A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes

Rahayu Ahmad[1,*] and Ramayah Thurasamy[2,3,4,5,6,7,8]

[1] *School of Computing, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia*
[2] *School of Management, Universiti Sains Malaysia, Minden, 11800 Penang, Malaysia*
[3] *Department of Information Technology and Management, Daffodil International University, Dhaka 1341, Bangladesh*
[4] *Faculty of Economics and Business, Universiti Malaysia Sarawak (UNIMAS), 94300, Sarawak, Malaysia*
[5] *Fakulti Ekonomi dan Pengurusan (FEP), Universiti Kebangsaan Malaysia (UKM), 43600 UKM, Bangi Selangor, Malaysia*
[6] *Department of Management, Sunway University Business School (SUBS), 47500 Selangor, Malaysia*
[7] *Faculty of Accounting and Management, Universiti Tunku Abdul Rahman (UTAR), 43000 Cheras, Kajang, Selangor*
[8] *Fakulti Pengurusan dan Perniagaan, Universiti Teknologi Mara (UiTM) 42300 Puncak Alam, Selangor*
E-mail: rahayu@uum.edu.my; ramayah@usm.my
[*] *Corresponding Author*

Received 23 November 2021; Accepted 15 April 2022;
Publication 06 June 2022

Abstract

Cybercrimes are increasing at an alarming rate and cause detrimental effects to the victims. Routine Activity Theory (RAT) is commonly used to understand the factors influencing cybercrime victimization. However, there have

Journal of Cyber Security and Mobility, Vol. 11_3, 405–432.
doi: 10.13052/jcsm2245-1439.1133

been inconsistent findings on the applicability of RAT theory. This study performs a Systematic Literature Review analysis to consolidate and provide a coherent analysis of the related studies employing RAT theory for cybercrime victimization. The articles were also differentiated based on the cybercrimes topologies being investigated; (a) cybercrime dependent (hacking and malware) and (b) cybercrime enabled (phishing, fraud and identity theft). The findings suggest that a refined specification and operationalization of RAT'S construct tailoring to the types of cybercrimes can arguably yield more accurate application and interpretation of RAT Theory in cybercrimes. Consequently, this will address the inaccurate measurement issues of some of the RATS's constructs, leading to inconclusive effects on cybercrime victimization. In addition, there is a need for more longitudinal studies to disentangle the effect of RAT's construct during pre and post cybercrimes. Security advocates can apply the findings of this research to formulate relevant cybercrime awareness programs. The findings also shed some insights into which groups should be targeted for different cybercrime educational and awareness programs. This study can increase the awareness among citizens in terms of their online activities, their attributes and the types of protection from becoming cybercrime victims.

Keywords: Hacking, online fraud, identity theft, cybercrimes.

1 Introduction

The Internet has revolutionised our daily lives. Much of our daily activities such as banking, communication, education, and purchasing are conducted online. Although many people enjoy the convenience of these online activities, there are also some who capitalise on the multiple opportunities to victimise others. As a result, cybercrime cases are continuously increasing every year. According to FBI statistics, in 2019, an average of 1300 cybercrimes was reported, amounting to $3.5 billion in losses to individual and business victims. These cybercrimes suggest that people are the most vulnerable entities to be exploited [1] as human reasoning can be subjugated by external manipulations [2].

In understanding the factors of cybercrime victimisation, one of the most frequently used theories is the Routine Activities Theory (RAT), which was initially developed by Cohen and Felson (1979). The essence of this theory is that when an individual possesses characteristics that attract the offender and is exposed to the motivated offender coupled with lack of protection from the attacker, he or she is likely to be the victim of a crime. Since this theory is initially used to explain physical crime, it is unclear whether it can be applied to online crime [3]. One of the issues plaguing cybercrime research is whether the concepts and constructs in the physical world can be applied and interpreted similarly in a virtual environment [4]. This problem has been partly reflected in the conflicting findings of studies that applied RAT for examining cybercrimes. One cluster of research demonstrates the favourable applicability of RAT in cybercrime victimisation. This group of research demonstrated that online shopping activities increase exposure to motivated offenders [4–6]. Additionally, several individual characteristics such as education [4, 7, 8], income [4, 9], and some behavioural traits such as clicking links [8] are associated with cybercrime victimisation. Furthermore, personal traits such as digital literacy [10] and online risk awareness [4] are considered guardianship factors and are significantly associated with cybercrimes.

Despite these promising findings, another stream of research has posited contradicting findings. In their review, Leukfeldt and Yar (2016) highlighted several studies showing the problematic application of variables in RAT in explaining cybercrime victimisation. In their earlier study, elements of RAT such as online activities and online accessibility did not increase the risk of victimisation (Leukfeldt, 2014). They also demonstrated that target attractiveness factors such as personal and financial characteristics are not significant towards cybercrime victimisation. Leukfeldt (2016) also highlighted the findings of Reyns et al. (2011), which found that online exposure variables in RAT did not consistently affect cyber-stalking victimisation. As for guardianship, which denotes technical, social or behavioral protection, the results were also mixed. While technical guardianship such as having anti-virus installed was initially argued to be significantly related to the risk of victimisation, some studies have refuted this argument [7, 11].

Due to the inconsistencies in findings, it is challenging to conclude RAT's applicability in explaining cybercrime victimisation. Therefore, this study aims to consolidate and provide a coherent analysis of the related studies employing RAT theory for cybercrime victimisation. The outcome of this study will provide a better understanding of the applicability of RAT theory for explaining cybercrime victimisation. In addition, the conflicting findings are partly due to the different nature of various cybercrimes [4]. Hence, for deeper understanding, this study will present the analysis of the applicability of RAT factors based on the typology of cybercrimes; cyber-enabled crime and cyber-dependent crime (Wall, 2007).

In a nutshell, this study presents a systematic review of empirical studies that utilise RAT to examine cybercrime victimisation. Specifically, the objectives of this SLR are:

(a) To analyse the usability of RAT in terms of these three concepts: (1) proximity to offender, (2) target attractiveness, and (3) guardianship.
(b) To compare the findings between cyber-dependent and cyber-enabled crimes studies that utilise RAT theory
(c) To discuss the applicability of RAT theory to cybercrimes and future direction.

2 Types of Cybercrimes

In this section, a brief description of common cybercrimes is presented before discussing cybercrime topologies. Hacking is one of the prevalent cybercrime approaches. Hacking can be defined as the unauthorised access and subsequent use of other people's computer systems with criminal intention. In performing the data gathering, hackers can use either a technological-based or a human-based approach to attack. The technological approach can be deceiving victims through fraudulent pop-up messages informing of some problems that require action or credentials by the potential victim [12]. The hackers can also use malicious software such as viruses and worms to infiltrate the target devices and accounts [13, 14]. Alternatively, the human-based approach can use persuasive messages and exploit human weakness (empathy, charity, love) in face-to-face interaction, communication over the telephone, or indirect interaction through letters, emails and websites, instant messaging, or even unidirectional interaction.

Another common cybercrime approach is phishing, which uses sophisticated lures to obtain valuable information such as credit card numbers, bank account details, and other confidential information from a target [15]. Phishing usually involves establishing a fraudulent website that closely mimics the official website [16]. Emails impersonating the trusted agencies will be sent out to potential victims [17]. These emails usually ask people to "validate" or "confirm" their credentials. To do so, users need to click links or attachments, which direct them to the fake website where the private information of the victims will be elicited [16]. After the targeted data has been retrieved, the user will be redirected to the actual website to prevent suspicion.

Cyberfraud or scamming is a form of deception to gain monetary benefits [12]. In e-commerce, an example of fraud includes the promise of goods or services that are non-existent. Meanwhile, online banking fraud refers to the 'fraudulent act of surreptitiously accessing and transferring funds from an individual's online bank account for financial gain. In some cases, individuals may even be duped by a criminal into making fraudulent money transfer themselves [4]. Finally, identity theft is usually linked to a scam or defamation. It refers to the use of unauthorised personal identification details for illegal purposes [18]. Another type of cybercrime that is excluded from this study is cyber-violence. It refers to harmful actions either through hate speech, cyberbullying, and other related aggression acts.

2.1 Cybercrimes Topology

In this study, it is vital to analyse the applicability of RAT based on relevant cybercrime typologies. The inconsistencies of RAT'S findings may be derived from concluding findings without differentiating the nature of cybercrimes. Cybercrimes arguably have different natures or modus operandi in their attacks. Akdemir & Lawless [19] provided an analysis of cybercrime typologies. According to them, cybercrimes can be classified based on different criteria. From their review, some scholars classify cybercrimes as Type I (technology-based) versus Type II (people-based crimes) [20]. In the former, the crime is usually facilitated by loggers or viruses into the victim's system, while in the latter, the crimes are the consequence of a victim's action or online activities such as clicking on malicious links or entering information on fake websites. Examples of Type I cybercrimes include phishing attempts, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud. Meanwhile, Type II cybercrimes include cyber-stalking and harassment, child predation, extortion, blackmail, and stock market manipulation.

In this study, we adopted Wall's [21] classification to differentiate between cyber-enabled, cyber-dependent, and cyber-related crimes. Cyber-dependent crimes are defined as attacks that can only be facilitated through Internet technologies. Without technology, these crimes are non-existent. For example, malware infection, hacking, and spamming constitute cyber-dependent cybercrimes. Meanwhile, cyber-enabled crimes are considered hybrid cybercrimes resulting from the integration of traditional crimes with Internet technologies. This type of crime can still exist without technologies, but the technologies can amplify the crimes to reach a broader range of victims. Examples of cybercrimes include phishing, online fraud, identity theft, and online pornography.

Meanwhile, cyber-related crimes are content-related offences such as cyber aggression, cyber-obscenity, cyber-violence, and cyberbullying. We adopted the Wall [21] typology for comparative analysis between RAT applicability in cyber-enabled versus cyber dependent crimes. Cyber-related categories are not included in our analysis. The rationale for selecting this typology is to deduce whether different RAT factors influence purely virtual-based crimes (cyber-dependent) versus hybrid types of crime (cyber-enabled).

3 Routine Activities Theory

Routine Activities Theory (RAT) is an extension of the lifestyle exposure theory. The Lifestyle Exposure Theory (LET) posits that some people are more prone to becoming victims of crime than others because of their lifestyle. Hindelang et al. [22] defined lifestyle as "routine daily activities, both vocational activities (work, school, keeping house, etc.) and leisure activities" (p. 241), where he argued that people whose daily routines bring them into contact with potential offenders are more likely to experience personal victimisation. RAT extends LET by having two additional elements; a motivated offender and capable guardianship besides the routine daily activities [23]. The basic premise of RAT is that crime occurs when three things converge in time and space: a motivated offender (through daily activities), a suitable target, and the lack of a capable guardian [24].

Traditionally, RAT is applied to explain physical crimes such as burglary [24], vandalism [25], and physical assault [26]. Recently many studies have adopted this theory to explain cybercrime victimisation. However, applying this theory to cyberspace is challenging since the convergence of spatiality and temporality is ruled out. In cybercrime studies, proximity to a potential offender is sometimes operationalised as the number of friends on social networks and strangers in the friend list [27]. In terms of lifestyle, exposure to victimisation is represented by the duration of time spent on various online activities like using social networking sites and instant messaging [4]. However, as we will explain later, frequency is not a stable predictor of risk victimisation [8]. Therefore, some scholars argue that the duration of time online is not sufficient to explain victimisation. Instead, the activities performed while being online (i.e. sharing location, commenting, active in forums) may be a better construct to explain the risk of victimisation.

Besides proximity, target attractiveness has been associated with the risk of victimisation. Target attractiveness is defined as the appealing characteristics of a person or object to potential offenders. It also describes the inertia of a person or object to be removed as a potential victim [28]. Visibility, inertia, value, and accessibility are the critical elements which constitute target attractiveness [29]. Visibility means a person or an object that is more visible to the offender is more susceptible to victimisation.

Meanwhile, accessibility is described as accessing the target and getting away from the crime scene [30]. In cybercrimes, the Internet is a public medium that allows for fake or anonymous identities, and provides high visibility and accessibility to potential victims [31]. The concept of value represents the worth of a target or objects either for personal pleasure, sales, and other purposes. In cybercrime, the value is usually on informational characteristics such as confidential data or passwords and intellectual properties objects such as music and computer software [31]. Meanwhile, inertia refers to an object or person of any inherent resistance to its removal. For cybercrimes, operationalising the inertia seems problematic as the objects are not tangible. Recently, scholars have argued that the file size can reflect the inertia of informational objects in cyberspace. For example, large data size may take more effort and time for an offender to steal, and needs to have appropriate storage capacity later [31].

Target attractiveness has been measured using several sociodemographic factors. For example, in cybercrimes, age, income, education, race, and residential setting have been used for representing target attractiveness [3, 32–34]. Furthermore, besides social demographics, some behavioural measures are also used to represent target attractiveness. For example, Ngo and Paternoster (2011) operationalised clicking or opening links to indicate target attractiveness. The current measures of target attractiveness, however, do not yield conclusive findings towards cybercrime victimisation.

The third dimension of RAT is guardianship. In cyberspace, guardianship can be classified as the following: technical guardianship, social guardianship, behavioural guardianship, and personal guardianship. Technical guardianship refers to the use of protective software such as firewalls, anti-virus programmes, filtering, and blocking software [35]. Social guardianship can be represented by social circles or people mediation that can dissuade cyber-deviance and potentially reduce the risk of cybercrime victimisation [32]. Behavioural guardianship is usually operationalised as protective actions such as regularly changing passwords. Finally, personal guardianship refers to an individual's attributes that may protect him or her from being victimised. Ngo [8] describes personal guardianship as a certain level of skill with computers and technology. In conclusion, this study will focus on synthesising these three factors of the RAT theory in explaining cyber-enabled and cyber-dependent crimes.

4 Methodology

Scopus and Taylor and Francis were the primary databases used to retrieve all the papers in this study. For papers to be qualified in the dataset, they need to contain routine activities theory and cybercrimes. Searching was conducted using the following search string: "Routine Activity Theory" AND "cybercrime victimisation" OR "cyber fraud victimisation" OR online crime victimisation.

For both Scopus and Taylor and Francis, the search fields were article titles, abstracts, and keywords, and set between 2015 and 2021. The search process began on 4 January 2021 and resulted in 635 papers, 138 papers from Scopus and 497 papers from the Taylor and Francis database. After duplicates were removed, a filtering process was carried out according to a framework called Preferred Reporting Items for Systematic Literature Reviews and Meta-Analyses (PRISMA) [36]. 632 papers remained for screening after the removal of the duplicates.

The papers were filtered based on the following inclusion and exclusion criteria: (i) papers were excluded if there was no application of the RAT theory; and (ii) the cybercrimes' victimisation and research were related to terms in the titles or abstracts. The screening process resulted in 35 papers remaining for further filtration. Next, the papers' full texts were assessed for eligibility. The eligible papers were included if they met the following criteria: (i) An empirical application of RAT theory in cybercrimes victimisation; and (ii) the cybercrimes are limited to only hacking, malware, fraud, and identity theft. The justification of having only empirical papers is to facilitate the analysis as these studies demonstrate the statistical effect of each factor towards cybercrimes victimisation. Meanwhile, papers containing the following criteria were excluded: (i) papers that address victimisation at national or organizational levels; and (ii) victimisation in online harassment, cyber aggression, cyberbullying, and romance scams. It is important to restrict the papers to individual level analysis for a meaningful comparison of findings.

The filtering process resulted in a total of 13 papers remaining. After the filtering process, snowballing was conducted based on the previous filtered results (13 papers) after PRISMA. Backward snowballing was carried out on Google Scholar [37]. where the reference list of the 13 papers was examined. Related papers based on their title abstracts were also included. The inclusion and exclusion criteria were the same as the ones adopted earlier. This process led to the final datasets, which contained 24 papers. The quality of papers was examined using Mixed Methods Appraisal Tool (MMAT) [38]. Basically, each paper in the dataset was assessed based on the following criteria:

- ➢ Is the sampling strategy relevant to address the research question?
- ➢ Is the sample representative of the target population?
- ➢ Are the measurements appropriate?
- ➢ Is the risk of nonresponse bias low?
- ➢ Is the statistical analysis appropriate to answer the research question?

Figure 1 diagrammatically shows the above-mentioned methodological process derived from the PRISMA framework.

5 Analysis and Findings

The table below demonstrates the final dataset of relevant papers derived from the PRISMA framework for further analysis.

The findings of the articles in Table 1 were analysed and classified based on the RAT components (activities that increase proximity to offenders, target attractiveness, and guardianship. The articles were also differentiated based on the cybercrime topologies being investigated; (a) cybercrime-dependent (hacking and malware) and (b) cybercrime-enabled (phishing, fraud, and identity theft). These studies were further refined into 3 contextual categories; (1) secondary data from citizens (SDC), (2) survey studies using citizens (SVC), and (3) survey studies using studies (SVS). The justification for refining the analysis based on the study approaches can help to identify whether differences of findings resulted from the different methods and types of samples used. The final data set comprised of (a) 11 SDC papers, (b) 6 SVC papers and (c) 6 SVS papers as shown in Figure 2. The result of the paper analysis based on these three categories is presented using graphs in Sections 5.1 to 5.3.

5.1 Activities Influencing Cyber-enabled Versus Cyber-dependent Crimes

There are no clear boundaries to distinguish which activities are more prone to cyber-dependent crimes compared to cyber-enabled crimes. However, several patterns emerged, which warrant further investigation.

Firstly, online shopping is one of the mutual activities that increases the risk of both types of crimes [4, 6, 7, 19]. Online shopping can be a fertile

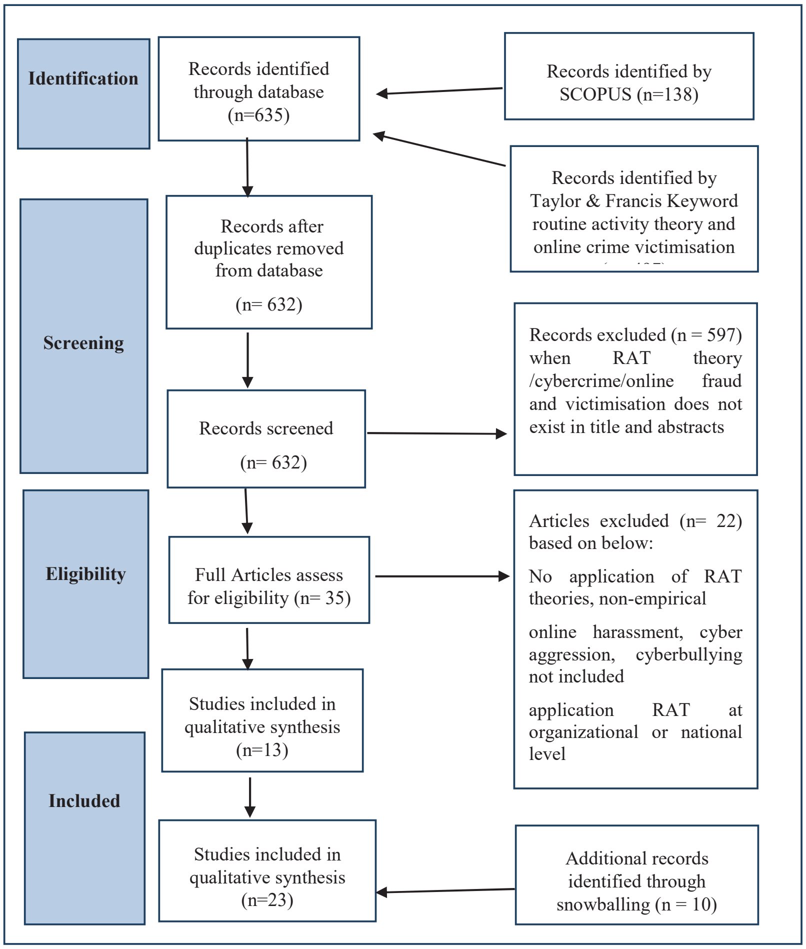
Identification
Records identified through database (n=635)
Records identified by SCOPUS (n=138)
Records identified by Taylor & Francis Keyword routine activity theory and online crime victimisation
Screening
Records after duplicates removed from database
(n= 632)
Records excluded (n = 597) when RAT theory /cybercrime/online fraud and victimisation does not exist in title and abstracts
Records screened
(n= 632)
Eligibility
Full Articles assess for eligibility (n= 35)
Articles excluded (n= 22) based on below:
No application of RAT theories, non-empirical
online harassment, cyber aggression, cyberbullying not included
application RAT at organizational or national level
Included
Studies included in qualitative synthesis (n=13)
Studies included in qualitative synthesis (n=23)
Additional records identified through snowballing (n = 10)

Figure 1 PRISMA framework for systematic literature review.

medium for online fraud/scam. This scam can be facilitated by fake websites mimicking authentic sellers with a familiar interface and logo. The scam is made even more attractive through offerings of popular items at much-reduced costs, which later becomes disappointing when the goods do not arrive. As for cyber-dependent crimes, attackers can seed apps or links in pop-up ads and coupons with malware to infect the victim's system. Another mutual activity influencing both types of cybercrimes is online banking [19, 34, 45]. Clearly, activities that involve financial transactions influence both types of cybercrimes.

Table 1 Articles in final dataset

Papers (References)	Context of Paper
[3]	Secondary Data from Eurobarometer (27,680 citizens)
[4]	Secondary Data (10,314 Netherland citizens)
[5]	Self-report survey (284 students)
[7]	Self-report survey (6,580 Swiss citizens)
[8]	Self-report survey (295 USA students)
[9]	Self-reported Survey (173 Korean academic profile)
[10]	Self-report survey (11,741 USA citizens)
[11]	Secondary Data (U.S. National Crime Victimisation Survey and Identity Theft Supplement (ITS)) (128,419 USA citizens)
[17]	Secondary Data (19,422 Canadian citizens)
[19]	Secondary Data (Crime Survey of England and Wales) plus 35,000 respondents
[34]	Telephone interviews (1447 USA senior citizens)
[39]	Self-report survey (11,534 USA citizens)
[40]	Self-report survey (295 Malaysian students)
[41]	Secondary Data from 23rd cycle of the GSS (19,422 Canadian citizens)
[42]	Secondary Data from Belgian Cost of Cybercrime Project (967 Belgian Citizens)
[43]	Secondary Data from Caught in the Scammers' Net national survey victimisation (1,539 USA citizens)
[44]	Secondary Data from Longitudinal Internet Studies (5,046 Dutch citizens)
[45]	Secondary Data from Longitudinal Internet Studies for the Social Sciences (18,343 Dutch citizens)
[46]	Secondary Data from Longitudinal Internet Studies for the Social sciences (5570 Dutch)
[47]	Self-report survey (570 USA students)
[48]	Self-report survey (104 Australian citizens)
[49]	Telephone survey (922 USA students)
[50]	Secondary Data from Longitudinal Internet Studies (9163 Dutch citizens)

For cyber-dependent crimes, (hacking/malware) activities that increase visibility/interaction such as Instant Messaging and online forums influence the risk of victimisation [4, 19, 51]. Most of these studies use secondary data from surveys with large respondents. One study which used students as a sample found a non-significant effect of Instant Messaging [47] (refer Figure 3).

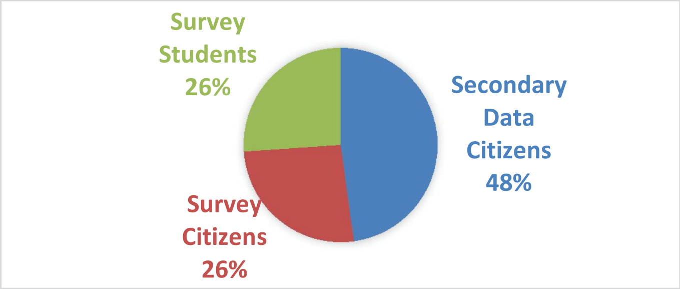

Figure 2 Distribution of papers in final dataset.

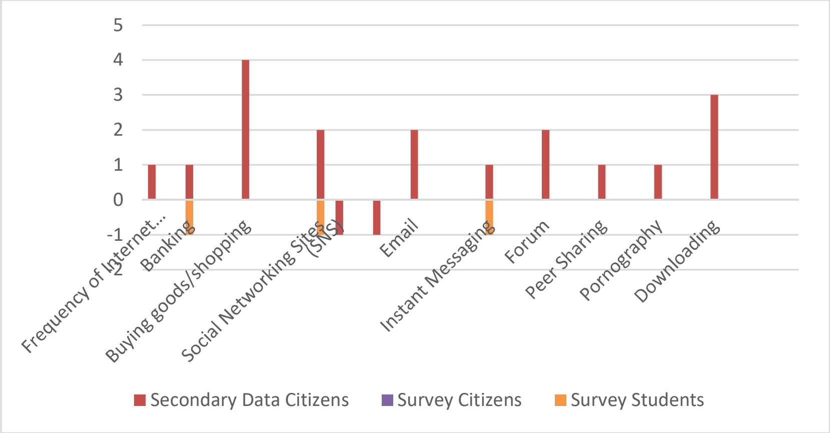

Figure 3 Activities significantly influencing hacking/malware victimisation (*Negative number denotes number of studies for non-significant effect).

In general, there was more evidence from large scale studies demonstrating that risky activities such as downloading media, peer-sharing, and pornography influence cyber-dependent victimisation [4, 19, 44]. These make sense as the perpetrator can often include viruses or malware during these activities. As for SNS activities, the large-scale secondary data studies suggest that Social Networking Site (SNS) activity do not influence phishing and fraud victimisation (see Figure 4), except for the research by [43], which used students as respondents.

One plausible reason for the insignificant relationship between SNS and cyber-enabled crimes is due to the measurement. In most of the studies, only frequency using SNS was measured. The implication of the RAT theory is that frequency of performing activities alone does not accurately explain

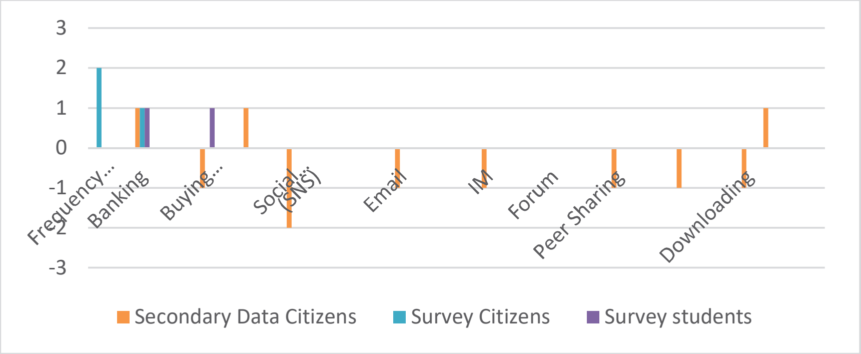

Figure 4 Activities significantly influencing phishing victimisation (*Negative number denotes number of studies for non-significant effect).

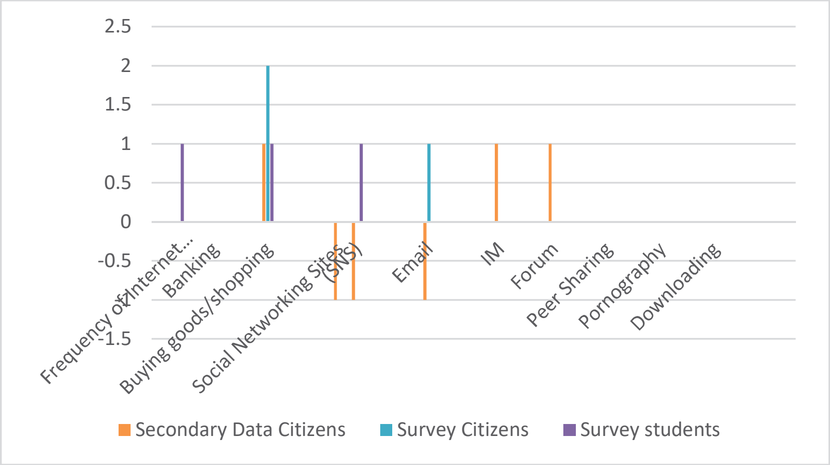

Figure 5 Activities significantly influencing fraud victimisation (*Negative number denotes number of studies for non-significant effect).

victimisation. Instead, the data revealed by those activities may possibly provide a better explanation. For example, just spending time lurking or scrolling on SNS will not reveal any data to a motivated offender. However, sharing posts, check-ins, and comments, especially on public walls, will reveal unique data about potential victims. Another study by Saridakis et al. (2016) supported this argument, demonstrating people who have higher usage of knowledge sharing on social media are more susceptible towards cyber-crime compared to people who frequently use social media. The amount of types of information disclosed on SNS may be a more accurate predictor for cyber-enabled victimisation [6]. This speculation has some support from [43] in their study, which demonstrated how SNS influences phishing through information disclosure.

It is noteworthy to mention that using students as a sample may lead to inconsistent results from the majority of findings as demonstrated in [47] and [40]. Future studies can probably formulate classification of activities and differentiate between cybercrimes. A typology of activities for different types of cybercrimes can be devised as follows; For example: (1) activities that increase visibility (forums, blogs, Instagram); (2) activities that involve transactional data (online shopping, online banking); and (3) deviant activities (pornography, cyber-aggression) and other relevant classification of activities. Analysis using categorisation of activities aligned with the cybercrimes' nature or approach (system versus human-based) may provide more meaningful results.

Additionally, examining the direct effects of frequency activities alone may yield an inaccurate interpretation. In the future, the effect of interaction between activities and information disclosure may portray a more accurate interpretation. Alternatively, more mediation factors should be considered regarding the frequency of online activities towards cybercrime victimisation.

5.2 Target Attractiveness Influencing Cyber-enabled Versus Cyber-dependent Crimes

Target attractiveness comprises two dimensions, which are the routine activities that make individuals or objects potential victims, and attributes of the individuals or objects that make them attractive targets [28]. Our SLR found that a few measurements have been used to represent target suitability, namely opening and clicking links, posting personal information, and risky online disclosure [6]. The concept of target suitability is also reflected by the objects/devices connected to Internet technologies. The attributes of the target devices themselves, such as the connectivity of the devices, represent target suitability.

The majority of the studies analysed demonstrated that posting personal information like pictures, phone numbers, and addresses [8] did not influence both types of cybercrimes' victimisation (see Figures 6, 7 and 8). Future researchers may want to untangle the meaning of this puzzling finding. In one study, posting accurate information significantly influenced both phishing and hacking, but was negatively correlated [17]. The authors speculated that

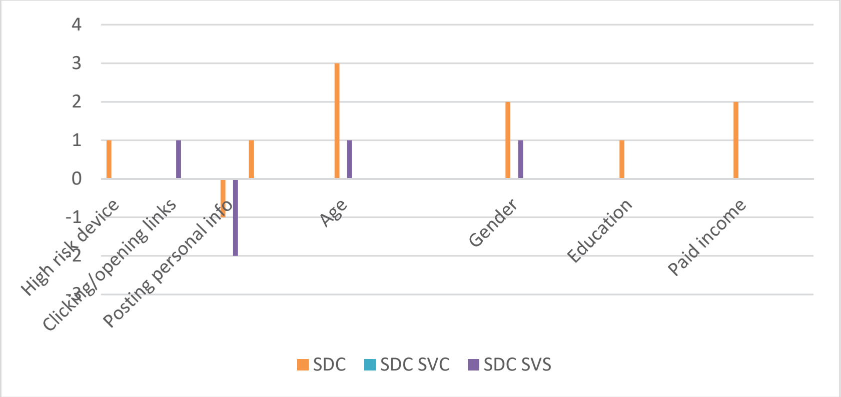

Figure 6 Target attractiveness factors significantly influencing hacking/malware victimisation (*Negative number denotes number of studies for non-significant effect).

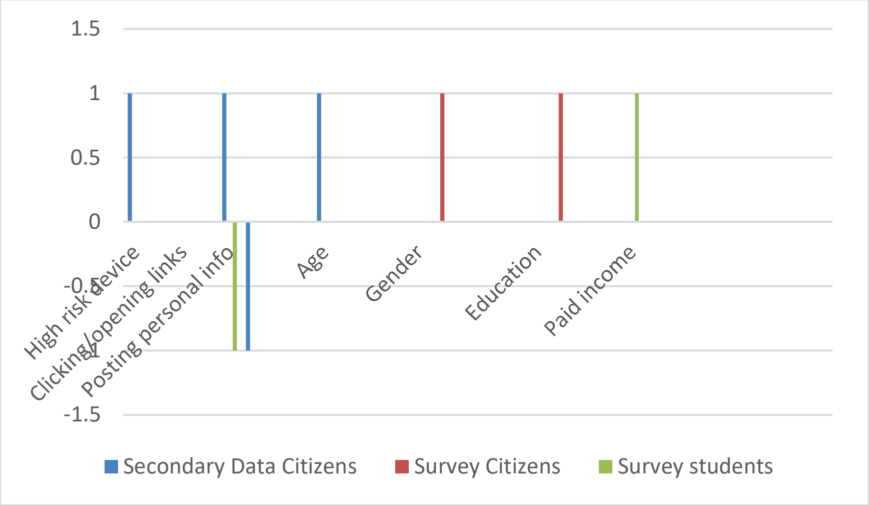

Figure 7 Target attractiveness factors significantly influencing phishing victimisation (*Negative number denotes number of studies for non-significant effect).

this might reflect a measurement issue. Posting accurate information may contradict the need to supply accurate details when making online purchases or online banking as both activities have been proven to influence both types of cybercrimes' victimisation. This result could also indicate that phishers prefer using large email lists, such as hacking into online retailers' databases, rather than searching for individuals' personal information on SNS or other

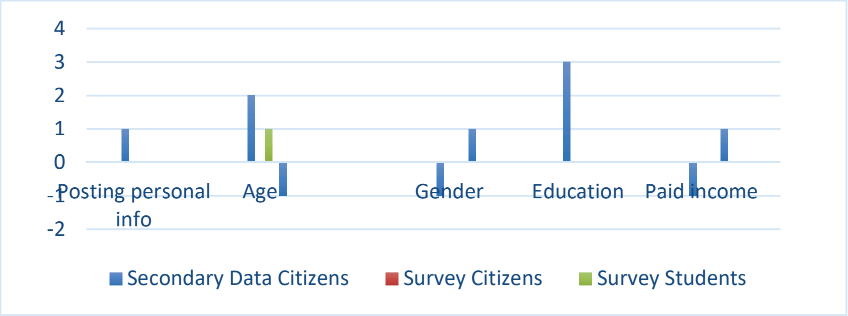

Figure 8 Target attractiveness factors significantly influencing fraud victimisation (*Negative number denotes number of studies for non-significant effect).

websites. Therefore, using SNS or being careless with personal information online might not be strongly related to phishing targeting.

There are also streams of studies that operationalise target attractiveness based on the attributes of devices. For example, Akdemir et al. [19] in their study represent target attractiveness as devices connecting to public Internet and laptops used away from home/work/school/college, thus exposing technological vulnerabilities. Both devices' vulnerabilities are prone to cybercrime victimisation [19].

Among the sociodemographic factors, education is the more stable predictor, especially for cyber-enabled crimes (see Figures 7, 8 and 9). For example, for identity theft cases, victims that are more highly educated are more attractive for victimisation [7, 11]. This finding makes sense as these victims have more credible social status [7], which lure potential offenders. In several studies, income also positively correlates with cyber-dependent crime [46, 53].

To fully comprehend the effect of age, an analysis of the interaction effect of age and online activities must be performed. For example, in cyber-dependent crimes such as hacking and malware, older people are less susceptible to virus attacks. This finding may be attributed to older people generally spending less time online, hence less exposure to attacks. On the other hand, in some cases, older people are more vulnerable to cyber-enabled crimes such as online scams and identity theft, potentially due to limited knowledge or self-efficacies in dealing with technologies. Contrarily, Junger et al. [3] demonstrated that younger people were more prone to online purchase fraud, while older groups are more likely to be victims of online banking fraud. This observation may be due to a similar justification. Further

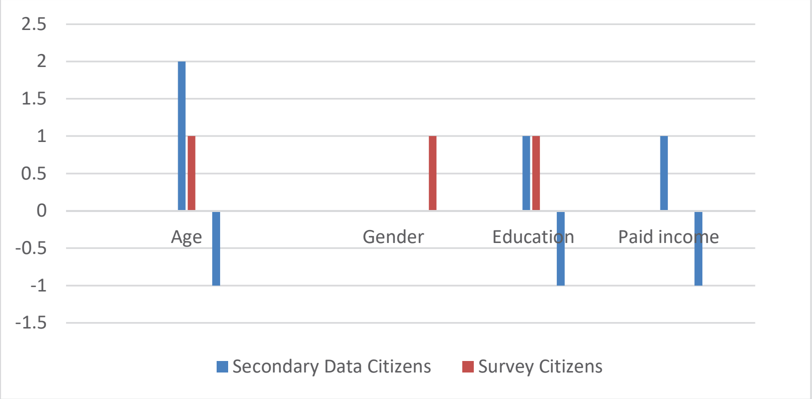

Figure 9 Target attractiveness factors influencing identity theft victimisation (*Negative number denotes number of studies for non-significant effect).

analysis needs to be done on the interaction effects of age and time spent online and age and lack of knowledge or self-efficacies.

The effect of gender towards cybercrime victimisation is inconclusive. Some studies have shown that women are more susceptible to cyber-dependent crimes such as hacking and malware [40, 47]. However, other studies reported a non-significant relationship of gender, especially in cyber-enabled crimes [7, 8].

5.3 Guardianship Influencing Cyber-enabled Versus Cyber-dependent Crimes

The analysis of guardianship factors towards cybercrimes is presented in Table 4 below. From the literature analysis, technical guardianship has not shown itself to be a good predictor for reducing cybercrime victimisation. Most of the studies showed that using anti-virus software is related to victimisation [32], regardless of the types of cybercrimes. For example, Bossler and Holt [47] demonstrated that anti-virus is not correlated with malware victimisation (see Figure 10). Additionally, anti-virus is not associated with cyber-enabled crimes such as identity theft [11]. What is more surprising is that in some studies, having anti-virus protection is associated with a higher risk of victimisation [7, 19]. Only one study demonstrated that having an email filter can reduce the risk of hacking/malware victimisation [44].

This contradicting effect of anti-virus towards victimisation has been argued to be related to the studies' nature. However, since most of the studies

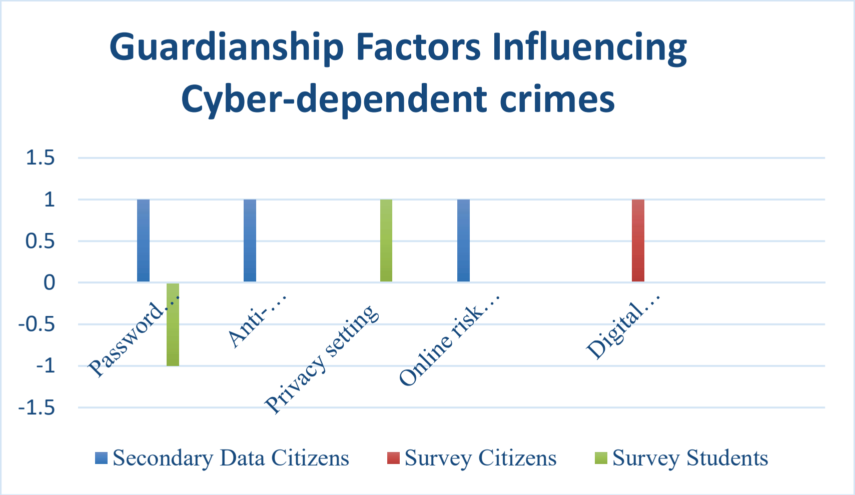

Figure 10 Guardianship factors influencing cyber-dependent crimes (*Negative number denotes number of studies for non-significant effect).

analysed are cross-sectional, there is a possibility that technical guardianship is adopted after being victimised. Therefore, installing anti-virus and other filtering software does not appear to reduce the risk of victimisation. However, prior victimisation experience influences guardianship, as demonstrated in Guerra's [45] longitudinal study. The study shows that previous victimisation influences greater levels of guardianship at time 2. However, the effect of guardianship at time 2 still does not influence victimisation at the subsequent time 3. In addition, Leukfeldt and Yar [4] argue that a user may still not be protected, especially from the cyber-dependent crimes of new or unknown malware types. An offender can also exploit a flaw in software despite the existence of an anti-virus.

As for personal guardianship, a few constructs have been used as proxies, namely digital skills/literacy and online risk awareness. Digital skills or digital literacy have been argued as one of the guardianships from the risk of victimisation. In a study by Milani [7], digital skills are represented by solving problems related to their smartphones independently. The result shows that people with higher digital skills are less prone to becoming victims of hacking and virus attacks. However, IT skills do not influence cyber-enabled crimes such as identity theft. In another study, digital skills are also known as digital literacy shows that this factor significantly influences cyber-enabled crime victimisation, i.e., responding to phishing emails.

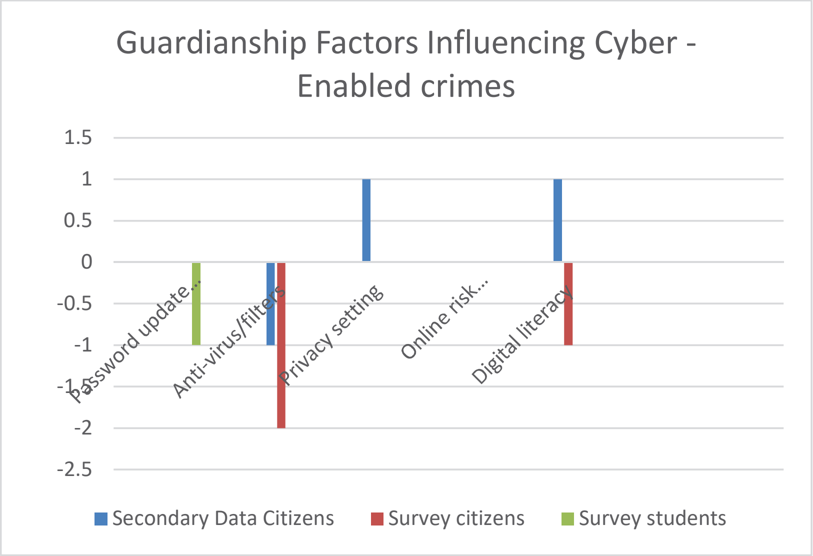

Figure 11 Guardianship factors influencing cyber-enabled crimes (*Negative number denotes number of studies for non-significant effect).

Based on the analysis, we can see that digital skills or literacy effects on risk of victimisation are more prominent in cyber-dependent crimes such as hacking. For cyber-enabled crimes, the role of digital skills has mixed findings (see Figure 11). We speculated that the measurement of digital literacy used might have contributed to these mixed findings. For cyber-enabled crimes like phishing or identity theft, digital literacy should assess the knowledge on social engineering approaches used in cybercrime. For example, in reflecting on Graham and Triplett's [10] study, a set of specific questions such as privacy policy, scam calls, knowledge about personal data protection, and other privacy-related questions were employed. Using this set of more pertinent questions to represent digital skills for cyber-enabled crimes demonstrates the significant role of victimisation risk. This operationalisation issue was also highlighted by Milani, where it was claimed that the internet-based competency used in their study was measured far too broadly in justifying their insignificant result. They represent basic internet competency as the ability to solve technology-related problems related to smartphones, which may not capture the related skills to combat or protect from cyber-enabled victimisation. For future research, a more delicate operationalisation for digital skills or competency needs to be formulated and targeted according to the types of cybercrimes. Another hypothetical reason is that users who perceive themselves as having high digital skills or IT efficacy can be described as overconfident, where overestimating what they know may diminish one's guardianship [54].

As for online risk awareness, people with higher online risk awareness have a lower risk of victimisation, especially in cyber-dependent crimes such as hacking [4]. However, unfortunately, there are no comparative studies to compare the effect of online risk awareness to cyber-enabled crimes like fraud and identity theft to deduce a meaningful conclusion.

6 Applicability of the Rat Theory in Cybercrimes and Future Research

Based on our review, we suggest a refined specification and operationalisation of RAT's components. The exposure, target attractiveness, and guardianship constructs need to be formulated and differentiated across cybercrimes. This study echoes the call for more adaptable measurements for different types of victimisation, rather than rejecting RAT's applicability [55].

Future studies may want to consider exposure not only in the form of time spent exposure, but also data exposure (what types of data disclosed). As mentioned earlier, time spent on SNS is insignificant in relation to victimisation, which may not depict an accurate picture. It is imperative to examine exposure in the form of time and data exposure (what information is being shared) simultaneously to fully comprehend the effect towards victimisation.

In differentiating or profiling activities that increase motivated offenders in cyber-enabled versus cyber-dependent varies may be more meaningful to analyse the effects towards victimisation. For example, in cyber-enabled crimes, the offender may exploit the transactional and personal data's visibility in the activities engaged in for trapping victims into fraud or identity theft incidents. On the other hand, in cyber-dependent crimes, the perpetrator may exploit security loopholes in activities such as downloading media and p2p sharing to embed viruses or malware. By profiling risky activities according to the types of cybercrimes may yield more meaningful results.

For target attractiveness, future research may want to move from individual-level analysis of sociodemographic factors and attributes, and instead classify the factors into a cluster of low-risk profile and high-risk profile according to types of cybercrimes. A profile may consist of an interaction effect between (1) age × efficacy, (2) gender × income, and other possible combinations of demographics. For example, a low-risk profile for a cyber-dependent crime like hacking may consist of older individuals with low-frequency use of the Internet and less visibility. On the contrary, a high-risk profile will be younger individuals with high-frequency use and active participation on social media and forums. As for cyber-dependent crimes such as scams and identity theft, a high-risk profile may constitute a young, educated, and higher income group. Alternatively, a high-risk profile can also include older people with low self-efficacy. Thus, more research is needed for profiling individuals into lower or higher risk groups of cybercrimes' victimisation.

In terms of guardianship, the current operationalisation of technical guardianship seems problematic. Installing anti-virus as a protective measure is sometimes shown not to be related, and at times is negatively correlated with victimisation. Therefore, this calls for more research to possibly examine the time framing of the installation of anti-virus, either pre or post victimisation. Anti-virus installation may also create a perception of low risk or less severity; hence, individuals are more active online and willing to share personal data. These correlations have not been tested before, which calls for an expansion of the RAT theory to include other constructs (mediators and moderators) to explain the victimisation process rather than the three structural elements (motivated offender, target attractiveness and guardianship).

Future research may explore other personal dimensions of protective measures that better align with cybercrimes' types under investigation. For example, one possible personal characteristic is confidence in detecting cyber-enabled crimes like phishing emails. Confidence can be classified into prospective and retrospective. Prospective confidence refers to the confidence in a person's ability to make a sound judgement. In contrast, retrospective confidence refers to the degree to which individuals believe their judgment is accurate [56]. We can speculate that the higher the retrospective confidence, the higher the risk of cybercrime victimisation.

Currently, most research examines the direct causal effects of RAT's constructs towards cybercrime victimisation. There is a need for more research to examine the intervening processes that exist between RAT'S constructs and cybercrime victimisation. For example, Holtfreter et al. [34] demonstrate that low self-control influenced cybercrime victimisation by mediating risky purchases. In addition, Pratt et al. [49] suggest that online activities mediate the sociodemographic effects. Furthermore, postulating relevant mediating constructs that interact with activities, personalities, target attributes, and guardianship will unfold the complex cybercrime victimisation process.

In conclusion, we recommend a typological application of RAT theory. This approach requires the operationalisation of RAT's constructs (activities, attractiveness, and guardianship) to be tailored according to the nature of the cybercrimes. Through this specification of typology, we can have (1) more refined and stable profiling of activities that increase the exposure to different types of cybercrimes, (2) a combination of attributes that better represents target attractiveness based on the nature of the cybercrimes, and (3) appropriate guardianship operationalisation towards a particular type of cybercrime victimisation.

References

[1] L. K. Ilves, T. J. Evans, F. J. Cilluffo, and A. Alec, "Institute for National Strategic Security, National Defense University European Union and NATO Global Cybersecurity Challenges: A Way Forward Source: PRISM, Vol. 6, No. 2 (2016), pp. 126-141 Published by: Institute for National Strategic Securi," vol. 6, no. 2, pp. 126–141, 2016.

[2] C. L. Cook and K. A. Fox, "Fear of property crime: Examining the effects of victimization, vicarious victimization, and perceived risk," *Violence Vict.*, vol. 26, no. 5, pp. 684–700, 2011, doi: 10.1891/0886-6708.26.5.684.

[3] M. Junger, L. Montoya, P. Hartel, and M. Heydari, "Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe," *2017 Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, Cyber SA 2017*, 2017, doi: 10.1109/CyberSA.2017.8073391.

[4] E. R. Leukfeldt and M. Yar, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis," *Deviant Behav.*, vol. 37, no. 3, pp. 263–280, 2016, doi: 10.1080/01639625.2015.1012409.

[5] F. T. Ngo, A. R. Piquero, J. LaPrade, and B. Duong, "Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online?," *Crim. Justice Rev.*, vol. 45, no. 4, pp. 430–451, 2020, doi: 10.1177/0734016820934175.

[6] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels, and K. Ponnet, "You've got mail! Explaining individual differences in becoming a

phishing target," *Telemat. Informatics*, vol. 35, no. 5, pp. 1277–1287, 2018, doi: 10.1016/j.tele.2018.02.009.

[7] R. Milani, S. Caneppele, and C. Burkhardt, "Exposure to Cyber Victimization: Results from a Swiss Survey," *Deviant Behav.*, vol. 00, no. 00, pp. 1–13, 2020, doi: 10.1080/01639625.2020.1806453.

[8] F. Ngo and R. Paternoster, "Cybercrime Victimization: An Examination of Individual and Situational Level Factors," *Int. J. Cyber Criminol.*, vol. 5, no. 1, p. 773, 2011.

[9] J. Suh, J. Choe, and J. Park, "A lifestyle-routine activity theory (LRAT) approach to cybercrime victimization: An empirical assessment of SNS lifestyle exposure activities," *Asia Pacific J. Inf. Syst.*, vol. 30, no. 1, pp. 53–71, 2020, doi: 10.14329/apjis.2020.30.1.53.

[10] R. Graham and R. Triplett, "Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization," *Deviant Behav.*, vol. 38, no. 12, pp. 1371–1382, 2017, doi: 10.1080/01639625.2016.1254980.

[11] D. Burnes, M. DeLiema, and L. Langton, "Risk and protective factors of identity theft victimization in the United States," *Prev. Med. Reports*, vol. 17, no. July 2019, p. 101058, 2020, doi: 10.1016/j.pmedr.2020.101058.

[12] H. S. Brar and G. Kumar, "Cybercrimes: A proposed taxonomy and challenges," *J. Comput. Networks Commun.*, vol. 2018, no. 1, 2018, doi: 10.1155/2018/1798659.

[13] L. A. Hughes and G. J. Delone, "Serious Crimes, Nuisance, or Both?," pp. 78–98, 2007.

[14] D. Maimon and E. R. Louderback, "Cyber-Dependent Crimes: An Interdisciplinary Review," *Annu. Rev. Criminol.*, vol. 2, pp. 191–216, 2019, doi: 10.1146/annurev-criminol-032317-092057.

[15] E. E. H. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Sci.*, vol. 3, no. 1, pp. 1–10, 2014, doi: 10.1186/s40163-014-0009-y.

[16] R. T. Wright and K. Marett, "The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived," *J. Manag. Inf. Syst.*, vol. 27, no. 1, pp. 273–303, 2010, doi: 10.2753/MIS0742-1222270111.

[17] B. W. Reyns, "A routine activity perspective on online victimisation: Results from the Canadian general social survey," *J. Financ. Crime*, vol. 22, no. 4, pp. 396–411, 2015, doi: 10.1108/JFC-06-2014-0030.

[18] B. J. Koops and R. Leenes, "Identity theft, identity Fraud and/or identity-related crime: Definitions matter," *Crime Deviance Cybersp.*, vol. 30, pp. 249–252, 2017.

[19] N. Akdemir and C. J. Lawless, "Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach," *Internet Res.*, vol. 30, no. 6, pp. 1665–1687, 2020, doi: 10.1108/INTR-10-2019-0400.

[20] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *J. Comput. Virol.*, vol. 2, no. 1, pp. 13–20, 2006, doi: 10.1007/s11416-006-0015-z.

[21] D. Wall, "CYBERCRIME:What is it and what do we do about it? – Mapping out and policing cybercrimes," pp. 1–42, 2011.

[22] M. Hindelang, "Race and Involvement in Common Law Personal Crimes Author (s): Michael J. Hindelang Source: American Sociological Review, Vol. 43, No. 1 (Feb. 1978), pp. 93–109 Published by: American Sociological Association Stable URL: http://www.jstor.or," vol. 43, no. 1, pp. 93–109, 2017.

[23] K. Choi, "Computer Crime Victimization and Integrated Theory: An Empirical Assessment.," *Int. J. Cyber Criminol.*, vol. 2, no. 1, pp. 308–333, 2008.

[24] Cohen, "Cohen_FelsonRoutine-Activities.pdf," *American Sociological Review*, vol. 44, no. August. pp. 588–608, 1979.

[25] R. Tewksbury and E. E. Mustaine, "Routine activities and vandalism: A theoretical and empirical study," *J. Crime Justice*, vol. 23, no. 1, pp. 81–110, 2000, doi: 10.1080/0735648X.2000.9721111.

[26] A. J. Stewart, M. Steiman, A. M. Cauge, B. N. Cochran, L. B. Whitbeck, and D. R. Hoyt, "Victimization and posttraumatic stress disorder among homeless adolescents," *J. Am. Acad. Child Adolesc. Psychiatry*, vol. 43, no. 3, pp. 325–331, 2004, doi: 10.1097/00004583-200403000-00015.

[27] B. W. Reyns, B. Henson, and B. S. Fisher, "Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization," *Crim. Justice Behav.*, vol. 38, no. 11, pp. 1149–1169, 2011, doi: 10.1177/0093854811421448.

[28] L. E. Cohen, J. R. Kluegel, and K. C. Land, "Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory," *Am. Sociol. Rev.*, vol. 46, no. 5, p. 505, 1981, doi: 10.2307/2094935.

[29] M. Yar, "The novelty of 'Cybercrime': An assessment in Light of routine activity theory," *Crime Deviance Cybersp.*, vol. 2, no. 4, pp. 3–24, 2017.

[30] R. B. Felson and S. F. Messner, "The control motive in intimate partner violence," *Soc. Psychol. Q.*, vol. 63, no. 1, pp. 86–94, 2000, doi: 10.2307/2695883.

[31] M. Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," *Eur. J. Criminol.*, vol. 2, no. 4, pp. 407–427, 2005, doi: 10.1177/147737080556056.

[32] B. W. Reyns, B. Henson, and B. S. Fisher, "Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept From Routine Activity Theory as It Applies to Online Forms of Victimization," *J. Contemp. Crim. Justice*, vol. 32, no. 2, pp. 148–168, 2016, doi: 10.1177/1043986215621378.

[33] B. W. Reyns, R. Randa, and B. Henson, "Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis," *Crime Prev. Community Saf.*, vol. 18, no. 1, pp. 38–59, 2016, doi: 10.1057/cpcs.2015.21.

[34] K. Holtfreter, M. D. Reisig, T. C. Pratt, and R. E. Holtfreter, "Risky remote purchasing and identity theft victimization among older Internet users," *Psychol. Crime Law*, vol. 21, no. 7, pp. 681–698, 2015, doi: 10.1080/1068316X.2015.1028545.

[35] M. J. Fleming, S. Greentree, D. Cocotti-Muller, K. A. Elias, and S. Morrison, "Safety in cyberspace: Adolescents' safety and exposure online," *Youth Soc.*, vol. 38, no. 2, pp. 135–154, 2006, doi: 10.1177/0044118X06287858.

[36] D. Moher et al., "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Med.*, vol. 6, no. 7, 2009, doi: 10.1371/journal.pmed.1000097.

[37] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," *ACM Int. Conf. Proceeding Ser.*, 2014, doi: 10.1145/2601248.2601268.

[38] Q. N. Hong *et al.*, "Mixed Methods Appraisal Tool (MMAT), Version 2018. User guide," *McGill*, pp. 1–11, 2018, [Online]. Available: http://mixedmethodsappraisaltoolpublic.pbworks.com/w/file/fetch/127916259/MMAT_2018_criteria-manual_2018-08-01_ENG.pdf%0Ahttp://mixedmethodsappraisaltoolpublic.pbworks.com/.

[39] H. Chen, C. E. Beaudoin, and T. Hong, "Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors," *Comput. Human Behav.*, vol. 70, pp. 291–302, 2017, doi: 10.1016/j.chb.2017.01.003.

[40] G. H. Kirwan, C. Fullwood, and B. Rooney, "Risk Factors for Social Networking Site Scam Victimization among Malaysian Students," *Cyberpsychology, Behav. Soc. Netw.*, vol. 21, no. 2, pp. 123–128, 2018, doi: 10.1089/cyber.2016.0714.

[41] B. W. Reyns and B. Henson, "The Thief with a Thousand Faces and the Victim with None," *Int. J. Offender Ther. Comp. Criminol.*, vol. 60, no. 10, pp. 1119–1139, 2016, doi: 10.1177/0306624X15572861.

[42] L. De Kimpe, M. Walrave, P. Verdegem, and K. Ponnet, "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context," *Behav. Inf. Technol.*, vol. 0, no. 0, pp. 1–13, 2021, doi: 10.1080/0144929X.2021.1905066.

[43] G. S. Mesch and M. Dodel, "Low Self-Control, Information Disclosure, and the Risk of Online Fraud," *Am. Behav. Sci.*, vol. 62, no. 10, pp. 1356–1371, 2018, doi: 10.1177/0002764218787854.

[44] T. J. Holt, J. van Wilsem, S. van de Weijer, and R. Leukfeldt, "Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization," *Soc. Sci. Comput. Rev.*, vol. 38, no. 2, pp. 187–206, 2020, doi: 10.1177/0894439318805067.

[45] C. Guerra and J. R. Ingram, "Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data," *Deviant Behav.*, vol. 00, no. 00, pp. 1–17, 2020, doi: 10.1080/01639625.2020.1774707.

[46] J. Van Wilsem, "Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization," *J. Contemp. Crim. Justice*, vol. 29, no. 4, pp. 437–453, 2013, doi: 10.1177/1043986213507402.

[47] A. Bossler and T. Holt, "On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory," *Int. J. Cyber Criminol.*, vol. 3, no. 1, p. 400, 2009.

[48] A. Hutchings and H. Hayes, "Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?," *Curr. Issues Crim. Justice*, vol. 20, no. 3, pp. 433–452, 2009, doi: 10.1080/10345329.2009.12035821.

[49] T. C. Pratt, K. Holtfreter, and M. D. Reisig, "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory," *J. Res. Crime Delinq.*, vol. 47, no. 3, pp. 267–296, 2010, doi: 10.1177/0022427810365903.

[50] E. R. Leukfeldt, "Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization," *Cyberpsychology, Behav. Soc. Netw.*, vol. 17, no. 8, pp. 551–555, 2014, doi: 10.1089/cyber.2014.0008.

[51] J. M. Guerra, I. Martínez, L. Munduate, and F. J. Medina, "A contingency perspective on the study of the consequences of conflict types: The role of organizational culture," *Eur. J. Work Organ. Psychol.*, vol. 14, no. 2, pp. 157–176, Jun. 2005, doi: 10.1080/13594320444000245.

[52] G. Saridakis, V. Benson, J. N. Ezingeard, and H. Tennakoon, "Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users," *Technol. Forecast. Soc. Change*, vol. 102, pp. 320–330, 2016, doi: 10.1016/j.techfore.2015.08.012.

[53] J. Jansen and P. van Schaik, "The design and evaluation of a theory-based intervention to promote security behaviour against phishing," *Int. J. Hum. Comput. Stud.*, vol. 123, pp. 40–55, 2019, doi: 10.1016/j.ijhcs.2018.10.004.

[54] C. Cheng, L. Chan, and C. lam Chau, "Individual differences in susceptibility to cybercrime victimization and its psychological aftermath," *Comput. Human Behav.*, vol. 108, no. October 2019, p. 106311, 2020, doi: 10.1016/j.chb.2020.106311.

[55] M. Näsi, P. Räsänen, M. Kaakinen, T. Keipi, and A. Oksanen, "Do routine activities help predict young adults' online harassment: A multi-nation study," *Criminol. Crim. Justice*, vol. 17, no. 4, pp. 418–432, 2017, doi: 10.1177/1748895816679866.

[56] I. E. Berger, "The Nature of Attitude Accessibility and Attitude Confidence," *J. Consum. Psychol.*, vol. 1, no. 2, pp. 103–123, 1992, doi: 10.1207/s15327663jcp0102_01.

Biographies

Rahayu Ahmad is an Associate Professor in School of Computing in Universiti Utara Malaysia. She received her PhD in Information Systems from University of Maryland Baltimore County, USA. Her research interest is in cybersecurity, social informatics and online learning.

Ramayah Thurasamy, is currently a Professor of Technology Management, School of Management, Universiti Sains Malaysia, Visiting Professor Minjiang University (China), Daffodil International University (DIU) Bangladesh, Universiti Malaysia Sarawak (UNIMAS), Universiti Kebangsaan Malaysia (UKM) and Universiti Teknologi MARA (UiTM), Adjunct Professor at Sunway University and Universiti Tenaga Nasional (UNITEN), Malaysia. He was also a Visiting Professor at King Saud University (Kingdom of Saudi Arabia) and Adjunct Professor at Multimedia University previously. He is also currently the Chief Editor of the Asian Academy of Management Journal (AAMJ) and Journal of Applied Structural Equation Modeling (JASEM). He also serves on the editorial boards and program committee of several international journals and conferences of repute. His full profile can be accessed from http://www.ramayah.com