber awareness, and cybersecurity play an important role in the online experience of individuals and need to be addressed accordingly. The Internet and the cyber world are a dangerous place where innocent users can inadvertently fall prey to the sly cybercriminals.

Cybersecurity awareness is the first line of defence against cyber-attacks. The understanding and awareness of digital vulnerabilities and cyber risk exposure is important to reduce risk in this digital transformation. Cybersecurity awareness and education are central to any attempt to secure cyberspace. In the education system, youth must be made aware of the possible attacks and types of intruders. The United Nations (UN) (2014, 5) asserts that most individuals are unaware of the incidents and the impact of cybercrime. These individuals are unaware of the extent to which their lives, financial status, businesses, families, or privacy might be affected by these crimes. Nor are they aware of how quickly the threat is growing. The rapid growth in the use of cyberspace is not matched by the necessary skills. Therefore, there is a need for broad-based education initiatives on Internet safety and security to tackle the issues of child protection and social security in general.

Social media plays a huge role in cybersecurity and contributes a lot to personal cyber threats. It allows people to be brutally honest and open about personal issues that they might fear discussing in face-to-face encounters. Social media is a transit place for most people, including offenders; people do not live in cyber space-they visit and exit as they do in any other place. The majority of people use social media or social networking sites every day and it has become a huge platform for cybercriminals for hacking private information and stealing valuable data. Individuals are easily attracted to social media and hackers use them as bait to get the information and the data they require. Not only individuals are attracted to social media, other organisations and businesses use social media to advertise the products or services they offer (Reddy and Reddy, 2014, np). According to Norton Cyber Security Insights Reports (2016, np), social media remains a favoured target of scammers as criminals seek to leverage the trust people have in their social circles to spread scams, fake links, and phishing. These dangers, combined with a population that has not had regular and sustained exposure to technology and broadband Internet access, expose community members to cyber threats (Grobler, Jansen van Vuuren and Zaaiman 2011, 113).

Additionally, there are currently no structures in place that parents can refer to when they become aware of cyberbullying. Low parental supervision and monitoring of Internet use is also an issue internationally. A lack of awareness among adults means that they are unable to take precautions on behalf of their children, who are also largely unaware of the risks in electronic media (Näsi, Oksanen, Keipi, and Räsänen, 2015, 203). This results in a lack of parental control due to inadequate education about online safety and prevents children from taking charge of their safety. Awareness campaigns and safety programs are therefore important to make both youths and adults aware of the potential threats and how to minimise them. Rather than prohibiting the use of electronic media or merely supervising their use, adults need to work towards empowering youth in their use of such technology so that they can take precautions and keep themselves safe online.

Reporting of Cybercrime Incidents

While waiting for the establishment of a dedicated cybercrime capacity and reporting mechanism in the South African Police Service (SAPS), any report of suspected cybercrime activities to the SAPS must be handled in the same manner as any other crime reported to the SAPS. The members receiving the report must assess, upon receipt of all relevant information, whether the incident constitutes a cybercrime incident. If the incident constitutes a cybercrime offence, the members must register a case docket on the Criminal Administration System (CAS) or Investigation Case Docket Management System (ICDMS). All cybercrime incidents registered on the CAS or ICDMS must be reported to the Section Head: Electronic Crime Unit, the Directorate for Priority Crime Investigation (DPCI), and the Head of Specific Crime Investigations, Detective Service. The CAS or ICDMS does not allow for the reporting of cybercrime incidents *per se*. Due to the pending enactment of the legislation, cybercrime incidents have to be reported as traditional crime types.

If the members receiving the report on an alleged cybercrime incident are not convinced that a criminal offense has been committed, he or she must obtain guidance from one of the officers in the DPCI Head Office. An investigation Diary (SAPS 5) entry or Occurrence Book (OB) entry must be made in respect of the name and rank of the DPCI, Crime Intelligence, or Detective Service official with whom the members speak and the recommendations of such official. If it appears, after the consultation with the DPCI, Crime Intelligence or Detective Service official, that no offense is committed or that the offense is committed outside the jurisdiction of South African courts, the person reporting the incident must be assisted with general advice contained in informative material compiled by SAPS Corporate Communications in conjunction with the DPCI, Detective Service and Crime Intelligence. If a reported incident does not fall within the ambit of offences listed in this policy, certain minimum information must be obtained from the report, namely:

- personal particulars of the victim;
- date and time of the incident;
- short description of the incident (*modus operandi*); and
- contact details of the suspect.

Where no cybercrime incident has been committed but the person reporting the incident is subjected to harassment, he or she may still apply for a protection order from a magistrate's court that has jurisdiction. A protection order can only be issued against a respondent who is located in the Republic of South Africa. Cybercrime awareness and information sharing of the latest trends and threats must be regularly communicated, in conjunction with the SAPS Corporate Communications.

Lack of Cybersecurity Technical Skills

There is a shortage of law officers trained in the technical aspects of the cybercriminal world and forensic experts in cybercrimes. The lack of qualified professionals to investigate cybercrimes will continue to benefit the criminals. Law enforcement involved in undercover investigations need more time to build relationships with the small circles of criminals involved in the cybercrime, (Chak 2015, 21).

Whatever the level of involvement in cyber investigations, an agency is obligated to collect evidence lawfully and competently. Evidence of traditional crimes as well as cybercrimes is frequently found on computers. Officers who are involved in virtually any investigation could face the risk of destroying evidence by either illegally seizing it or causing it to be physically destroyed because of the traps laid by the suspect (Finnie, Petee and Jarvis, 2012, 102).

Even though the prevalence of cybercrime has increased rapidly and cybercrime has become part of everyday life, a major problem remains that victims of cybercrime are far less likely to report their victimisation to the police than victims of traditional crime (Leukfeldt 2017, 47). It is of great importance that victims report these crimes to the police, not only because it is necessary for starting a criminal investigation but it also increases the knowledge of the number and types of crimes that are committed. Clark and Diliberto (1996, 1) state that most cybercrimes are not reported because of the lack of confidence in the ability of law enforcement to investigate. Most law enforcement agencies lack experienced investigators with technical computer experience. Many investigators are considered to be experts by their departments because they can use MS Word and get around Windows. This type of experience is of more help to the criminal than to the public and gives the criminal a huge advantage over law enforcement. Due to the sophisticated methods used to commit cybercrime, the implementation and investigation of cybercrime have become more demanding and time-consuming (Bernik 2014, np). For the police to investigate and punish acts of crime successfully, it is necessary to know and understand the operation of the perpetrators. Casey (2011, 31) argues that the dynamic and distributed nature of networks makes it difficult to find and collect all relevant digital evidence. Although there is no way to guarantee the prevention of cybercrime, there is much hope in raising awareness. As today's children mature, our society will become more attentive to the hazards of cybercrime as well as the skills needed to help prevent it.

Explaining Cybercrime using Criminological Theory

Criminological theoretical frameworks view hacking as a criminal act, exploring the how who and why of cybercrime, as is the case with other forms of criminal behaviour. According to UNODC (2013, 8), within cyberspace, people may show the differences between their conforming (legal) and non-conforming (illegal) behaviour as compared with their behaviour in the physical world. Identity flexibility, dissociative anonymity, and a lack of deterrence factors may provide incentives for criminal behaviour in cyberspace. Crime among the youths is often accidental or unpredictable rather than being planned or anticipated by those committing it. Brewer, Cale, Goldsmith, and Holt (2018, 117) argue that even before the arrival of the Internet, psychologists viewed adolescence as a period of enormous biological, psychological, and social change. During puberty, adolescents experience rapid growth, expand their social skills and circles, and mature sexually. The increase in the exposure of the young adults in particular age towards electronics and technology has increased the information flow, but along with it, has increased the grounds where online stalking and sexual harassment, cyber sexting and fraud are very common (Shabnam, Faruk, and Kamruzzaman, 2016, 2). In spite of positive advocacy towards the Internet, internet and technology have become the platform where deviant behaviour has grounds to grow and has made the situation very conducive for cybercrime. Youths are susceptible to outside influences as they become teenagers (Shabnam *et al.* 2016, 2). Pornography is also on the rise in the digital age (Shah, Shukor, Ali, Ghafar, Ahmad, and Yusof, 2018, 323). With smartphones, individuals can watch pornography as well as use it to collect, edit, disseminate, and circulate personal information. The organisation of the Internet and various connectivity points affect the criminogenic nature of cyberspace (Oksanen and Keipi, 2013, 298).

The Internet can facilitate a better, more connected world and yet at the same time produce massive isolation (Jaishankar 2011, 75). Cybercrime, like any other crime in general, may be explained by the conjunction of three factors, namely motivation, opportunity, and the absence of capable guardianship. While motives tend to change, the variety and number of opportunities for cybercrime are growing (Grabosky, 2000, 1). From a criminological perspective, the suggestion that ICT and the increasing use of the Internet create new opportunities for offenders and facilitate the growth of crime is highly plausible (Oksanen and Keipi, 2013, 298). While several different criminological theories are applicable, cybercrime represents a new and distinctive form of crime, creating challenges in predicting developments and in its prevention when reverting to traditional theories of crime. One key proposition is that the emergence of cyberspace creates new phenomena that are notably distinct from the (mere) existence of computer systems themselves and the direct opportunities for crime that computers present. Within the field of criminology, several theories that exist attempt to explain why some people engage in deviant behaviour, while others abstain from it. Although these theories are originally meant to explain crimes committed in the real world, they can still be applied to cybercrime.

Cybercrime Victimisation through the Prism of Lifestyle/Routine Activity Theory (LRAT)

The originators of lifestyle/routine activity theory (LRAT) (Cohen and Felson, 1979, 588) point out that crime as a non-accidental phenomenon in society is dependent on three components: First, a motivated offender must exist for the victimisation to occur. Secondly, the presence of a suitable target is necessary for the occurrence of the victimisation. Thirdly, the absence of a capable guardian makes easy access for offenders to victimise the target. Combining these elements increases the likelihood of criminal or deviant activity and increases the likelihood of victimisation (Yar, 2005). Thus, the absence of one of the three components is likely to decrease or eliminate the victimisation occurrence. Lifestyle/routine activities, which create variable opportunity structures for successful predation, always occur in particular locations at particular times and the spatial-temporal accessibility of targets for potential offenders is crucial in determining the possibility and likelihood of an offense being committed (Yar, 2005; Reyns, 2013). Yar (2005) describes this requirement as a barrier between LRAT and cybercrime. The writer contends that problems in the transmission of LRAT to cybercrime are caused by temporal and spatial diversity in cyberspace. However, his findings suggest that with certain modifications, the theory can also be applied to cybercrime. Therefore, the first element based on the LRAT is realised due to the nature of visibility and accessibility within the cyber environment. This allows motivated cyber offenders to detect crime targets and commit offenses from anywhere in the world. This is added by the second element − the presence of a suitable target that is necessary for the occurrence of the victimisation. This fulfils the third element, the absence of a capable guardian makes easy access for offenders to victimise the youths. Association with deviant peers and involvement with substance abuse increases the risk of victimisation (Shabnam *et al*. 2016, 5). Now cybercrime is a newly developed crime but the pattern and nature of cybercrime increase day by day which causes so many types of crimes like property crime (credit card fraud. bank deceit, etc) and physical crime such as familiarity via cheat chatting that causes even rape (Shabnam *et al.* 2016, 5). When an online user accesses the Internet, personal information in his or her computer naturally carries valuable information into cyber space that attracts computer criminals. Also, if computer criminals have sufficiently capable computer systems, the inertia of the crime target becomes almost weightless in cyberspace. The nature of visibility and accessibility within the cyber environment allows motivated cyber offenders to detect crime targets and commit offenses from anywhere in the world (Yar, 2005, 407).

METHOD

The problem that was identified in this study is that youth are largely unaware of the prevalence and nature of cybercrime, which increases victimisation and a lackluster approach by the SAPS to identify and respond to victims. A systematic problem of youth victimisation exists due to the lack of current strategies by the SAPS as well as relevant stakeholders to provide adequate cybercrime awareness education. Therefore, it is necessary to implement effective and efficient mechanisms to review and monitor the processes or practices that respond to victims of cybercrime in South Africa. This study used a phenomenological design that was both descriptive and explorative.

Furthermore, the use of a qualitative research approach enabled an in-depth appreciation of the participant responses and a detailed understanding of the form and nature of current strategies regarding cybercrime awareness in the Gauteng province, South Africa.

Study Population and Sampling

Given the sensitive nature of the topic, the authors used a snowball sampling method. Access to participants was a serious challenge, so the writers had to resort to the snowball sampling technique to find the right participants. The authors began with a list of possible participants within the SAPS mandated to work with reported cases of cybercrime and who should provide with the awareness, prevention, and combatting of cybercrime in South Africa, including areas to easily locate the youth in the study area. Once permission to conduct research was obtained from the SAPS Gauteng Provincial Office, the first author contacted the participants and requested access authorisation, as well as permission, to interview the officials. Through this combination of methods, five participants from Crime Intelligence offered themselves voluntarily. Participants from DPCI refused to participate. Of the total participants, the majority were females (n=18) and 12 were males (n=12).

All participants ranged in age from 19 to 59 years old. The data was obtained from the selected participants in response to the drafted interview guide, outlining questions related to the subject under study. This ensured that the elicited data aligned with the study's objective and with the problem statement. The collected data were read several times to grasp the perspectives of the participants, the researchers also took cryptic written notes of statements made during the interviews. All participants of this study participated in a semi-structured interview, which took approximately 45 minutes. All interviews were undertaken with the informed written consent of participants. Confidentiality and anonymity were maintained through the secure storage of data in password-protected computers and under lock and key and by using pseudonyms or generic summarisation of the data. Ethical clearance was obtained from the Tshwane University of Technology (TUT) and permission to conduct this research was obtained from all the participating departments. Data saturation was achieved in terms of the thematic analysis. There are also potential limitations in terms of the generalisability of the findings.

RESULTS AND INTERPRETATION

From the thematic analysis, the following two themes emerged:

- Emerging theme 1: Lack of awareness; and
- Emerging theme 2: Lack of effective strategies.

These themes are discussed below.

Lack of Awareness

For this specific section of data presentation, analysis, and interpretation, the responses were from key informant interviews. The findings reported below were similar among all the selected participants, regardless of the study location. When asked how effective the implementation of cybercrime strategies was by the SAPS targeting the youth in Gauteng province, it emerged that the majority of participants concurred that, first, public awareness was still a challenge, and secondly, the attacks were becoming increasingly sophisticated, which posed a challenge for the SAPS.

Some of the participants said:

> *I don't think it's effective at all, not when it comes to the youth. No. There is nothing in place when it comes to the youth making them aware of cybercrime. At this stage nothing, I think it will only start to happen when the Bill is signed because then SAPS does not have the resources to do actual intervention or awareness but as soon as the Bill is signed off then it's gonna be a priority and SAPS is gonna be instructed to say," listen, here are your resources now your priority is 1,2,3.*" (KII-01:06:01)

> *I think the awareness that comes from the police is a good platform as much as they can do with the capacity that they have and remember that we also take into account the stakeholders. For example, I would say like Samsung and the different cell phone users, they should also create that awareness because there is a market target, remember we are not selling the product to the youths, the youths are purchasing the products from service providers manufacturers so other stakeholders should also play a part in the awareness of cybersecurity. They should also make parents and children aware that we are giving you facility along with the risk factor, then every stakeholder can play an important part so then eventually we all can say collectively that we are making a difference*. (KII-01:03:01).

When asked what impact does the ineffective implementation of cybersecurity awareness have on the youth, the majority of participants said that the youths were subjected to various victimisations including identity theft, cyber bullying and sexting; all of which have social implications for the self-worth and confidence. Youth victimisation history increases risk of involvement with delinquent peers and of subsequent delinquent behaviour. A kind of role modelling effect takes place in the at-risk age of 13–17 years old and when the persons become older than 18 they become either a repeat victimiser or victim. Association with deviant peers and involvement with substance abuse increases the risk of victimisation (Shabnam *et al*., 2016, 5). Some of the participants said:

> *Youth becomes victims of cybercrime due to a lack of awareness and information about cyber-related crime* (KII-01:04:02).

> *Youth fall victims and a lot of cases were not reported as victims and they were not well informed about cybercrime* (KII-01:05:02).

> *They are exposed so they are gonna be exposed, groomed, and abused through our social media, through our Internet, and visiting websites. I don't think there is anything else that we can do because they will just be in danger since they are not properly informed about what is the dangers when it comes to cybercrime. What types of cybercrime are they, we have to go out and inform them what cybercrime is. If you try to buy anything online with your credit card or send money or you start this whole website and you trying to get money. Is it a crime? Is it a crime if you accept money? What types of crimes are they under the category of cybercrime? I don't even think that adults know* (KII-01:06:02).

Lack of Effective Strategies

When asked how effective the current strategies were in dealing with cybercrime, the majority of participants confirmed that the SAPS are still lacking, compared to other law enforcement agencies across the globe, in terms of adequate education targeting the youth to be aware of cybercrime. Some of the participants said:

> *I feel like it is not in the SAPS's interest to educate about cybercrime and cyberbullying, even though at the end of the day it is the SAPS that has to resolve such crimes. I feel like multimedia and digital companies should take a stand when coming to ensure that people are safe when using the Internet* (KII-03:01:04).

> *They are not that effective because there is still a high rate of cybercrimes and a lot of people are still lacking the information* (KII-04:01:04).

> *Current strategies are not effective because people are still being targeted daily* (KII-02:01:04).

The responses above painted a bleak picture and the implications are that the youth will remain victims of cybercrime. These responses corroborate the previous research, which indicates that many parents and teachers do not have the capacity or self-confidence to address cyber risk, with the result that problems such as cyberbullying are a major concern (Kritzinger, 2017, 29). Therefore, the SAPS must realise immediately the urgency of developing effective strategies such as offline resources for delivery into schools and other youth environments by working with relevant stakeholders such as local professionals, including teachers, police, and child protection workers to create awareness of cybercrime and how to increase their protection when surfing the Internet to eliminate victimisation.

Youth, when asked what current strategies on cybercrime, they are aware of that focus on creating awareness regarding cybercrime by SAPS, expressed these views:

> *None of the SAPS that I am aware of* (KII-02:01:03).

> *Not really, I have recently just moved to the City of Johannesburg* (KII-03:01:03).

> *I don't know of any strategy* (KII-04:01:03).

The responses above indicate that the SAPS are ill-equipped to implement cyber crime awareness among the youth. This could be due to the fact that the officials might lack ICT knowledge. There might also be no commitment from the South African government to enhance cyber-safety awareness among the youth, nor are there any strategies that target the youth to educate them about the dangers associated with online surfing. There is a significant need for up-to-date technological tools and equipment for the SAPS to increase awareness among the youths in South Africa. The youths in South Africa, like those from many countries around the world, use the Internet daily. Therefore, the youth are at risk of cybercrime. The SAPS officials cannot prosecute cybercriminals unless the Bill is passed into legislation, as well as creating the adequate capacity to outlaw certain criminal activities, such as cyberbullying. Research indicates that there is a need for resources capable of ensuring that cybercrime can be properly investigated at all levels of law enforcement (Huebner and Bynum, 2016:41). Furthermore, criminal laws regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cybercriminals in different countries.

RECOMMENDATIONS

Based on the findings above, the following are several recommendations given to reduce victimisation among the youths:

Increasing Cybersecurity Awareness in Collaboration with Relevant Stakeholders

It is recommended that the SAPS should mobilise the youths through national advertising campaigns with relevant stakeholders such as professionals, teachers, celebrities, and parents to raise awareness. There should be a concerted effort from the SAPS to target the youth through specific articles in a variety of publications, including gaming, youth magazines, and youth television programs.

Furthermore, it is recommended that the SAPS need to collaborate with other stakeholders from both the government and private sector, to fight cybercrime as they cannot do it alone. Research indicates that it is vital to involve all role players in ICT and cyber-safety awareness, especially schools that provide or have access to ICT devices in the school environment (Kritzinger, 2017, 29). ICTs are becoming part of life in the 21st century, with learners being exposed to devices at school, ranging from cell phones, tablets to computer labs (Department of Basic Education, RSA, 2012,32).

Increasing cyber awareness initiatives among the youths might decrease cybercrime victimisation. The SAPS capabilities dealing with cybercrime should be strengthened for them to effectively fight cybercrime with strategic international partnerships and cooperation. Currently (2020), there are inadequate provisions made in the school curriculum that create awareness relating to cyberspace and its dangers. The SAPS cannot handle cybercrime. *The modus operandi* of cybercriminals, based on the responses, are constantly changing. Therefore, there is a need for adequate training to improve intelligence for the SAPS to combat cybercrime as well as create adequate awareness among the youths. Reporting of cybercrime to the SAPS needs serious consideration and needs to be discussed thoroughly.

Fritzvold (2017, 65) points out that cyber security is important because of the potential damage an attacker can do to a nation, company, or an individual. Sensitive information and data can be lost or fall into the wrong hands. Critical societal functions can be compromised. The dependency on digital systems is increasing along with the increasing cyber-attacks and cyber threats. One should learn how to protect computers and personal information from being hacked and should engage inappropriate online behaviour to eliminate the chances of cyber threats, thereby creating a safer online environment. Business organisations, mainly small and medium, face critical challenges in protecting their data. Due to limited financial and technological resources, it is difficult for them to upgrade security systems and to stay updated with technology. However, better awareness of cybersecurity and proper planning can prove to be very beneficial for such business organisations in protecting their information and trade secrets from being disclosed.

Effective Implementation of Cybercrime Strategies by the SAPS

It is recommended that the criminal justice system, together with other stakeholders, public, private, and NGOs, create national cybersecurity awareness programs to educate all members of society about cybercrime and how to protect themselves while online. SAPS officials have limited ICT knowledge and skills and are ill-equipped to assist the youth regarding the challenges associated with social media. Research indicates that youth represents a vulnerable group of users who spend a lot of time on the web and social networks. They are exposed to the same threats as adults but the effect on them can be more devastating (Curtis and Colwell, 2000, 24). Knowledge is, therefore, very important for the youth to prevent cybercrime (Curtis and Colwell 2000, 24). Chawki (2005, 55) states that educating the youth would help decrease the risk of students in cyberspace. Knowledge helps people to be more aware of cybercrime (Levin, Foster, West, Nicholson, Hermandez, and Cukier: 2008, np).

Proactive strategies and measures are needed to tackle cybercrime and cybersecurity issues in South Africa. It is recommended that the government fund cyber security-related research. Government and its departments should ensure that all networks are secured. South Africa can learn from countries such as the USA on cyber intelligence and cybersecurity measures to predict computer-related threats better and counteract them. Other strategies towards cybercrime involve being proactive, rather than being reactive. The focus should shift from prosecution to prevention as domestic solutions are inadequate because cyberspace does not recognise any geographical boundaries and many computers with access to the Internet can be easily accessed from anywhere in the world. The number of cybercrime victims could be reduced by introducing proper awareness activities such as training programs, sufficient resource for compliance, develop policies and regulations, and sufficient protection of personal information (Choi 2008, 308; Levin *et al.* 2008, np; Chawki 2005, 50).

MANAGEMENT IMPLICATIONS

Based on the findings, the ineffective implementation of cybercrime strategies has demonstrated many paradoxes involved in a complex ecosystem in a cyber-physical society. Lack of technical skills to develop necessary strategies poses a risk for youth to experience victimisation due to a lack of educational awareness campaigns. Ignorance, a limited understanding of what needs to be done, limited awareness of the issue despite its significance and urgency, have resulted in a lack of action, planning, and policies. What makes communication in this area so challenging? Cybersecurity concerns both humans and systems, but the complexity of this interaction goes beyond the understanding of most people, especially youth. Integrated cybersecurity should, therefore, be adopted by the SAPS to target the youth and ensure that they are aware of cyber risks. Deep knowledge of cybersecurity and the types of attacks that are possible are necessary to understand the problem and the SAPS should be at the forefront of empowering the public. This also requires policies to be in place and that people understand what is required.

As highlighted in this study unawareness on the part of users can introduce further vulnerabilities; for example, by using weak passwords, installing untrustworthy software, and using insecure devices and applications. People want to be safe and secure, but may not be aware of the risks involved with the use of the Internet, except those already in the labour market with bank accounts, where the relevant banks warn them about the dangers posed by technology. The public expects that the government to take responsibility, but the measures implemented by governments might not be sufficient if individuals do not also take some responsibility.

CONCLUSION

This article investigated how effective the current cybercrime strategies were, which are employed by the SAPS targeting the youth in Gauteng province and what impact did the cybersecurity awareness have on the youth, to address victimisation among the youths. This research identified several key issues that we're currently lacking about cybercrime awareness and education by the SAPS in the Gauteng province. The findings indicated that the SAPS had not developed adequate and effective strategies yet towards awareness among the youths. Both the key experts as well as the youth concurred that the SAPS is lacking in terms of effective cybercrime awareness and cybersecurity among the youth. It is the view of the authors that cybersecurity education and awareness have become vital necessities for the youth and parents or guardians in South Africa. The Fourth Industrial Revolution highlights the necessity of cyberspace security and this accentuates the need for protecting the youth and parents from cybercrime. It is a fact that the Internet has provided a wide array of learning opportunities, but there are risks too. Photos, videos and other personal information shared by an individual on social networking sites such as Facebook and Twitter can be inappropriately used by others and may lead to serious and even life-threatening incidents. Social networking sites have become the most popular medium for sharing information and connecting with other people. However, these sites have created varied opportunities for cybercrimes, compromised personal identities, and information leakage. Therefore, it is important for individuals to understand how to protect themselves against cyber threats and to comprehend the difference between the virtual and the real world. Seen from within the space transition theory, the researchers argue that the Internet revolution and the advancement of technology in the country have posed unintended risks to the society as evidenced by the increasing number of cybercrimes targeted at youth, such as cyberbullying and identity theft.

LIMITATIONS OF THE STUDY

The sample for the study was selected from three municipalities in Gauteng province, requiring extensive travelling on the researchers' part. In certain instances, only one participant was interviewed per day after the researcher had travelled a long distance (from Pretoria to Boksburg), resulting in travelling to the venue on the following day, depending on the availability of the selected participant. In other instances, the researcher travelled to Johannesburg CBD but youth were not prepared to participate. They all giving reasons that they know nothing about cybercrime and they do not want to be interviewed. Even after granted permission from the SAPS Research office to conduct the study, I was never allowed to interview members of the DPCI. And after agreeing to the interview, some members of the SAPS cancelled with the reason of not knowing cybersecurity and cybercrime.

AUTHOR CONTRIBUTIONS

MP Aphane and JT Mofokeng have reviewed the related kinds of literature, designed and developed the concept of all analyses prepared and written, and edited the manuscript text.

ACKNOWLEDGMENTS

The authors would like to thank Linda Scott for her comments, insightful suggestions, and careful reading of the article.

CONFLICT OF INTEREST

The authors declare no potential conflict of interest regarding the publication of this article. All ethical issues such as consent, misconduct, fabrication of data, plagiarism, or double submission have been completely adhered to.

ABBREVIATIONS

CAS	=	Criminal Administration System
DPCI	=	Directorate of Priority Crime Investigation
ICDMS	=	Investigation Case Docket Management System
ICT	=	Information and Communication Technologies
KII	=	Key Informant Interview
LRAT	=	Lifestyle/Routine Activity Theory
OB	=	Occurrence Book
SACSAA	=	South Africa Cyber-Security Academic Alliance
SAPS	=	South African Police Service
TUT	=	Tshwane University of Technology
UN	=	United Nations
UNODC	=	United Nations Office on Drugs and Crime

HIGHLIGHT

1. The findings of this study highlighted that there was a lack of current strategies in place by the SAPS towards educating the youth about the risks associated with cybercrime. The other challenges highlighted by the SAPS were a lack of capacity, resources, and training to increase the technical skills amongst the SAPS members to work effectively on cybercrime-related challenges, lack of collaboration among role players to respond adequately to cybercrime, and ineffective implementation of cybercrime policies; hence, the lack of cybercrime-related campaigns.

2. Members of the SAPS and youth interviewed clearly explained that there were currently no cybersecurity awareness strategies targeting youth to educate them about the dangers related to cyberspace. The SAPS went even further to explain that the lack of proper legislation makes it impossible to deal with cybercrime. A high-level awareness about information security and cybercrime issues amongst users at home, in government, and educational institutions, especially youth, would decrease the occurrence of cybercrime. The participants mentioned that people, particularly the youth, tend to relax on social media platforms because they lack awareness.

3. There is a lack of trained law enforcement officials to deal with cybercrime. Police officials, magistrates, and judges are not properly trained to arrest, prosecute, and try cybercriminals. Law enforcement agencies are inadequately equipped in terms of personnel, intelligence, and

infrastructure. Therefore, in reported cases, perpetrators may not be found guilty because the evidence given may lack electronic technology. Furthermore, it stands to reason that the SAPS alone cannot stop cybercrime. Based on the above, the SAPS still requires more training when it comes to dealing with cases of cybercrime and raising awareness.

4. There should be a collaboration between the police, the private sector and academia to combat cybercrime.

REFERENCES

Bernik, I. (2014) *Cybercrime and Cyberwarfare*. John Wiley. https://doi.org/10.1002/9781118898604

Brewer, Russell. *et al*. (2018) 'Young People, the Internet, and Emerging Pathways into Criminality: A study of Australian Adolescents', *International Journal of Cyber Criminology*, 12(1), pp. 115-132.

Casey, E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. California: Elsevier Inc.

Chak, S. (2015) *Managing Cybersecurity as a Business Risk for Small and Medium Enterprise*. M.A. Thesis. Maryland: Johns Hopkins University.

Chawki, M. (2005) 'A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy', *ICFALL. Cyberlaw*, 3, pp.1-55.

Choi, K. (2008) 'Computer Crime, Victimization and Integrated Theory: An Empirical Assessment'. *International Journal of Cyber Criminology*, 2(1), pp. 308-333.

Clark, F and Ken D. (1996) *Investigating Computer Crime*. Florida: CRC Press LLC. https://doi.org/10.4324/9780367802035

Cohen, L. and Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach'. *American Sociological Review*, 44, pp. 588-608. https://doi.org/10.2307/2094589

Curtis, P and Colwell L. (2000) *Cyber Crime: The Next Challenge: An Overview of the Challenges Faced by Law Enforcement While Investigating Computer Crimes in the Year 2000 and Beyond*. Available at: https://www.cji.edu/wp-content/uploads/2019/04/cyber_crime_paper.pdf.

De Joode, A. (2011) 'Effective Corporate Security and Cybercrime'. *Network Security*, 9, pp. 16-18. https://doi.org/10.1016/S1353-4858(11)70097-6

De Lange, M and Von Solms R. (2011) The Importance of Raising e-safety Awareness amongst Children. In: *Proceedings of the 13th annual conference on WorldWide Web applications*, 14.

Department of Basic Education, RSA. (2012) *Guidelines on e-Safety in schools: Educating towards responsible, accountable and ethical use of ICT in education*. Available at: https://wcedonline.westerncape.gov.za/circulars/minutes18/CMminutes/del4_18.pdf.

Dlamini, Z and Modise, M. (2013) Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. Case Studies in Information Warfare and Security: For Researchers, Teachers and Students, 1.

Finnie, T., Petee T. and Jarvis, J. (2010) Future Challenges of Cybercrime. In: *Proceedings of the Futures Working Group*. Available at: http://www.foresightfordevelopment.org/sobipro/55/1162-future-challenges-of-cybercrime-volume-5-proceedings-of-the-futures-working-group

Fritzvold, E. (2017) *Cyber Security in Organizations*. M.Sc, Thesis. University of Stavanger. Available at: https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2460083/Fritzvold_Einar.pdf?sequence=1&isAllowed=y.

Grabosky, P. (2000) Computer crime: A criminological Overview. In: *Proceedings of the tenth United Nations Congress on the prevention of crime and the treatment of offenders*. Available at: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/Grabosky2000_UNCongress_ComputerCrimeCategories.pdf.

Grobler, M., Jansen van Vuuren, J. and Zaaiman, J. (2011) *Evaluating cyber Security Awareness in South Africa*. Available at: http://researchspace.csir.co.za/dspace/bitstream/handle/10204/5108/Grobler1_2011.pdf?sequence=1&isAllowed=y.

Huebner, B. and Bynum, T. (2016) *The Handbook of Measurement Issues in Criminology and Criminal Justice.* https://doi.org/10.1002/9781118868799

Ismailova, R and Muhametjanova G. (2016) 'Cyber Crime Risk Awareness in Kyrgyz Republic', Information Security Journal: A Global Perspective, 25(1-3), pp. 32-38. https://doi.org/10.1080/19393555.2015.1132800

Jaishankar, K. (2011) *Cyber criminology: Exploring internet crimes and criminal behavior*. New York: Taylor & Francis Group. https://doi.org/10.1201/b10718

Kemp, S. (2020) *Digital 2020: South Africa*. Available at: https://datareportal.com/reports/digital-2020-south-africa

Kortjan, N. (2013) *A Cyber Security Awareness and Education Framework for South Africa*. M-Tech Dissertation. Nelson Mandela University.

Kortjan, N. and von Solms R. (2014) 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal,* 52, pp. 29-41. https://doi.org/10.18489/sacj.v52i0.201

Kortjan, N. and von Solms R. (2013) 'Cyber Security Education in Developing Countries: A South African Perspective', *In e-Infrastructure and e-Services for Developing Countries*, 289-297. https://doi.org/10.1007/978-3-642-41178-6_30

Kritzinger, E. (2017) 'Growing a Cyber-Safety Culture amongst School Learners in South Africa through Gaming', *South African Computer Journal,* 29(2), pp. 16-35. https://doi.org/10.18489/sacj.v29i2.471

Kritzinger, E. and von Solms S. (2010). 'Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement', *Computers & Security*, 29(8), pp. 840-847. https://doi.org/10.1016/j.cose.2010.08.001

Laplante, P., Michael B and Voas, J. (2009) 'Cyberpandemics: History, Inevitability, Response' *IEEE Security & Privacy*, 7, pp. 63-67. https://doi.org/10.1109/MSP.2009.4

Leukfeldt, R. (2017) *The Human Factor in Cybercrime and Cybersecurity*. Available at: https://www.researchgate.net/publication/317191029_ Research_agenda_The_human_factor_in_cybercrime_and_cybersecurity.

Levin, Avner. *et al*. (2008) *The Next Digital Divide: Online Social Network Privacy. Ryerson University, Ted Rogers School of Management, Privacy and Cyber Institute*. Available at: https://www.ryerson.ca/content/dam/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf.

Näsi, Oksanen *et al*. (2015) 'Cybercrime Victimization among Young People: A Multi-Nation Study', *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16(2), pp. 203-210. https://doi.org/10.1080/14043858.2015.1046640

Norton Cyber Security Insights Reports. (2016) *Understanding Cybercrime and the Consequences of Constant Connectivity*. Available at: https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/2016-Norton-Cyber-Security-Insights-Report.pdf.

Oksanen, A. and Keipi, T. 2013 'Young People as Victims of Crime on the Internet: A Population-based Study in Finland', *Vulnerable Children and Youth Studies*, 8(4), pp. 298-309. https://doi.org/10.1080/17450128.2012.752119

Reddy, G. and Reddy, U. (2014) *A Study of Cyber Security Challenges and its Emerging Trends on latest Technologies.* Available at:___https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies.

Reyns, B. W. (2013) 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses', *Journal of Research in Crime and Delinquency*, 50(2), pp. 218–238. https://doi.org/10.1177/0022427811425539

Riem, A. (2001) 'Cybercrimes of the 21st Century', *Computer Fraud & Security*, 4, pp. 12-15. https://doi.org/10.1016/S1361-3723(01)00417-1

Shabnam, N, Faruk, O. and Kamruzzaman. (2016) 'Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students', *Social Sciences*, 5(1), pp. 1-6. https://doi.org/10.11648/j.ss.20160501.11

Shah, Hendum *et al.* (2018) 'Child Delinquency on the Internet', *International Journal of Engineering & Technology,* 7(3.30), pp. 320-324. https://doi.org/10.14419/ijet.v7i3.30.18270

South Africa Cyber-Security Academic Alliance (SACSAA). (2014) *Welcome to SACSAA*. Available at: http://www.cyberaware. org. za.

United Nations (UN). (2014) *Tackling the Challenges of Cybersecurity in Africa.* Available at: https://www.uneca.org/sites/default/files/Publication Files/ntis_policy_brief_1.pdf.

United Nations Office on Drugs and Crime (UNODC). (2013) *Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private sector.* Available at: https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html.

Yar, M. (2005) 'The Novelty of Cybercrime: An Assessment in light of Routine Activity Theory', *European Society of Criminology,* 2, pp. 407-427. https://doi.org/10.1177/147737080556056

Received on 01-11-2020 Accepted on 01-12-2020 Published on 07-12-2020

DOI: https://doi.org/10.6000/1929-4409.2020.09.159