International Journal of Education, Business and Economics Research (IJEBER)

ISSN: 2583-3006

Vol. 2, Issue.4, July - Aug 2022, pp. 1-15

To cite this article: Budiandru, Karsam and Zakkiandri (2022). Cybercrime Software Fraud In Jakarta And Tangerang. International Journal of Education, Business and Economics Research (IJEBER) 2 (4): 1-15

CYBERCRIME SOFTWARE FRAUD IN JAKARTA AND TANGERANG

Budiandru, Karsam and Zakkiandri

[1]Accounting, University of Muhammadiyah Prof. Dr. HAMKA, Jakarta, Indonesia
[23]Postgraduate of Accounting, STIE Swadaya, Jakarta, Indonesia

ABSTRACT

This study was made to find out how well social users understand cybersecurity, cybercrime and information systems against fraud in the DKI Jakarta and Tangerang areas. The population of this research is social media users in DKI Jakarta and Tangerang. The method in this research is quantitative. In this quantitative research, it is not in the form of statistics, in this quantitative research through the process of collecting data by distributing questionnaires and using a sampling method that aims to eliminate the problem of extensive data collection to make population conclusions so that data collection will be practical, cost-effective and convenient. The sampling technique is analysis of the outer model (measurement model) and analysis of the inner model (structural model) using the Smart PLS 3 Multivariate Structural Equation Model (SEM) technique. Partially, the results of this study indicate that cyber security has an effect on fraud. Cybercrime software has no effect on fraud and information systems have no effect on fraud. Simultaneously the value of R – Square (R2) is 0.579 or 57.9%, which means that fraud is influenced by cyber security, cybercrime software and information systems by 57.9%. The contribution of this research shows that cyber security has a positive impact on fraud, in this case the users / users of computerization / digitization must pay attention to the security of the PC / software used. The quantity of this research shows that cyber software security is still having an impact due to lack of caution towards technology and information users.

KEYWORDS: Cyber Security; Cybercrime Software; Fraud; Information Systems

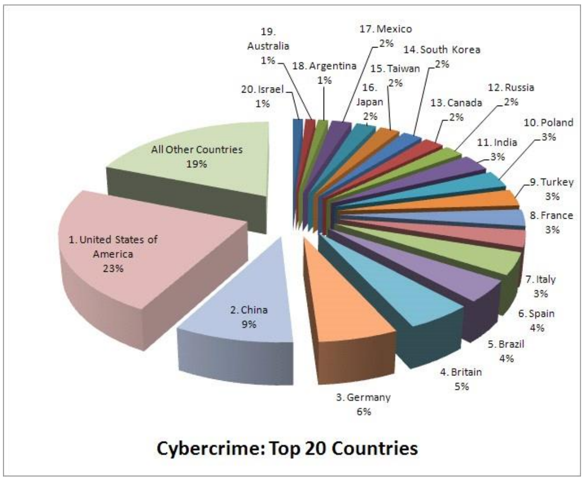
I PRELIMINARY

The development from time to time information communication technology (ICT) is rapid. So that these developments have encouraged various government organizations and institutions (E-government) to adopt technology in order to increase competitive advantage. The method of e-government is changing Government operations were formerly carried out employing current information and communication technologies, as opposed to historically facilitate people, corporations, and government organizations have access to government services **(Adopsi et al., 2020).**

The result of the development of communication technology is the emergence of smartphones equipped with various applications for chat, email, telephone, social media, and other applications **(Km & Km, n.d.).** The Internet is the result of information technology's advancement. A system that links computers to computer networks is the internet. Information technology can be used people may simply access everything they want by using the internet and current social media freely and without restrictions. Cyberspace is a new world presented by the internet **(Asean, n.d.).** There is also cyberspace, which serves as a location for electronic work, as well as a virtual community that has grown thanks to timely communication across constantly connected computer networks **(Fahlevi et al., 2019).** Internet technology-based activities, is no longer a new thing in society. Almost all. Layers of society have become internet users, ranging from small children, teenagers to the elderly **(Umanailo et al., n.d.).** Since the Covid-19 Pandemic in terms of facilities, as many as 195.3 million people or equivalent to 94.6% of the internet, are accessed via smartphones with an average access of 8 hours 52 minutes every day (**Iswardhana et al., 2021).** Indonesians using the internet are consistently rising. Hot suite and We Are Social presented a study in January 2020 stated About 175.4 million people in Indonesia now utilize the internet. Approximately 272.1 million people live in Indonesia. Compared to 2019, this number has grown, which was only 27 million or so users **(Di & Pandemi, 2020).**

The positive impact of information technology on society is due to its ability to support daily activities and extend its duration, as well as its negative impact on the misuse of this technology which can endanger the general welfare of society as a whole **(Komang et al., 2022)**. a term used to describe criminal activities Internet-based information technology is used to carry out these operations to commit criminal acts such as attacking public data or important and confidential personal data **(Deora et al., 2021).**

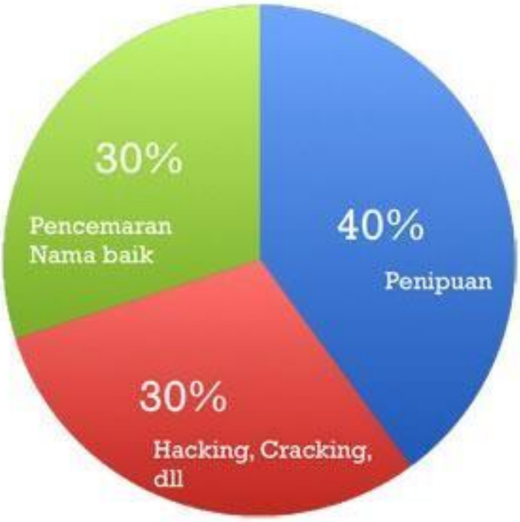
Table I.I Data Percentage Country of Origin Cyber Attack.



Source: **(Jain & Gupta, 2020)**

Cybercrime crimes that frequently occur worldwide include identity theft, data manipulation, phishing, and hacking, spyware, and information leaks. The above crimes are examples of illegal use of telecommunications infrastructure **(Chouiekh & El Haj, 2018).** Often this type of crime is undertaken for self-gratification and financial reasons; it means that this offense is carried out for personal or group gain to make others lose economically. Since due to the Covid-19 virus, the issue of cybercrime has grown more rampant **(Kemp et al., 2021).**

Table 1.2 Percentages of Cybercrime Cases.



Source: http://eptikbsipwt.blogspot.com/2013/05/kasus-cybercrime.html

Of the many cases of crime on the internet (cybercrime), it is dominated by cases of fraud, which is 40% of all cases. 30% were cases of defamation and the rest were cases of other internet crimes (hacking, cracking, etc.) during that period **(2015 – Maret 2018).**

People who commit fraud and people who take part in fraudulent activities for personal gain are called Scammers **(Male et al., 2021).** Pisher is a type of intruder who tries to steal sensitive user information, such as username and password, by using various forms to deceive victims, for example: receiving fake emails, links or attachments and/or voice calls **(Yordania, 2020).** Research shows that the observed reductions Australia, Germany, England and Wales, the US, and other countries all have pretty constant rates of crime. That's why cybercrime is unable to clarify how robberies with forcible entrance are denied yet not forced entry: According to the security hypothesis that the reason for this is increased windows and doors have security features. Contrary to popular belief, the cybercrime hypothesis various security-related evidence tabulated by Tilley et al **(Farrell & Birks, 2018).**

In Indonesia, both the public and the government are now concerned about cybercrime, because there was formerly was cybercrime isn't covered by any ITE Law regulations, and previously Laws pertaining to the problem of cybercrime were implemented in response. However, now incidents of cybercrime have been ITE Law Number 8 of 2011 and thereafter must comply with amendments to Law Number 19 of 2016, particularly in sections 27 to 30 pertaining to behavior things should be avoided when using the internet. Online criminal activity is difficult to avoid despite the existence of a law that governs it, there are yearly instances of cybercrime in Indonesia do not decrease and continue to increase. This topic is extremely intriguing since, according to earlier study by Lubis and Maulana, Indonesian law has several flaws, such as some of the loopholes observed in Electronic Transactions and Information (ITE) law that regulates actions on the internet. Consequently, there is also a conversation regarding vulnerabilities making recommendations in Indonesia for cybersecurity. But one thing stands out to note that Policing is not only an organization but also involves activities and policy-making itself **(Rizqullah et al., 2021).**

A technique known as cybersecurity guards against hostile parties accessing and using digital assets without authorization. Insiders to outsiders are all examples of these harmful actors groups of incredibly driven and creative hackers who target computer systems over the internet. Today, Security is seen as a crucial digital technique that protects individuals, companies, and institutes of higher learning, organizations, and governments. The goal of cybersecurity is to secure and safeguard digital systems, networks, equipment, and information against any illegal access, modification, or disclosure of information, tampering, monitoring, eavesdropping, or devastation **(Wasif et al., 2021).**

Cybersecurity focuses on protecting the confidentiality, integrity, and availability of digital assets and data, officially known as the CIA triad. The CIA triad contains three main concepts that security professionals must understand in order to properly enforce CIA principles: authentication, authorization, and non-repudiation. Cyberattacks have sharply increased in frequency over the past for a few years owing to unsatisfactory expansion of security measures. While massive companies have always had a following target for cybercriminals, even small businesses have also been targeted in most recently. According to estimates, small firms were the targets of 43% of all cybersecurity assaults in 2015. Majority of small enterprises tend due to a lack of sufficient finances or staff, could be more susceptible to cybersecurity assaults, It may be used for cybersecurity tasks, in addition to underestimate internet security dangers. The danger of cyberspace was highlighted as one of the primary issues small firms have with employing information technology (IT). This anxiety is valid due to a cybersecurity issue within an organization cost-prohibitive and have a negative impact on the organization's operations and reputation. However, the decision of adoption of IT by small enterprises is strongly impacted by the surroundings or outside forces. In many nations, small firms are compelled to use IT in order to satisfy client needs and compete with rivals. Those are therefore placed if they find themselves in a have to deploy despite the possibility that it may be attacked by hackers, IT attacks, which are difficult for them to prevent **(Yudhiyati et al., 2021).**

II LITERATURE REVIEW

Definition of Cyber Security

Social cybersecurity refers to a scientific field that emphasizes the use of science to describe and comprehend, and predict cyber-mediated building the cyber infrastructure, as well as alterations in human behavior and social, cultural, and political repercussions necessary societal progress survive in terms of the world's fundamental nature. Shifting situations, present or impending societal cyberthreats, and the cyber-mediated information environment (Rock & Rock, n.d.). Another definition of cyber security is digital asset protection technique that prevents unwanted access so that they are not misused and exploited by nefarious actors. These harmful actors might include insiders and groups of incredibly driven and creative hackers who attack information systems, one example being hackers. Hackers can be used not only by tech-savvy individuals for petty offences, but also by organized groups with truly bad intentions, such as terrorists (Minal & Apandkar, 2017). One essential digital safeguard for companies, enterprises, and educational institutions is cybersecurity, governments and individuals. Banking and financial institutions are the sectors most in need of cybersecurity (Kshetri, 2019). Cybersecurity is concerned with securing and protecting digital systems, digital equipment, networks, alteration, tampering, disclosure of information, eavesdropping, monitoring, or destruction and information from unauthorized access.

Cyber Security Standards

Security standards defined by NIST, CC, ISO, can be followed for system maintenance and optimization as needed. Manual security and verification for every computer on the entire network is a very laborious task. Network administrators can follow these security standards, manually, to strengthen OS security, and there may be automated tools to verify system-wide integrity that generate reports based on existing configurations. Cybersecurity awareness can influence the adoption of secure behavior online (Maria, 2019) so that it can reduce the number of victims of cybercrime.

Definition of Cybercrime.

Cybercrime is various kinds of illegal access to a data transmission. In other words, cybercrime is an unauthorized activity on a computer system or is included in the category of cybercrime. Cybercrime can also be said to be a crime of abusing internet information technology that is used to attack public data or important private data that is confidential. The target of this cybercrime is a computer connected to the internet network. The development of the internet also develops cybercrime. People who commit fraud and people who take part in fraudulent activities for personal gain are called Scammers.

The cybercrime factor, often described by the crime triangle, is that in order for cybercrime to occur, there must be three factors, namely: victims, motives, and opportunities (Lallie et al., 2021). To reveal news about fraud or other malicious activities are now shared through mobile applications or social media platforms including WeChat, Line, blogs, WhatsApp, and others, which are spread by netizens and their families and friends (Chacng et al., 2018) and also Mobile Banking (Anderson et al., 2012). The more technology develops, the more cybercrime happens (Okutan & Çebi, 2019) because the development of technology has given rise to opportunities for irregularities and criminal activity (Berbasis et al., 2020).

Law on Cybercrime.

In Indonesia, both the public and the government are now concerned about cybercrime, because before this, there was no ITE Law rule that dealt with cybercrime directly, and previously laws were implemented to address the issue of cybercrime related solve the issue. However, now incidents of online crime have been in accordance with ITE Law No. 8 of 2011 regulations, are modifications to the law that followed number 19 of 2016, specifically articles 27 through 30 related to behavior things should be avoided when using the internet. Online criminal activity is difficult to avoid despite the fact that legislation has been passed to control it, Indonesia sees an increase in cybercrime each year do not decrease and continue to increase.

Types of Crime in Cybercrime.

There are several types of crimes in cybercrime that can be classified based on activities such as **(Utama Siahaan, 2018):**

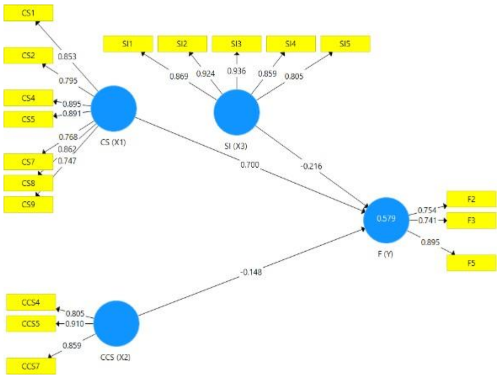
- Unauthorized access, the event that someone infiltrates or enters into without the owner's consent or knowledge, someone may access a computer network system. Instances of these crimes investigating and porting.
- Unlawful Content, which is done information or data by inputting on the internet regarding things that are false, immoral, and is an act that violates the law, such as spreading pornography or untrue news.
- Spread of Viruses. Individuals whose email systems that are contaminated with viruses are unaware of this. Email is typically used to spread this virus.
- Cyberespionage is illegal and includes acts like sabotage and extortion committed by doing done by means of the internet network espionage of others, by going to the target computer system network. Extortion and vandalism are types of crimes committed by deleting or interfering with data, computer programs alternatively, internet-connected computer network architectures.
- The act of carding is illegal. With the intention of stealing using someone else's credit card number and using it for commercial transactions on the Internet to commit fraudulent transactions. The high level of sophistication of the perpetrators so that many fraudulent activities remain undiscovered (Durham et al., 2020).
- Hacking and Cracking. Cracking activities range from hijacking accounts of other individuals, investigations, website hijacking, Virus transmission, to deactivating targets. Does is the most recent action (Denial of Service). A denial-of-service attack (DoS attack) seeks to stop the target from providing services by causing it to hang or crash.
- E-squatting, as well as Typosquating. Attempting to sell a firm's domain name to another corporation for more money is known as "cybersquatting," which is illegal. Making bogus domains with names that are similar to those of others is known as typosquatting.
- Cyber Terrorism, acts of cybercrime including whether cyberterrorism poses a danger either the people or the government, clamping down on the military locations or the government.
- Identity Theft. Identity Theft is a type of fraud where someone pretends to be someone else and commits a crime on behalf of someone else (Komputer, 2015).

III RESEARCH METHODOLOGY

This research is a comparative case study that uses quantitative methods need a thorough comprehension of cybercrime and cyber security. In quantitative the technique of gathering data is used in research rather than statistics by distributing questionnaires and using sampling methods that aim to eliminate the problem of extensive data gathering to create conclusions from the population, such that information collection will be utilizable, easy and affordable. The population in this study is social media users throughout DKI Jakarta and Tangerang from March to August 2022. To assess the study's postulated hypothesis, a causality model was applied in the analysis, SEM is the analytical method employed (Structural Equation). Modeling) that is managed by the AMOS software. Factor analysis and regression analysis are combined in the multivariate statistical method known as SEM (correlation), It seeks to look at how variables in a model relate to one another, be it relating metrics and their constructions, or connections between various constructions. Sampling is intended for 100 users of information technology.

IV RESULTS AND DISCUSSION

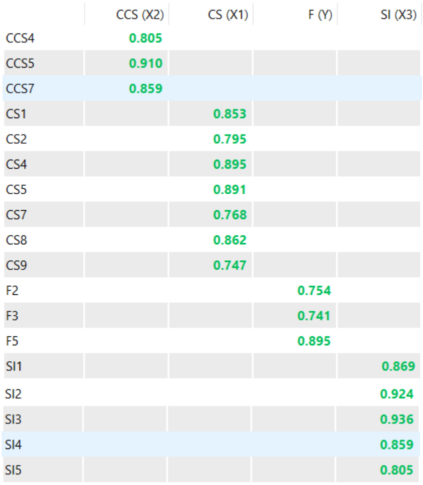
(Table 1. Measurement Model / Outer Model)



source: OutputSmartPLS, 2022

The measurement models on the convergent validity of Reflexive indications are evaluated using the relationship between the construct score determined by PLS and the item score, component score, or both. For specific reflexive measures, it can be being high if it is correlated > 0.70 with respect to the measurement build. Nevertheless, for research that is still creating a measuring scale at a loading factor value of 0.50 – 0.60, it is considered sufficient.

(Table 2. Loading Factor)

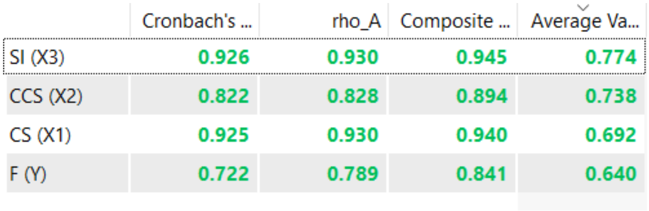


	CCS (X2)	CS (X1)	F (Y)	SI (X3)
CCS4	0.805			
CCS5	0.910			
CCS7	0.859			
CS1		0.853		
CS2		0.795		
CS4		0.895		
CS5		0.891		
CS7		0.768		
CS8		0.862		
CS9		0.747		
F2			0.754	
F3			0.741	
F5			0.895	
SI1				0.869
SI2				0.924
SI3				0.936
SI4				0.859
SI5				0.805

source: OutputSmartPLS, 2022

This study has a loading factor value > 0.70 so it can be declared valid. The first indicator in cybercrime software has 4 indicators, namely CCS4 showing a result of 0.805, CCS5 of 0.910 and CCS7 showing a result of 0.859. The second indicator on cyber security has 7 indicators, namely CS1 showing results of 0.853, CS2 of 0.795, CS4 of 0.895, CS5 of 0.891, CS7 of 0.768, CS8 of 0.862 and CS9 showing results of 0.747. The third indicator of fraud which has 3 indicators, namely F2 shows a result of 0.754, F3 is 0.741 and F5 shows a result of 0.895. The fourth indicator in the information system has 2 indicators, namely SI1 which shows a value of 0.869, SI2 of 0.924, SI3 shows a value of 0.781, SI4 is 0.859 and SI5 shows a result of 0.805.

(Table 3. Average Variance Extracted)

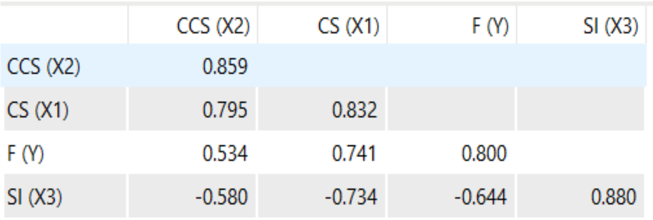


	Cronbach's ...	rho_A	Composite ...	Average Va...
SI (X3)	0.926	0.930	0.945	0.774
CCS (X2)	0.822	0.828	0.894	0.738
CS (X1)	0.925	0.930	0.940	0.692
F (Y)	0.722	0.789	0.841	0.640

source: OutputSmartPLS, 2022

The value of Average Variance Extracted (AVE) for information system variables, cybercrime software, cyber security and fraud > 0.50 which means that each variable has good discriminant validity. In discrimiant validity testing, the commonly used approach is the Fornell-Larcker Criterion (FLC) and Cross Loadings, which are indicators of latent constructs that are expected to be greater than the values of cross loadings on other latent constructs.

(Table 4. Fornell-Larcker Criterion (FLC)

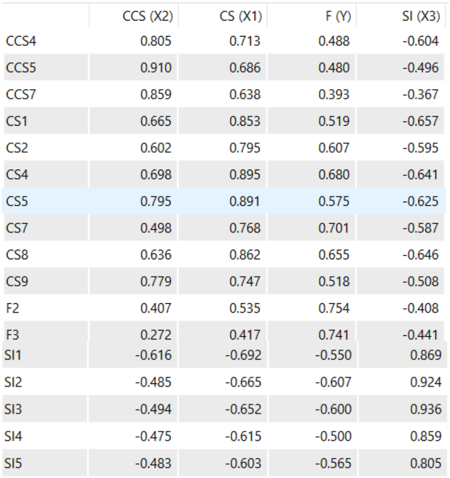


	CCS (X2)	CS (X1)	F (Y)	SI (X3)
CCS (X2)	0.859			
CS (X1)	0.795	0.832		
F (Y)	0.534	0.741	0.800	
SI (X3)	-0.580	-0.734	-0.644	0.880

source: OutputSmartPLS, 2022

The Fornell-Larcker Criterion (FLC) value on the cybercrime software variable has the highest FLC value in the latent construct itself, which is 0.859 compared to the FLC value in other constructs of 0.795, 0.534 and -0.580. The highest FLC latent construct value in cyber security variable is 0.832 and the other construct values are 0.741 and -0.734. The fraud variable has the highest latent construct FLC value of 0.800 and for the FLC value of other constructs it is -0.644. The information system variable has the highest FLC value in its latent construct of 0.880.

(Table 5. Cross Loading)

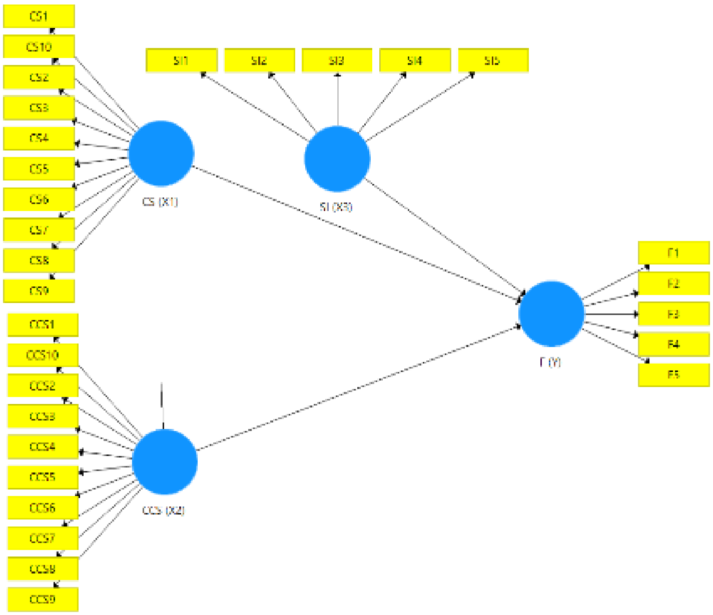


	CCS (X2)	CS (X1)	F (Y)	SI (X3)
CCS4	0.805	0.713	0.488	-0.604
CCS5	0.910	0.686	0.480	-0.496
CCS7	0.859	0.638	0.393	-0.367
CS1	0.665	0.853	0.519	-0.657
CS2	0.602	0.795	0.607	-0.595
CS4	0.698	0.895	0.680	-0.641
CS5	0.795	0.891	0.575	-0.625
CS7	0.498	0.768	0.701	-0.587
CS8	0.636	0.862	0.655	-0.646
CS9	0.779	0.747	0.518	-0.508
F2	0.407	0.535	0.754	-0.408
F3	0.272	0.417	0.741	-0.441
SI1	-0.616	-0.692	-0.550	0.869
SI2	-0.485	-0.665	-0.607	0.924
SI3	-0.494	-0.652	-0.600	0.936
SI4	-0.475	-0.615	-0.500	0.859
SI5	-0.483	-0.603	-0.565	0.805

source: OutputSPSS Versi 25.0, 2020

Considering the table above, it shows the significance of the correlation between the factors and the indicators surpasses the value in value of the relationship with other variables. Therefore, all latent variables have good discriminant validity or indicators in the indicator block of these variables are better than indicators in other blocks.

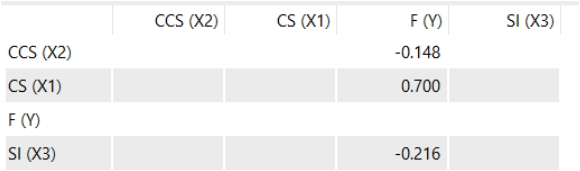
(Table 6. Structural Model / Inner Model)



source: OutputSmartPLS, 2022

Model for structures testing aims to see each endogenous latent variable's R-Square value, which measures the structural model's capacity for prediction.

(Tabel 7. Path Coeffisient)

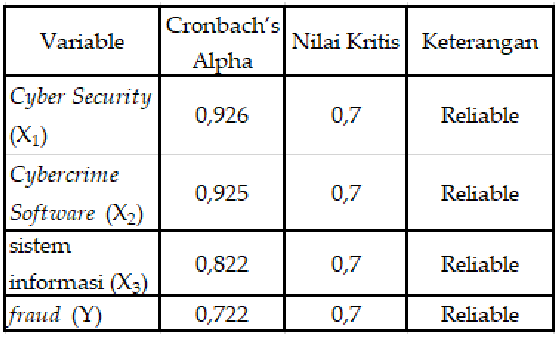


	CCS (X2)	CS (X1)	F (Y)	SI (X3)
CCS (X2)			-0.148	
CS (X1)			0.700	
F (Y)				
SI (X3)			-0.216	

source: OutputSmartPLS, 2022

Cyber security variable (X1) on fraud variable (Y) has a path coefficient worth of 0.700, this implies cyber security has a constructive force on fraud. The cybercrime software variable (X2) has a path coefficient value of -0.148 to the fraud variable (Y), which means that the auditor's experience has a negative influence on fraud. The information system variable (X3) has a path coefficient value of -0.216 against fraud (Y), which means that auditor professionalism has a negative influence on fraud.

(Table 8. Reliability Test Results)

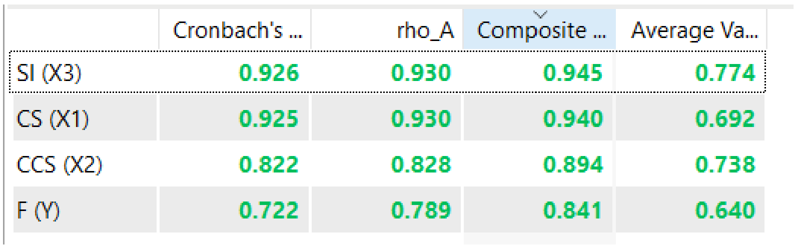


Variable	Cronbach's Alpha	Nilai Kritis	Keterangan
Cyber Security (X_1)	0,926	0,7	Reliable
Cybercrime Software (X_2)	0,925	0,7	Reliable
sistem informasi (X_3)	0,822	0,7	Reliable
fraud (Y)	0,722	0,7	Reliable

source: OutputSmartPLS, 2022

The results of Cronbach's alpha reliability of cyber security instruments are 0.926, cybercrime software is 0.925, information systems are 0.822 and fraud is 0.41. Of the four instruments that have a Cronbach's alpha value > 0.7, namely cyber security, cybercrime software, information systems and fraud which are declared reliable or meet the requirements.

(Table 9. Reliability Test Results)

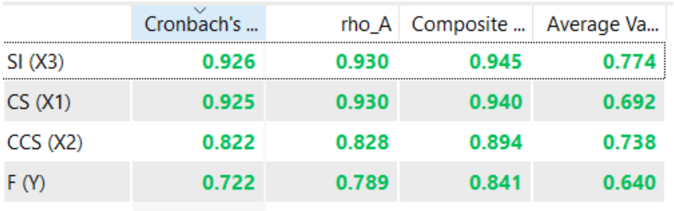


	Cronbach's ...	rho_A	Composite ...	Average Va...
SI (X3)	0.926	0.930	0.945	0.774
CS (X1)	0.925	0.930	0.940	0.692
CCS (X2)	0.822	0.828	0.894	0.738
F (Y)	0.722	0.789	0.841	0.640

source: OutputSmartPLS, 2022

According to the above table, it shows that CR stands for Composite Reliability. for each variable is above 0.700. The information system variable has a CR value of 0.945, cyber security has a CR value of 0.940, cybercrime software has a CR value of 0.894, and fraud has a CR value of 0.841. With the values generated in the Composite Reliability test research, all variables have good reliability and are in accordance with the predetermined minimum value limit.

(Table 10. Cronbach Alpha Results)

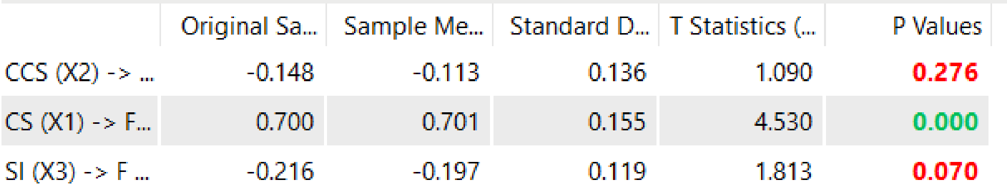


	Cronbach's ...	rho_A	Composite ...	Average Va...
SI (X3)	0.926	0.930	0.945	0.774
CS (X1)	0.925	0.930	0.940	0.692
CCS (X2)	0.822	0.828	0.894	0.738
F (Y)	0.722	0.789	0.841	0.640

source: OutputSmartPLS, 2022

According to the above table, the results show that the Cronbach Alpha (CA) value for the information system variable has a CA value of 0.926 > 0.700, the cyber security auditor variable has a CA value of 0.925 > 0.700, the cybercrime software auditor variable has a CA value of 0.822 > 0.700. , and the fraud auditor variable has a CA value of 0.722 > 0.700, so these four variables have a high level of reliability.

(Table 11. T Test – Statistics / Bootstrapping)

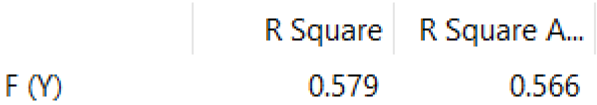


	Original Sa...	Sample Me...	Standard D...	T Statistics (...	P Values
CCS (X2) -> ...	-0.148	-0.113	0.136	1.090	0.276
CS (X1) -> F...	0.700	0.701	0.155	4.530	0.000
SI (X3) -> F ...	-0.216	-0.197	0.119	1.813	0.070

source: OutputSmartPLS, 2022

According to the above table, It is apparent that the cybercrime software variable (X2) has a P-Values value of 0.276 and the information system (X3) has a P-Values value of 0.070 therefore, it may be said that the two factors have no bearing on fraud while the cyber security variable (X3) has a P-Values of 0.000, it can be concluded that cyber security has an influence on fraud.

(Table 12. Determination Test or R – Square / R2)

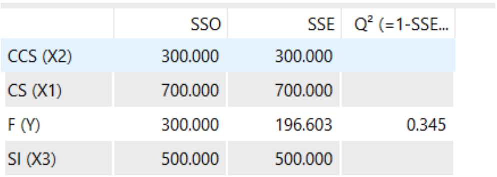


	R Square	R Square A...
F (Y)	0.579	0.566

Sumber: OutputSmartPLS, 2022

According to the above table, the R – Square (R2) value is 0.579 or (57.9%). This demonstrates the percentage of the fraud variable is 57.9% or to put it another way, the variable can be affected by cyber security, cybercrime software and information systems 57.9% while the remaining 42.1% can be Influenced by unresearched additional factors in the study. This. The value of Q - Square in this study is used to determine the goodness of the model, namely the increasing value of Q - Square, the more suitable the structural model with the data. The Q – Square test in this study is as follows.

(Table 13. Construct Cross validated Redundancy Q – Square)

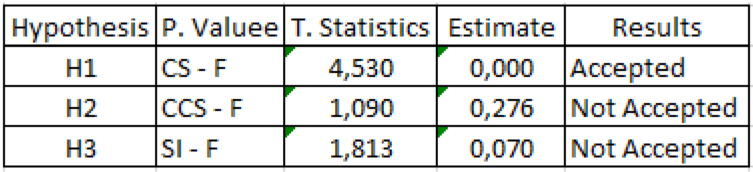


	SSO	SSE	Q² (=1-SSE...
CCS (X2)	300.000	300.000	
CS (X1)	700.000	700.000	
F (Y)	300.000	196.603	0.345
SI (X3)	500.000	500.000	

Sumber: OutputSmartPLS, 2022

The value of Q – Square on the endogenous variable is 0.345, which means that the amount of data diversity described in this research model is 34.5%. While the remaining percentage of 65.5% is clarified by further variables that are in addition to this study model. Therefore, this research model is declared having fulfilled the requirements of goodness (model fit).

(Table 14. Hypothesis Results)



Hypothesis	P. Valuee	T. Statistics	Estimate	Results
H1	CS - F	4,530	0,000	Accepted
H2	CCS - F	1,090	0,276	Not Accepted
H3	SI - F	1,813	0,070	Not Accepted

Sumber: OutputSmartPLS, 2022

The results of data processing carried out to answer the findings from the proposed hypothesis; It is obvious that there are two unacceptable hypotheses and one acceptable hypothesis. This shows that an important difference and no significant impact between the independent and dependent variables.

Effect of Cyber Security on Fraud

According to the findings of hypothesis testing, it is known that the T - Statistics value is 4,530 and the P - Values that form the influence of cyber security on fraud is 0.000 < 0.05, so it can be stated that cyber security has a positive effect on fraud. This shows that lack of knowledge of cyber security can increase fraud in DKI Jakarta and Tangerang.

Effect of Cybercrime Software on Fraud

According to the findings of hypothesis testing, it is known that the T - Statistics value is 1.090 and the P - Values that form the influence of cybercrime software on fraud is 0.276 > 0.05, so it can be stated that cybercrime software has no effect on fraud. This shows that cybercrime software cannot increase fraud on social media users throughout DKI Jakarta and Tangerang.

Effect of Information Systems on Fraud

According to the findings of hypothesis testing, it is known that the value of T – Statistics is 1.813 and the value of P – Values that forms the effect of independence on auditor performance is 0.070 > 0.05, so it can be stated that the information system has no effect on fraud. This shows that not getting education about information systems can increase fraud on social media users throughout DKI Jakarta and Tangerang.

CONCLUSION

Considering the data analysis and discussion results, we might thus say that based on the statistical T-Test hypothesis testing (Bootstrapping) that cyber security has an effect on fraud. Cybercrime software has no effect on fraud and information systems have no effect on fraud in the DKI Jakarta and Tangerang areas. Based on the value of R - Square (R2) of 0.579 or (57.9%). alternatively put, these various factors can affect variables cyber security, cybercrime software and information systems by 57.9% while the remaining 42.1% can be impacted by factors not investigated in this research.

BIBLIOGRAPHY

[1] Adopsi, F. M., Hanum, S., Adawiyah, R. Al, & Sensuse, D. I. (2020). Faktor-faktor yang Memengaruhi Adopsi e-Government (Studi Kasus Adopsi Sistem Informasi di PPATK). 22(1), 19–30.

[2] Anderson, R., Barton, C., Böhme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2012). Mengukur Perubahan Biaya Kejahatan Dunia Maya 2 Kerangka Kerja Kami untuk Menganalisis Biaya Kejahatan Dunia Maya. 1–32.

[3] Asean, S. (n.d.). Kebijakan Keamanan Siber dan Implementasinya di Indonesia.

[4] Berbasis, P., Koziarski, J., & Lee, J. R. (2020). Menghubungkan Bukti-. 0, 1–23. https://doi.org/10.21428/cb6ab371.40515372

[5] Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. Regulation and Governance, 12(1), 101–114. https://doi.org/10.1111/rego.12125

[6] Chouiekh, A., & El Haj, E. H. I. (2018). ConvNets for fraud detection analysis. Procedia Computer Science, 127, 133–138. https://doi.org/10.1016/j.procs.2018.01.107

[7] Deora, R. S., Indrashil, U., Chudasama, D. M., & Indrashil, U. (2021). Studi Singkat Cybercrime di Internet Studi Singkat Cybercrime di Internet. https://doi.org/10.37591/JoCES

[8] Di, K., & Pandemi, M. (2020). Skala Perilaku Kerentanan Keamanan Siber di. 09(November), 395–399.

[9] Durham, P. U., Road, S., & Raya, I. (2020). Literasi Keuangan dan Deteksi Penipuan

∗. 44(0).

[10] Fahlevi, M., Saparudin, M., Maemunah, S., & Irma, D. (2019). Bisnis Cybercrime Digital di Indonesia. 21001, 1–5.

[11] Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop? Crime Science, 7(1). https://doi.org/10.1186/s40163-018-0082-8

[12] Iswardhana, M. R., Cyber, D., & Komunikasi, T. (2021). Diplomasi Cyber Dan Tindakan Perlindungan Terhadap Ancaman Teknologi Komunikasi Informasi Di Indonesia Kata Kunci : Diplomasi Siber , Indonesia , Teknologi Informasi Komunikasi

, Perkembangan teknologi informasi dan komunikasi (TIK) telah terkoneksi den. 2.

[13] Jain, A., & Gupta, N. (2020). Kejahatan dunia maya Anant Jain, Namit Gupta CCSIT, TMU, MORADABAD. 0, 152–158.

[14] Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. Journal of Contemporary Criminal Justice, 37(4), 480–501. https://doi.org/10.1177/10439862211027986

[15] Km, J. K., & Km, J. K. (n.d.). Analisis Aktivitas Kesadaran Pengguna Smartphone. 129(2), 1–6.

[16] Komang, N., Widiasari, N., & Thalib, E. F. (2022). Dampak Perkembangan Teknologi Informasi Terhadap Cybercrime Tarif di Indonesia Abstrak. 1.

[17] Komputer, D. I. (2015). Pentingnya Keamanan Cyber. 7, 14–17.

[18] Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

[19] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, 1–20. https://doi.org/10.1016/j.cose.2021.102248

[20] Male, H., Murniarti, E., Gunawan, R., & Simatupang, M. (2021). Linguistic Manipulation by Scammer as Cyber Crime: Viewed from Law and Education. 14–15. https://doi.org/10.4108/eai.14-4-2021.2312842

[21] Maria, B. A. M. S. dan P. J. R. (2019). Kampanye Kesadaran Keamanan Cyber: Mengapa mereka gagal untuk mengubah perilaku. arXiv: 1901.02672.

[22] Minal, M., & Apandkar, A. (2017). Keamanan cyber. September. https://doi.org/10.1093/hepl/9780198708315.003.0027

[23] Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. Procedia Computer Science, 158, 287–294. https://doi.org/10.1016/j.procs.2019.09.054

[24] Rizqullah, J., Sekolah, S., & Kepolisian, T. I. (2021). Pemolisian dalam Mencegah Penipuan Siber di Indonesia Kebijakan Sosial Pekerjaan Sosial. September 2020, 0–69. https://doi.org/10.13140/RG.2.2.14771.55844

[25] Rock, L., & Rock, L. (n.d.). Perspektif Keamanan Cyber Sosial Keamanan Cyber Sosial sebagai Ilmu Sosial Komputasi. 1–6.

[26] Umanailo, M. C. B., Daulay, P., Meifilina, A., Alamin, T., Fitriana, R., Sutomo, S., & Sulton, A. (n.d.). Kasus Cybercrime Sebagai Dampak Perkembangan Teknologi Komunikasi Yang Meresahkan Masyarakat.

[27] Utama Siahaan, A. P. (2018). Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia. Jurnal Teknik Dan Informatika, 5(1), 6–9.

[28] Wasif, S., Hamdani, A., Abbas, H., Ieee, S. M., Janjua, R., Shahid, W. B. I. N., Amjad, M. F., Ieee, M., Malik, J., Murtaza, H., Nasional, U., Khan, A. W., Nasional, U., & Komputer, I. (2021). Standar Keamanan Siber dalam Konteks Sistem Operasi : Aspek Praktis , Analisis , dan Perbandingan. 54(3).

[29] Yordania, U. A. (2020). Efek Kejahatan Dunia Maya pada Masyarakat Yordania. 12(3).

[30] Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. Journal of Information, Communication and Ethics in Society, 19(4), 446–462. https://doi.org/10.1108/JICES-03-2021-0035