The Impact of Cybercrime in Modern Generation Based on Systematic Literature Review Analysis

Kong Ming Chai[1], Ang Zi Xuan[1], Muhaymin Hakim Abdullah[2*]

[1]Faculty of Mechanical & Manufacturing Engineering,
 Universiti Tun Hussein Onn Malaysia, Batu Pahat, 86400, MALAYSIA

[2]Centre for General Studies and Co-Curricular,
Universiti Tun Hussein Onn Malaysia, Batu Pahat, 86400, MALAYSIA

*Corresponding Author

Abstract: Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission. Due to the pervasive presence of the internet, the modern generation faces unprecedented challenges posed by cybercrime. Cybercrime has brought a lot of impacts to individuals, societies, and institutions in contemporary times. Sadly, it has become one of the most worrying issues in the current world. This study was done to determine the impact of cybercrime in modern generation. This research employs a qualitative approach by conducting a systematic literature review utilizing the PRISMA method. Moreover, it incorporates the outcomes of prior studies by employing a screening process to identify and critically access each one, thereby reestablishing their significance with the current study. The results of the study found impacts of cybercrime in modern generation which are financial consequences, expanding security budget, social implications, information security concern, and psychological and emotional toll.

Keywords: Social sciences, modern generation, cybercrime, cybersecurity, social media implication

1. Introduction

Cybercrime is a word that concludes all kinds of criminal activity that involves computers or computers network (Das & Nayak, 2013). The advancement of technology has profoundly changed how people use technology. It is always true to say the routing of a large amount of people use the Internet to work, do online shopping, and for entertainment (Monteith *et al*., 2021). As the online duration has increased enormously, cybercrime has also grown large businesses, academia, and governments. Cybercrime was labeled as a major global risk (The Global Risk Report, 2019). Cybercrime has a lot of impact on the modern generation and the impact of cybercrime extends beyond individuals to businesses and organizations. Cyberattacks, cyberbullying has become something very common making some places ban the usage of social media. For example, the US believes that social media is a potential threat to national security, hence, the use of social media is banned in government workplaces (Hammaad Salik *et al*., 2019).

In this modern generation, social media has become an inevitable part of human life. Based on research in 2019, there is 3.5 billion (45.5%) people often use social media for at least 2.8 hours per day (Ortiz-Ospina, 2019). However, cybercrime has emerged as a critical issue in the modern generation. It is because of the increasing connectivity, society is too dependent on social media, making cybercrime an ever-growing threat. The medieval era witnessed the emergence of the Renaissance and Restoration periods, which brought about a transformation in the understanding of "crime." These epochs introduced novel perspectives and approaches to crime, such as utilitarianism, a positive outlook, analytical

reasoning, the principles of natural justice, and the ideas of laissez-faire, hedonistic philosophy, and the pain and pleasure theory. These concepts and ideologies that emerged during this time expanded the horizons of studying crime. In the subsequent periods, particularly during the scientific and industrial revolutions, a rational approach to interpretation gained prominence, shaping the prevailing mindset (Das & Nayak, 2013).

This study mainly focuses on the modern generation as social media or digital technology is advancing at a rapid rate in this modern era. The parameter of this study is worldwide to conclude the common impact that is caused by cybercrime. The major context of this study is to investigate the impact of cybercrime that exists in the modern generation due to the increasing usage of social media by referring to the published research papers as guidance for the research process. Hence, ten articles are reviewed to obtain an overview of the impact of cybercrime on the modern generation. The research problem is "What is the impact of cybercrime?" To be able to answer the research problem, this study aims to determine the impact of cybercrime. The method used is based on the qualitative method of systematic literature review, through a filtering process to figure out and review the article in detail.

2. The Impact of Cybercrime in the Modern Generation

Undeniably, technology is advancing at an uncontrollably fast pace in this modern generation and has brought tons of benefits to society. However, at the same time, it has also been misused, causing harm to society, which is a new form of criminal activity called cybercrime. The impact of cybercrime has become a major concern in the current society. It is because cybercrime causes financial consequences (Benedikter, 2022; Mason, 2020; Gapsalamov *et al.*, 2020; Kotlyarevskyy *et al.*, 2022). One of the most appealing impacts is the financial consequences, cybercrime leads to the substantial financial losses incurred by individuals, businesses, and governments. For example, bank account details can be hacked, and the account can be drained, money is lost (Benedikter, 2022). The users' information is easily stolen by cybercriminals, the financial information can be accessed by them and engage in fraudulent activities. Sometimes the costs of incident response, data recovery, and system repair that are caused by the cyberattack can be staggering as well. In short, it causes money to restore the effect caused by cybercrime, and money is lost in the process.

Other than that, cybercrime also has been a threat to information security. It has been a global concern as information can be easily hacked by cybercriminals (Dwiyanti & Ketut Jati, 2019; Ayob, 2020; Rajeswari, 2020; Grubicka, 2019). It has been a global issue as cybercrime causes information security breaches significantly. This has a chance to destabilize governments, disrupt essential services and compromise diplomatic relations. The safeguard at this level is not strong at all and the information online is very vulnerable, this has become a tough challenge yet to be solved. Besides, cybercrime also affects individuals, organizations, and governments to expand security budgets to protect online premises under them. For example, cybercrime will cost $6 trillion to be solved (Benedikter, 2022). In the report of an undergraduate study, it stated that the security budget is indicated to be expanded to $15 million (Vosen, 2021). Cybercrime really requires a lot of budgets to solve, and it is not fully guaranteed that the security system is able to block all sorts of cyberattacks.

Moreover, the impact of cybercrime also causes a psychological and emotional toll. In this context, cybercrime does not only affect the financial status, but it also affects the emotions. The feeling after experiencing an invasion of privacy, the feeling of violation, and the loss of personal data can lead to stress and anxiety (Rajeswari, 2020; Vosen, 2021; Wayne Patterson, 2022). Cybercrime is destructive to social objects of both personal and structural entities in cyberspace (Grubicka, 2019). Cybercrime causes fear and the victim will hinder online activities and undermine trust in the digital ecosystem. To sum up, the impact of cybercrime in the modern generation must be magnified and solved diligently. Cybercrime has brought a lot of negativities into this society, it affects the financial, emotion, and the overall societal fabric. Hence, it is very crucial to know the impact and actions need to be done to prevent or minimize the rate of cybercrime in this modern generation.

3. Methodology

The research was conducted qualitatively using systematic method by analyzing literature reviews which also known as SLR (systematic literature review) in order to reintegrate past studies and researches. The obtained results will go through screening process in order to evaluate and identify every result so that irrelevant documents, journal and books will be excluded.

3.1 PICo for Qualitative Research Questions

The PICo process or framework is a formulation of focused questions to develop literature review search strategy. The term "PICo" stand for, 'P' - Problem, 'I' - Intervention and 'Co' - Context. In this research, two main elements will be used to formulate the hypothese or the question of study. These two main elements are the modern generation as the context, and cybercrime as the problem.

3.2 Searching Strategies

For the searching strategies, PRISMA model searching method is used to extract elements from documents, studies, researches, books, and journal that are related to the effect or impact of cybercrime in modern generations. This strategy is also an effective process when it comes to collect, reviews, resources and analysis obtained results from the database by using the first step which is identifications. Next, screening process will be carried out to remove resources that does not match with the criteria's such as the publication date, language, non-articles, and so on. Then, the remaining resources will be assessed to check for eligibility where the resources that does not cover the main elements will be eliminated and excluded. Lastly, only a small number of resources from the database will be chosen and included in the research to be analyze.

3.3 PRISMA

It is a systematic reviews and meta-analysis used to report and identify the least set of items based on evidence. Fundamentally, PRISMA model focused on the reporting of reviews assessing the impacts of interventions. However, other than assessing interventions, it can aslo be utilized as a premise for reporting systematic reviews with goals such as assessing aetiology, predominance, determination or forecast an outcome. In this research, PRISMA model is used to analyse and select related articles and resources after excluding the unwanted contexts that does not cover the topic regarding cybercrime in modern generations.

3.4 Resources

Resources for this research will be obtained from Google Scholar and Scopus. In this matter, Google Scholar database will be the main platform to identify and find the related articles, whereas Scopus database will function as the second platform for additional resources and articles. Google Scholar was chosen as the main platform because Google Scholar which is released in November 2004, is a freely accessible web search engine that records a wide array content or metadata of academic literature that incorportates a lists of peer-reviewed academic journals, conference papers, thesis, reports, books and so on.

On the other hand, Scopus that was launched in year 2004 by Elsevier which is a company from Netherland, is also a trusted academic literatures search engine. Scopus covers as much as approximately 36,000 titles from more than 11,000 publishers from across the globe. The list of records in Scopus are all top-level tier and high quality academic literatures from life sciences, social sciences, health sciences and physical sciences. Scopus contain 3 main variety of resources which are book, journals and trade journals. Thus, resources that were analysed for this research regarding the impact or effect of cybercrime in modern generations will all be obtained from Google Scolar and Scopus, this two trusted and reliable academic literature web search engine.

3.5 Eligibility and Exclusion Criteria

This research will only use article, journal or book that was written in English language only for easier understanding. Any other resources such as reports will not be analyzed, same goes to resources that was written in Russian, German and so on will all be excluded during the screening process. Apart from that, only resources that was published since year 2019 and above will be obtained in order to eliminate resources that was published too long ago. These criteria were made in order to check for the eligibility and whether the resources are accurate and relevant to the impact or effect of cybercrime in modern generation.

Table 1 - Criteria eligible and excluded

Criteria	Eligible	Excluded
Types of Resources	Article, Journal, Book	Reports
Language	English	Other than English
Publication Timeline	2019 – 2023	<2019

3.6 Systematic Review Process

The first step will be identification of records from Google Scholar and additional records from Scopus. Keywords will be used at this stage in order to reduce the range of resources and results shown. Synonyms for keywords that carries the similar meaning which were identified through Thesaurus website will also be put into the searching and identifications keywords as shown in Figure 1. A total of 54 records were identified from Google Scholar web search engine, and 1 additional record was identified from Scopus. After the records were identified, screening process will be carried out to remove and exclude unwanted resources. No duplicated or repeated records were identified at this stage. Resources that were outside the field of article, journal and book will be removed. Apart from that, resources that does not uses English language and resources that was published before year 2019 will also be excluded. A total of 27 resources

were eliminated and excluded at the screening stage. Next, it will be the stage where resources will be assessed to check for eligibility. Resources that are irrelevant and does not cover the main topic about the impact or effect of cybercrime to modern generations will be excluded. 18 resources were eliminated in the process. Lastly, only 10 article journals were chosen to be analyze.
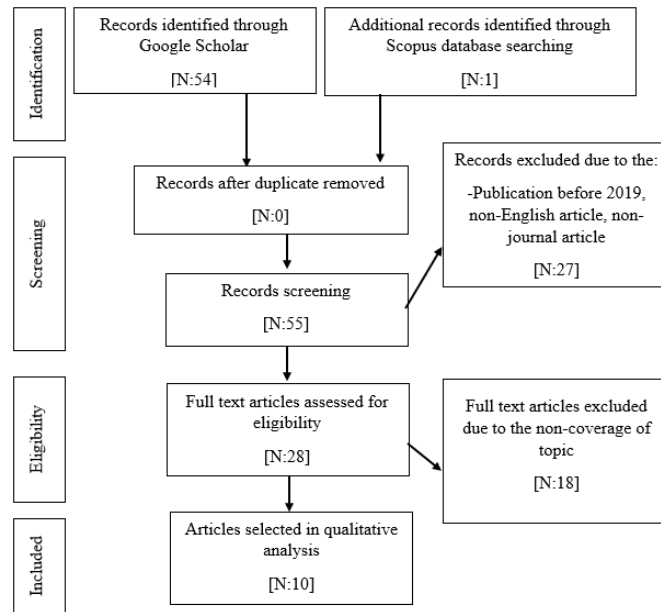

Fig. 1 - PRISMA model

3.7 Data Abstraction and Analysis

The remaining 3 article journal will be assessed in details in order to obtain the content that matches the topic and answers the question of study. Abstracts and full reading of the entire article to obtain the themes and sub-themes of digital ethics strengthening elements found in the journal articles.

Table 2 - Keywords used during identification of records

Database	Search
Google Scholar	("impact" OR "effect") AND ("cybercrime") AND ("modern generations")
Scopus	(TITLE-ABS-KEY ("impact" OR "effect")) AND (("cybercrime")) AND ("modern generations") AND (LIMIT-TO (PUBYEAR , 2023) OR LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019))

4. Result and Analysis

Based on a review of literature over a 5-year period, it has been identified that there are five major impacts of cybercrime in this modern generation. These impacts include financial consequences, expanding security budget, social implications, information security concerns and psychological and emotional toll. This collection of studies was published between 2019 and 2023. There were 2 studies published in 2019, 4 studies in 2020, 1 study in 2021, 3 studies published in 2022, and 0 study published in 2023. The literature review was conducted based on the impact of the cybercrime in modern generation. All articles were qualitatively investigated.

Table 4 has shown the impact of cybercrime in modern generation, with a total of 10 studies conducted from 2019 to 2023. Among the 10 studies analyzed, the primary impact that was most commonly seen for cybercrime in the modern generation is information security concern, accounting for 80%. This is followed by the second-highest impact, which is the financial consequences and psychological and emotional toll, both accounting for 40%. Finally, the least impact seen in cybercrime in the modern generation is expanding security budget and social implications, both accounting for 20%.

Table 3 - The percentage of impact of cybercrime in modern generation

No	Impact	Quantity	Percentage for each Impact (%)
1	Financial Consequences	4	40%
2	Expanding Security Budget	2	20%
3	Social Implications	2	20%
4	Information Security Concern	8	80%
5	Psychological and Emotional Toll	4	40%

Table 4 - Impact of cybercrime in modern generation

No	Author	Year	Impact of Cybercrime in Modern Generation				
			FC	ESB	SI	ISC	PET
1	Ida Ayu Intan Dwiyanti & I Ketut Jati	2019				■	■
2	Joanna Grubicka	2019		■			
3	Angel Candice Mason	2020	■			■	
4	Chennareddy Sirichandana Pvn Rajeswari	2020	■			■	■
5	A. R. Gapsalamov et al.	2020	■			■	
6	Zalina Binti Ayob	2020				■	
7	David J. Vosen	2021			■	■	■
8	Y. Kotlyarevskyy et al.	2022	■			■	
9	Roland Benedikter	2022		■	■		
10	Wayne Patterson Jeremy Blackstone	2022				■	■
	Total Percentage	-	40	20	20	80	40

Legend Key: -
  FC- Financial Consequences   ESB- Expanding Security Budget   SI- Social Implications
  ISC- Information Security Concern   PET- Psychological and Emotional Toll

5. Discussion and Recommendation

Throughout the years, the field of technology has progressed with an unprecedented pace, resulting in notable advancement, development, and innovation. Technology, the "science of craft" is the collection of technique, skill, and knowledge for practical purpose. Today technology plays a vital role in our daily life. Technology made vast amount of information and resources available at our fingertip. This enhances the efficiency and productivity since technology can help us to obtain researches and knowledges more easily which indirectly helps with the time taken to complete a task, promotes streamline processes and increase productivity.

Technology also revolutionized the communication system, allowing an individual to instant get in contact with one another through messaging, call, email and conferencing globally. This also promotes global connectivity as now people are allowed to get in contact, discuss, make friend, exchange ideas, and collaborate globally anytime anywhere. Due to all these advantages, the issue of people nowadays became overreliance on technology to do anything. The advancement of technology had led to the arise in other side effects and disadvantages. For instance, as the technology advances, so is the cybercrimes committed. The amount and level of cybercrimes committed has grown exponentially with the growth of technology.

This is mainly due to the modern generation that are very depending and relying on the technology to do anything. This opens an opportunity to certain individuals that took advantage of technology to carry out cybercrime activities since that majority of the people trust fully and will not doubt what they found on the Internet whether if it is logical or not. In order to curb this problem, the impact of cybercrimes on modern generations need to be discussed so that more people will be aware of the uprising of cybercrime due to certain individuals who misuse technology to carry out crime activities. Thus, this research is carried out alert people about the effect or impact of cybercrime on modern generations nowadays, and also to investigate the sources or factors or causes that leads to increment in cybercrime activities, and also how to combat and prevent it from happening again.

In order to find the factors and ways to overcome cybercrime activities, it is vital for first understand what cybercrimes and the types of cybercrimes is existing. Generally, cybercrime means criminal activities committed by using technology, computer or software. This includes malware attack on computer, stopping certain software from working properly as what it is designed to do, spreading viruses online, hack or stole data, internet fraud, theft in online payment and many more. Cybercrime activities that are usually seen are email or internet fraud, theft of financial or card payment, crypto jacking, illegal gambling, ransomware and so on.

The causes of cybercrime to happen is usually due to the information are too easy to be accessed. Highly technical led skilled hackers with advanced techniques will be able to bypass and breach the securities and firewall to obtain personal information, codes, passwords, and so on. The complexity of the systems is also one of the factors leading to cybercrime activities. This is because computers or any software usually runs on multiple operating systems programmed with millions of codes. The complexity in system codings making it hard to detect even if there is a loophole or imperfections in the systems, which gaveaway a huge gap for cybercriminals to attack and hack it (Bandakkanavar, 2023).

Furthermore, although it is now in the year of 2023, there are still many individuals that are lack of cybersecurity awareness. Most of them have insufficient knowledge regarding cybersecurity measures, making them more vulnerable to cyberattacks. Apart from that, cybercriminals can easily evade laws as they can hide their identity on the internet, making them hard to be identified and trace. Cybercriminals may also be attacking from any corner in the world, making it extremely difficult and challenging for authorities to find them. This makes most of the criminals think that it is okay to carry out cybercrimes since it is very fast and safe as it does not have any consequences.

The easiest way of combating cybercrimes will be keeping all systems up to date. Individuals should constantly check on the versions of firewall, security software, operating system and so on and immediately update it whenever upgrade is available. This ensures that the computer and software will be equipped with latest protection available. Next, strong, unique passwords with multifactor authentications is encouraged. For instance, include numbers, symbols, uppercase and lowercase alphabets to make passwords long and complex. It is also encouraged to link accounts with smartphones as recognized devices and link with phone numbers. It is to do so that if any unrecognized device trying to log in can be stopped by simply blocking them on smartphone or when anyone who attempt to change anything in the account, a warning text or message will be received immediately on smartphone before it is too late.

Next, people should be more careful when using public Wi-Fi. This is because anyone nearby that is connected to the same Wi-Fi with the Information and Communication Technologies (ICTs) knowledge will be able encrypt, stalk, check the activities on the computer or smartphones that are connected to the same Wi-Fi. Moreover, agencies can launch awareness campaigns, workshops, programs, talk or videos on social medias with alert society about common cybercrimes. It can be used to educate people about the importance and ways of implementing strong security measures to safeguard their information.

Individuals should also invest in implementing trustable security software in computer. Security software such as Kaspersky, Norton 360, McAfee and many more usually comes with all-in-one protection for devices that helps protect online privacy, identity and constantly check for the security level whenever it goes online.

6. Conclusion

In conclusion, technology did change the world in many aspects, making our life more convenient and effective. However, the fact that amount of cybercrime also increases rapidly throughout the years along with technology advancement must not be neglected as well. Since that nowadays, basically everyone uses technology to save, keep and send any information related to themselves, people should be more careful to cybercrime. It is indeed that technology made our life more assessable, convenient, and fast, but it also means it opens a gateway for people who we do not even recognize to access to some of our personal information. We must learn to protect our own account and information about ourselves by hiding them and private the information or use a fake one or simply use the traditional way and jot down in books rather than relying fully on technology. This especially goes to the group of people who have low level of understanding about technology and internet as the people usually likes to target people who does not understand technology well to carry out cybercrime activities. Nowadays there are still many loopholes in technology products that can giveaway personal information that opens gateway for cybercrimes to happen.

In this matter, the research about the impact and effect of cybercrime on modern generation is carried out to show people about the influence lead by cybercrimes. The main aim of this research is to alert people about the danger and consequences of cybercrimes so that more people will be aware of it. Technology, a science created by mankind should have been a medium for a better life and world and not a platform for people that is up to no good to grab the opportunity and carry out cybercrime activities. People should practice good behavior such as professionalism, positive, awareness, and so on when using technology to avoid cybercrime activities. It is to do so that the rate of cybercrimes to occur will drop and everyone can use technology without having the risk of being scammed. Technology should be used as what it is originally designed, which is to enhance human life by providing tools, solutions and information that simplify tasks, increase efficiency, and expand capabilities. It should be used to solve problem and get information, and not a tool for scam or phishing.

References

Ayob, Z. B. (2020). MARA and public user characteristics in response to phishing emails.

Benedikter, R. (2021). *Religion in the age of re-globalization: a brief introduction*. Springer Nature.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2), 142-153.

David. J. V. (2021). An Exploration of Cyberpsychology Strategies Addressing Unintentional Insider Threats Through Undergraduate Education: A Qualitative Study. Thesis. Colorado Technical University. ISBN: 9798460482467

Gapsalamov, A. R., Bochkareva, T. N., AKHMETSHIN, E. M., Vasilev, V. L., & Anisimova, T. I. (2020). DIGITAL SOCIETY: NEW CHALLENGES FOR EDUCATION. *Periodico tche quimica*, *17*(34).

Grubicka, J. (2019). Information society in the context of threats to personal security in cyberspace. *Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska*.

Hammaad, S.& Zaheema, I. (2019). Social Media and National Security. Geopolitics.com. Dated September 9, 2019. Retrieved from: Accessed on October 1, 2023. https://thegeopolitics.com/social-media-and-national-security/#

Kotlyarevskyy, Y., Petrukha, S., Mandzinovska, K., Brynzei, B., & Rozumovych, N. (2022). Impact of Modern Information and Communication Technologies on Economic Security in the Context of COVID-19. *IJCSNS*, *22*(1), 199.

Mason. A. C. (2020). Artificial Intelligence Cybersecurity Threats: Determining Strategy and Decision-Making Effects. 2020. Thesis La Jolla, California. Northcentral University Pro Quest Dissertations Publishing, 2020. 27993340.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*, 1-9.

Ortiz-Ospina, E., & Roser, M. (2023). The rise of social media. *Our world in data*.

Patterson, W., & Blacksttone, J. (2022). A Metric to Assist in Detecting International Phishing or Ransomware Cyberattacks. *Human Factors in Cybersecurity*, *53*(53).

Pulyaevskiy, N. Y., & Shabunin, K. (2023). Impact of Information Technologies on the Formation of Modern Youth. *Язык в сфере профессиональной коммуникации.—Екатеринбург, 2023*, 482-488.

Bandakkanavar, R. (2023). Causes of CyberCrime and Preventive Measures. KrazyTech. Published Mac 14, 2023. Retrieved from: https://krazytech.com/technical-papers/cyber-crime

Rajeswari, P., & Sirichandana, C. Crime Data Analysis Using Hadoop Ecosystem. *European Journal of Molecular & Clinical Medicine*, *7*(11), 2020.

World Economic Forum (2019). The global risks report 2019. Published January 15, 2019. Accessed on October 1, 2023. Retrieved from: https://www.weforum.org/reports/the-global-risks-report-2019