Global virus lockdown and cybercrime rate trends: a routine activity approach

I Govender1*, B W W Watson2 and J Amra3

1Department of Mathematical Sciences, University of Stellenbosch, Ryneveld Street, Stellenbosch, South Africa.
2Department of Information Science, University of Stellenbosch, Ryneveld Street, Stellenbosch, South Africa.
3PwC, 34 Richefond Circle, Umhlanga Rocks, Durban, 4319, South Africa.

*E-mail: ieg@sun.ac.za

Abstract. Cybercrime perpetuates as a major threat to the reputation and economy of a nation. There is consensus in the media and academic journals alike, that cybercrimes have incremented over the years. During the coronavirus pandemic in the year 2020, a global lockdown imposed by governments forced people to be homebound, leading to a subsequent surge in online users. This resulted in cybersecurity risk hitting close to home, with an upsurge in cybercrimes. This article attempts to make sense of the elevated cybercrime landscape. For the last two decades, criminological research have attempted to explore variants of technology-enabled crime and have examined theories to account for offending. This study proposes ‘Routine Activity Theory’ to explain the magnitude of cybercrimes during this unprecedented period that reshaped people’s routine lifestyles. Routine activity theory predicts that changes in opportunity situations (increase in online users), potentially escalates the convergence of motivated offenders and suitable targets in the absence of capable guardianship. Guardianship (security measures) is pivotal in this theory, to protect the targets (online users) from offenders (cyber threat actors). Furthermore, this paper offers practical security measures, in light of the specified cyber-attacks during this unprecedented period. If this theory is empirically validated, it offers opportunities to mitigate the extent of cybercrimes with an upsurge of online users, and more so for cybercrimes in general.

1. Introduction
There is no doubt in the significant surge attributed to cybercrimes. The last two decades has witnessed substantial scholarship that addresses a myriad of online offenses, including hacking, malicious software, fraud and sexual victimisation [1]. Illicit activities on computers/electronic devices and computer networks have advanced in relation to the growth and advancement of technology [2].
today’s globally interconnected society, communications and online transactions are facilitated by internet technology [3]. Unfortunately, this technology comes with an ever-growing wave of cybercrime that impacts upon society, businesses and governments [4].

Cybercrime is generally used broadly to describe various crimes committed online, which can occur through a myriad of threats such as malware, scams and the like. Cyberattacks have been the cause of major global economic losses [5], impacting not only on financial losses but also bearing reputation damage [6]. Cyber-attacks have brought day-to-day business operations to a standstill, compounded by reputational damage. The reputational loss as a result of cyberattacks on organisations listed in the stock market is estimated to be up to 5% of its stock price [7]. Cybercrime involves a wide variety of criminal and noncriminal abusive behaviours, inside and outside of formal organisations [8]. Digitalisation of products and services has escalated information security to the top of organisational concern [9].

Globalisation and the digital economy have resulted in organisations becoming dependent on the effective use of information systems. Subsequently, securing these systems and the accompanying data has become of significance and necessity.

Cyber-attacks (2020) reports an increase in both, the sophistication and impact of cyberattacks, the world over. The report elaborates that although it’s essential for organisations to safeguard against a plethora of cyberattacks, a threat actor only requires a single weak-link in an organisation’s defences, to infiltrate the organisation. Cyber threats have been identified as the fifth largest threat to growth globally, following over-regulation, uncertainty in policies, the availability of skills and trade conflicts [10]. Organisations are increasingly embracing digitisation and automation resulting in the risk of cybercrime growth. This resulting high risk comes with a price, forecasting that the emerging cybercrime insurance industry could be worth up to 7.5 billion dollars globally by the close of 2020 [10]. The rise in data breach disclosures has prompted an increase in cybersecurity insurance (cyber-insurance) coverage adoption.

The year 2020 will be remembered as a turnaround point in human history, when the world came under attack by the coronavirus. Governments responded by enforcing lockdown regulations, confining citizens to their homes to mitigate the spread of the virus. This unprecedented lifestyle change resulted in a surge of online users, with those able to work from home, turning to remote working. This resulted in cybersecurity risk hitting close to home, with a corresponding increase in cybercrimes. Cybersecurity threats and attacks became faster and more persistently than ever before, especially with the scattered nature of companies and the altered day-to-day operations of nearly every business in the world economy.

This paper examines the current cybercrime landscape and delves into the lockdown period, commonly referred to as the COVID-19 era, in an attempt to make sense of the spike in cyber-attacks. Subsequently, the research question posed is, ‘What has led to the upsurge in cybercrimes during the lockdown period?’ In an attempt to address cyber risks and make informed decisions about cyber security, Choo (2011) argues for clarity in understanding the cyberthreat landscape and look ahead to future offending in the online platform. This article attempts to contribute to a better understanding of the current cyber threat landscape, but more so, in an era of the coronavirus, when globally, people are homebound and their lifestyles are online, for both work time and off time. To this end, this study draws on ‘Routine Activity Theory’ to explain the upsurge in cyberattacks during the lockdown period. Moreover, the article explicates how Routine Activity Theory could enhance cybercrime prevention strategies. The authors who come from both, the IT security corporate sector and academia, facilitated the process of aligning cybercrime from a practitioner perspective with theory, in an attempt to explain causation. Consequently, the article attempts to contribute to both theory and practice in the cybercrime domain.

A narrative review of the literature on cybersecurity breaches from a practitioner perspective is used to summaries key findings from reputable online sources. This article draws from these studies, which were conducted by internationally established entities in the field of IT security. A literature review of the academic databases was explored to identify theories in cybercrime. An attempt was made to align the spike in cyberattacks during the lockdown period with Routine Activity Theory, to propose ex-
planation for the current event. This rest of the paper is as follows. The next section articulates the current global cyber threat landscape. The following section specifies cyber threats/attacks specific to the global lockdown period, or commonly referred to as the COVID-19 pandemic. The next section theorises on the cyber-attacks using Routine Activity Theory. The final section contributes to mitigate against cybercrimes by outlining the recommended security measures.

2. The Cyber Threat Landscape: Overview
A search was conducted through reputable research reports, to gauge the cybercrime landscape. The findings revealed that nation state cyber-attacks and activity mirroring geopolitical conditions were found to be on an increase [10]. Business Email Compromises (BEC’s) focus on compromising email systems to perpetrate fraud. This has become a common attack vector as attackers can easily impersonate individuals once legitimate email accounts or boxes are compromised [11]. Malware, which is a broad term for malicious software was rife. Ransomware attacks, a variant of malware was on the increase, with a growing trend in 2019 towards targeted Ransomware attacks. A notable attack seen during this period was an attack against government systems in the United States, causing the city of New Orleans to declare a state of emergency and various government agencies taken offline, due to cyber-attacks [12]. Other variants of malware currently being used by organized crime syndicates are aimed at bypassing multifactor authentication as financial organizations start shifting to 2 Factor Authentication (2FA) for their customers [12]. In July 2019, a new module added to the Trickbot malware was designed to aid in conducting SIM-swapping attacks. This would allow criminals to port a user’s mobile phone number to one of their devices thereby assisting them with compromising voice and SMS information used for 2FA. Trusted third parties have also provided an attack vector, allowing attackers to leverage them in order to reach other organisations [12]. The supply chain became increasingly targeted which includes: trusted software providers; partner organisations and organisations providing support, for example, application or IT support. Their objective is to infiltrate customers of these organisations who are the actual targets of attack [13].

3. The Cyber Threat Landscape: Routine Activity
The global lockdown period in the year 2020 due to the coronavirus pandemic brought drastic changes to peoples’ routine lifestyle, confining them to their homes, resulting in an online lifestyle, for both work and social activities. This change in routine activity brought about significant changes in the cyberthreat landscape, where threat actors exploited the abnormal situation caused by the coronavirus pandemic [13]. Consequently, this global coronavirus lockdown era, brought about a spike in cybercrime.

Interpol (2020) cautioned against three key cyberattacks i.e. malicious domains, malware and ransomware. There was a vast number of registered domains on the Internet that contain the terms: "coronavirus", "corona-virus", "covid19" and "covid-19". Cybercriminals created a huge number of new sites daily to carry out spam/phishing/malware campaigns, [13]. Threat actors were using COVID-19 phishing lures as early as January 2020 of the pandemic, while the crisis was still in its infancy. Cybercriminals exploited the widespread global communication interactions on the coronavirus to cover up nefarious intentions. Malware, spyware and Trojans were found immersed in interactive coronavirus maps and websites, with spam emails becoming widespread; tricking users to click links that download malware to their computers and mobile devices [14]. There was a surge in hospitals and associated medical centres targeted by cybercriminals for ransomware attacks. Considering that these organisations are overwhelmed by the COVID-19 crisis and cannot afford to be denied access to their computer networks, the offenders suspected that they would likely to pay the ransom [14].

The COVID-19 outbreak caused an escalation in both, likelihood and impact of cyber-attacks [15]. PwC’s (2020) whitepaper outlines how COVID-19 initiated new opportunities for cyber threat actors and further goes to recommend guidelines for organisations to mitigate these risks [15]. The COVID-19 pandemic necessitated organisations to rapidly move to remote working, which was expected to significantly impact on organisational cyber-defences. The security controls already in place, could not
be rapidly applied to new systems or tools to suddenly support employees working remotely. Furthermore, standard procedures and good practices may be deficient or unavailable [15].

3.1. Nation State Attacks
In the resulting global pandemic situation, nation state attacks perpetuated. The FBI and the ‘Cybersecurity and Infrastructure Security Agency (CISA) forewarned organisations in the health and research sectors working on COVID-19 responses to be prepared for threat actors against network compromises from the People’s Republic of China [16]. Furthermore, government agencies and organisations were cautioned to be vigilant against further attacks. A further attack vector arising from the pandemic is potentially one where organisations who are typically not in the health sector but are assisting with the manufacture of essential items for healthcare or equipment, are targeted [16].

3.2. Cybercriminals
Government security agencies across the world cautioned that exploits being utilised by cybercriminals pivots around the pandemic and an increase in remote working practices by many organisations, using malware, especially ransomware [16]. These opportunistic cyber attackers exploited the pandemic scenario to socially engineer lures, which enticed users to download or open the content. Various forms of phishing were found, including impersonating the World Health Organisation (WHO) officials. Furthermore, registering of new domains themed to the current pandemic, with the expectation that these will be used to lure users in order to disseminate malware [16].

3.3. Remote working and related infrastructure
The rapid changes to working practices by organisations during the pandemic required a shift to remote working within a very short space of time. Whilst some organisations were ready for this migration, others had to deploy new IT infrastructure. The USA Department of Homeland Security discovered Exploiting vulnerabilities on VPN infrastructure and attempts of exploits of Virtual meeting platforms (Zoom and Microsoft Teams) [16].

4. Routine Activity Theory
Routine Activity Theory (RAT) is an established theory that has been used to analyse diverse types of criminal behaviour [1]. It was a key theoretical approach in criminology in the late 1970s, to predict street crimes, followed by crimes in general and has since been adapted from terrestrial crimes, to the cybercrime fit [2]. A point of view in criminology is that it’s a case of familiar criminal activities pursued with some new tools and techniques or in Peter Grabosky’s metaphor, it’s basically a case of ‘old wine in new bottles’[17]. According to the originators of RAT [18], three integral components need to converge, in order for a crime to occur: a suitable target, the absence of a capable guardian, and a likely or motivated offender (Figure 1). Moreover, they assert that crime is not a random occurrence, but rather, follows a regularity of patterns that require these 3 components.

RAT explicates that the degree to which one is a suitable target for a motivated offender, largely explains victimisation. A suitable target refers to a person’s availability as a victim, inclusive of the person’s attractiveness to the offender [18]. Guardianship refers to the ability of persons and objects to limit a crime from taking place and can take two forms: i.e. social and physical [18]. Finally, a motivated offender refers to persons who are willing to commit a crime when opportunity presents itself through the presence/absence of the previous two components [19]. To this end, RAT explains that if a motivated offender converges with a suitable target that is not safely guarded against victimisation, a criminality will likely arise [19]. RAT can be viewed as a situational crime theory i.e. a criminal-friendly situation/setting where offenders choose to commit crime based on their perceptions of available opportunities.
This paper weighs in on Routine Activity Theory to the backdrop of the current change in people’s routine activities, to that of an upsurge in online users, in attempting to explain the corresponding surge in cyber-attacks. In the context of the current situation where people are homebound, spending time online more than ever before, is a motive for cybercrime offenders. Aligned to this theory, the ‘motivated offender’ represents the threat actors exploiting the current opportunistic situation with more online users as the ‘suitable targets’, and the ‘guardian’, referring to security measures. Cohen and Felson (1979), the originators of routine activity theory, predict that changes in opportunity situations (change in routine vis-à-vis surge in online users), together with an absence of capable guardianship, will increase the convergence in time and space of motivated offenders and suitable targets [18]. Pratt et al. (2010) assert that “this theory assumes a constant supply of motivated offenders, focuses on the behaviours, activities, and situational contexts that place would-be targets at risk for victimization”. Routine activity theorists affirm that the changing organisation of social activities is best placed to account for patterns or trends in criminal activity [20]. In the current situation (global lockdown due to COVID-19), this theory may be of even more relevance, such that more persons are online, including with work related matters, but outside the organisation’s firewall and security controls.

In cybercrime, an assumption is that cyber criminals are (1) criminally/financially motivated who seek out (2) opportunities that cyberspace provides, and (3) target weakly protected systems/networks [21]. Yar (2005) offers an elaborate theoretical review on RAT’s capacity to explain patterns of cybercrime. He delineates each of the key elements of RAT’s schema of the crime-situation (motivated offenders, suitable targets, and absence of capable guardianship); applied in the context of the online environment [20]. It’s a given that there is no shortage of supplies of motivated offenders in cyberspace among hackers, fraudsters, pirates, stalkers. So too, are an abundance of suitable targets for predation on proprietary data, personal information, purchasing services and online transactions [1]. In the context of the global lockdown era, the surge in online users have contributed to “an abundance of suitable targets for predation.”

Over the years, more elements relating to the suitability of the target have been incorporated into the routine activity approach [21], namely as acronyms CRAVED and VIVA. Clarke (1999) identified common attributes of “hot products” or those most frequently targeted by thieves, outlining that they are concealable, removable, available, valuable, enjoyable, and disposable, hence CRAVED [22]. They relate to attributes/characteristics that attract criminals [21]. Research in criminology focused on Internet-related criminal activities (credit card fraud, cyber bullying, identify theft etc), which has contributed to understanding of Internet victimisation, however, more interrogation into offense-specific explanations of targeting has the potential to improve crime prevention endeavours [23].
This theoretical model is not just for the benefit of understanding causal mechanisms underlying fraud targeting and victimisation, but also for improving crime prevention approaches [23]. Regarding internet fraud, routine activity theory has significant implications for crime control policy, in that the potential victims can be educated/trained/made aware about changes to their online behaviour to reduce victimisation. In applying this model to cyberspace, a key target of Internet crime is information [24]. Databases containing personal information (names, addresses, passwords and various banking details) fit the characteristics Clarke (1999) refers to as CRAVED and have become the target for cyber criminals [25].

The ‘target suitability’ can be further unpacked to sub-variables [1]. Yar (2005) argues that the conceptualisation of a suitable target in RAT is itself an aggregate of different components, captured in the acronym VIVA (value, inertia, visibility, and accessibility) [20]. The properties of potential targets across these four components determine how suitable they are for predation. The element value refers to offenders’ goals; that which they target and can be varied, inclusive of information, intellectual property, monetary gain and the like [20]. Inertia is the physical property of the item and refers to how easy is it for the item to be taken [18]. Visibility refers to how visible are the objects to the offender. Online visibility of a victim may contribute to persons being suitable targets for the motivated offender [1]. The four dimensions outlined above can be utilised to explain the intensified cyberattacks in the period of upsurge in online users.

The concept of ‘capable guardians’ in RAT include end-users themselves, together with technical staff (network administrators), as well as automated protections such as firewalls, virtual private networks, anti-virus and anti-intrusion software, and ID authentication and access management systems [1]. Behaviours that are more vulnerable to offenders, such as the duration spent online, increase in Internet banking and online purchases, are often are more likely to be targeted by offenders [2]. According to RAT, the impact of capable guardianship is the most important factor for reducing victimisation [1]. The absence or presence of guardians at the point at which potential offenders and suitable targets converge in time and space is key to determining how likely an offence will occur.

This paper proposes RAT as a theoretical perspective to inform the causal mechanisms that underlie both: cybercrimes in general, and the variants of offense-specific online cybercrimes. Although an understanding of the cyber-attacks on the internet has been explored, more insight into offense-specific explanations of targeting could improve crime prevention. In the study of street crime victimisation, routine activity theory has guided public policy, especially concerning the development of situational crime prevention strategies intended to increase guardianship [24]. Yar (2005) asserts that crime prevention strategies derived in part from RAT, have been proposed as viable responses to Internet crime. As aforementioned, guardianship is an integral component of RAT to mitigate victimisation. Subsequently, the next section advances guardianship as ‘security measures’ in the context of the current situation in lifestyle change.

5. Security Measures in Disruptive Routine Activity
The global coronavirus pandemic has re-shaped societal lifestyle, inclusive of work style, where the work office has become home-based, resulting in people trending online. As outlined in RAT, the presence of guardianship is crucial in mitigating cybercrimes. The standard security measures that organisations should have in place under normal circumstances are critical and provide a baseline level of security for organisations, but may need to be enhanced or customised, in view of the current situation. Given the complexity of cyber security, this paper aims to provide high level considerations at a strategic, information technology level and for general users from a practitioner perspective.

5.1. Strategic Considerations
The global lockdowns regulated by governments resulting in abrupt migration to work from home practices, impacted standard good governance practices implemented in normal work situations. In retrospect, organisations should review areas where standard good practices are inevitably compromised. Moreover, due consideration should be given to freezing non-essential changes where governance processes can’t be followed and re-evaluate how governance processes can be re-designed
to support the new working practices. Furthermore, systems that were deployed just prior to lockdown in order to facilitate working from home should be reviewed to ensure that adequate consideration to security measures were considered.

Oversight, inclusive of the Board, risk, audit and governance committees should be responsive, ensuring that the organisation is taking cognisance of the rapidly changing threat landscape together with the IT security team and translating threat information into tangible controls or monitoring activities where necessary. ISC2’s (2020) snap survey indicated a concerning trend where 47% of IT security staff indicated that they had been re-deployed to assist with IT tasks and 22% of respondents indicated that their organisations lacked resources to support remote working for staff. Organisations should rather consider bolstering IT staff capabilities by drawing on outsourced vendors to ensure that the cyber security function is maintained. It is imperative that the overall COVID-19 crisis team responsible for managing the organisations’ response has adequate representation from the information security team.

5.2. Information Technology Considerations

Cyber Security Incident Response Plans and Playbooks provide all of the organisational members with a clear understanding of their roles and responsibilities regarding responding during cyber event; especially before, during and after a security incident. Incident response procedures need to be re-evaluated, gaps identified and remediated to ensure that the plans are still viable. Playbooks supporting these plans will also need to be tweaked in order to cater for the changing work environment and the resultant threat vectors being exploited by threat actors. In cases where organisations have not developed plans, the use of 3rd party providers should be considered for the immediate future.

Monitoring is key to being able to detect potential attacks. IT should ensure that in addition to having network visibility, potential attacks on endpoints can be detected and contained as quickly as possible. Security teams should also be alerted to the fact that users will probably not work strictly within normal office hours when working remotely.

The IT department should ensure that the business needs of users are catered for when working remotely or else users will start using unapproved applications to fulfil their tasks, which can lead to malicious software being introduced into the environment. Where new applications are deployed to cater for these needs, users should receive adequate training to use these applications securely. Patching and update processes should be re-evaluated to ensure that all end points, remote access systems, security software and critical infrastructure are still being patched. This provides basic security to known threats and should be re-visited to ensure that user devices are still being updated even though they are working remotely. Remote access systems and user authentication systems will be a critical component from an IT perspective. In terms of continuity, IT should ensure that these systems are resilient and plan for having backup platforms in place. Due to the criticality of remote access and authentication mechanisms, they should be further hardened against Distributed Denial Of Service (DDOS) attacks.

Due to staff working remotely, there is an increased risk of insider threats to organisations, especially in cases where employees are being terminated or if there is uncertainty regarding their job security. IT should consider enhancing controls to prevent data loss and the ability to block users logical and physical access to devices, should the need arise. Furthermore, access should be reviewed to be in line with the Principle of Least Privilege (PoLP), i.e. staff members are only granted access to the data required to perform their job functions. Organisations need to have a view of what their trusted business partners are doing, to ensure protection of their own networks and environments; this is key, as given the interconnected business environment vulnerabilities in their security posture, translates into risks for all interconnected parties.

5.3. General User Considerations

Based on all of the attacks discussed in this paper, probably the most critical consideration should be that of user security, education, training and awareness. End users should be made continuously aware of the latest attacks being used by threat actors through a combination of advisories, e-learnings and virtual training sessions. Most of the attacks currently being carried out rely on lures which are socially
engineered, to garner interest from users. User awareness should also be raised around information handling and working in a secure manner as they will no longer be working within the confines of access-controlled workspaces and may inadvertently divulge sensitive information to unauthorised individuals. Users should be trained on virtual working tools and the available security configurations; this is especially required for virtual meeting applications which have become a focus of threat actors. As an example, meetings should be set to only allow specific participants to join and not be open to the public and require passwords. The dangers of sharing screenshots of meeting invites through unsecure communication channels should also be highlighted to staff members. There is also an expectation that there will be a rise in fraud on e-commerce channels, where attackers will focus on first time users of these platforms who will be novice users due to lockdown restrictions. Providers of such services should provide basic security guidelines catering for this category of users. Finally, home users should ensure that basic security measures are maintained in terms of anti-virus and anti-malware software being installed and updated, having basic firewalls in place, not clicking on unknown links or attachments, and not enabling macros on documents being sent from unknown parties.

6. Conclusion
The routine activity approach has been repeatedly proposed as a theory with the potential to be adapted in cyberspace [20]. Guardianship in RAT highlights the ability of ‘objects’ and ‘persons’ to mitigate a crime from occurring. Aligned with ‘objects’, Yar (2005) asserts that RAT’s concept of capable guardianship from the terrestrial world (burglar bars/alarms) is transposable to cyberspace, which already has an abundance of physical and technological guardians, inclusive of automated agents that exercise perpetual vigilance amongst firewalls, intrusion detection systems and the like. The ‘persons’ aspect of guardianship could be viewed as the IT security personnel in organisations responsible for cybersecurity, together with the likely targets expected to comply with security measures when using their devices [19]. Persons who avail themselves for victimisation are those who have not taken the necessary precautions to safeguard themselves. Laws and regulations also play an overarching role in terms of guardianship, however, due to the complexity and extensiveness of this aspect, this study focused on guardianship in the context of security measures that individuals and organisations can implement.

This article brings to the fore, the current cybercrime landscape; more specifically, highlighting the upsurge in cyberattacks during the global lockdown coronavirus era in the year 2020. Routine Activity Theory is proposed as a probable explanation for the rampant cyberattacks during this era, noting its alignment with the spike in cyberattacks in this period. Routine activity theory predicts that changes in opportunity (increase in online users) can increase the convergence of motivated offenders and suitable targets in the absence of capable guardianship. The originators of RAT [18] published this theory in their paper, “Social change and crime rate trends: A routine activity approach”, which informed the deliberate title of this article, “Global Virus Lockdown and Cybercrime Rate Trends: A Routine Activity Approach”. This theory could explain how the motivated offender in this opportune time targets the likely victim who is not observing the necessary security measures, exacerbated by the absence of guardianship. The article concludes with recommending security measures to mitigate the current cyberattacks during this unprecedented period. According to the World Health Organisation, the coronavirus and its global impact is likely to be around for a while, resulting in large parts of the population remaining home-based, spending time online. Furthermore, in general, the number and frequency of online users have increased over the years, inclusive of people working from home. For all of these aforementioned reasons, this article is deemed of relevance, in this day and age.
7. References

[1] Leukfeldt E R and Yar M 2016 Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis Deviant Behavior 37 263–80

[2] Kigerl A 2012 Routine Activity Theory and the Determinants of High Cybercrime Countries Social Science Computer Review 470–86

[3] Bendovschi A 2015 Cyber-Attacks – Trends, Patterns and Security Countermeasures Procedia Economics and Finance 24–39

[4] Interpol 2018 Cyberattacks know no borders and evolve at a rapid pace https://www.interpol.int/CRimes/Cybercrime/COVID-19-cyberthreats

[5] Miller S, Wagner C, Ackelin U and Garibaldi J M 2016 Modelling cyber-security experts’ decision making processes using aggregation operators Computers and Security 62 229–45

[6] Lagazio M, Sherif N and Cushman M 2014 A multi-level approach to understanding the impact of cyber crime on the financial sector Computers and Security 45 58–74

[7] Smith K T, Jones A, Johnson L and Smith L M 2019 Examination of cybercrime and its effects on corporate stock value Journal of Information, Communication and Ethics in Society 17 42–60

[8] Willison R, Warkentin M and Johnston A C 2018 Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives Information Systems Journal 28 266–93

[9] Niemimaa M and Niemimaa E 2019 Abductive innovations in information security policy development: an ethnographic study European Journal of Information Systems 28 566–89

[10] Operations C T 2020 Cyber Threats 2019: A Year in Retrospect https://www.itweb.co.za/content/JBwErvn5wg2q6Db2

[11] EC - Council 2019 MOST COMMON CYBERATTACKS OF 2019 Q4

[12] Winder D 2019 The Top 10 Cybersecurity Stories Of 2019—A Window Onto The 2020 Threatscape https://www.forbes.com/sites/daveywinder/2019/12/27/the-top-10-cybersecurity-stories-of-2019-a-window-onto-the-2020-threatscape/#7d6846087992

[13] PwC 2020 Behaviourally-inspired measures to lower the risk of cyber-attacks in your organisation https://www.pwc.co.za/en/press-room/cyber-attacks.html

[14] Interpol 2020 https://www.interpol.int/CRimes/Cybercrime/COVID-19-cyberthreats?cv=1

[15] PwC 2020 How to manage the impact of COVID-19 on cyber security https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/how-to-manage-the-impact-of-covid-19-on-cyber-security.html

[16] FBI National Press Office 2020 FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations https://www.fbi.gov/news/pressrel/press-releases/fbi-and-cisa-warn-against-chinese-targeting-of-covid-19-research-organizations

[17] Smith R G and Grabosky P N 2001 Online Securities Fraud Journal of Financial Crime

[18] Cohen L E and Felson M 1979 Social Change and Crime Rate Trends: A Routine Activity Approach American Sociological Review 44 588–608

[19] Marcum C D, Higgins G E and Ricketts M L 2010 Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory Deviant Behavior 31 381–410

[20] Yar M 2005 The Novelty of ‘Cybercrime’: An Assessment in Light of Routine Activity Theory European Journal of Criminology 2 407–27

[21] Choo K K 2011 The cyber threat landscape: Challenges and future research directions Computers & Security 719-31.

[22] Jansen J and Leukfeldt R 2016 Phishing and malware attacks on online banking customers in
the Netherlands: A qualitative analysis of factors leading to victimization International Journal of Cyber Criminology

[23] 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 47 267–96

[24] Newman G R and Clarke R V 2013 Superhighway robbery: Preventing e-commerce crime

[25] Clarke R V. 1995 Situational Crime Prevention Crime and Justice 91–150