# SINTA 4 Turnitin - CYBER HARDWARE FRAUD IN JAKARTA AND TANGERANG.id.en.pdf

*by* Turnitin .

**Submission date:** 25-Jul-2022 12:17PM (UTC+0900)
**Submission ID:** 1874777002
**File name:** rnitin_-_CYBER_HARDWARE_FRAUD_IN_JAKARTA_AND_TANGERANG.id.en.pdf (640.31K)
**Word count:** 3685
**Character count:** 24051

# CYBERCRIME HARDWARE FRAUD IN JAKARTA AND TANGERANG

**[1*]Zakiandri, 2Kasman, 3Budiandru**

**Postgraduate of Accounting STIE SWADAYA, Jakarta, Indonesia**
**Accounting, University of Muhammadiyah Prof. Dr. HAMKA, Jakarta, Indonesia**
**Email : 1*zakkiandri@gmail.com; 2karsamse86@gmail.com; 3budiandru@uhamka.ac.id**

**Abstract**

*The purpose of this study is to determine Cyber Security, Cyber Hardware, Information Systems against Fraud. The population of this study are users of information technology in Jakarta and Tangerang. This research method is a qualitative method and the type of primary data by collecting questionnaires. Types of primary data are data taken directly from the object of research, using a questionnaire with 103 respondents. While secondary data is data obtained from documents from banks and other sources related to this research. The sampling technique is analysis of the outer model (measurement model) and analysis of the inner model (structural model) using the SmartPLS 3 Multivariate Structural Equation Model (SEM) technique. Partially, the results of this study show that cybersecurity and cyber hardware have a positive effect on fraud. The performance of this research shows that cyber security and cyber hardware have an effect on fraud, so that users or users are more careful in using information technology and always take action. Simultaneously the R-Square value of 0.257 or 25% means cyber security, cyber hardware is influenced by information systems against fraud by 25%. The quantity of this research shows that cyber crime security, hardware will still have an impact on the lack of prudence in the use of technology and information systems.*

***Keywords***: *Cyber Security, Cyber Hardware, Information Systems, Fraud*

## 1. Introduction

The increasingly rapid development of information technology causes very important social, economic and cultural changes (Fahlevi et al., 2019), which offer the same benefits and impacts depending on the users of the information technology (Fahlevi et al., 2019). Anggono & Riskiyadi, 2021). The positive benefit of information technology is that it makes it easier for individuals or groups to carry out their activities, but the negative impact is that individuals or groups use technology for cybercrime that can harm others stemming from abuse (Gani, 2014).

Rapid technological advances have also been accompanied by improvements in security systems to respond to the dramatic increase in cybercriminal activity (Peters et al., Nd). As a result, cybercriminals are becoming increasingly active, quickly creating new breakthroughs in security systems known as cybercrime prevention or cybersecurity. If the perpetrators of cybercrimes are also experts in dealing with cybercrimes, then a very worrying situation arises. As a result, it is difficult to detect and solve new types of cybercrime with cybersecurity. Cybercrime attacks continue to grow rapidly, but cyber security stagnation is a problem that needs to be resolved immediately (Anggono & Riskiyadi, 2021).

Damage caused by cybercrime is difficult to estimate and prove, because in addition to financial loss, damage, loss of personal data or other damage from disclosure can damage the reputation of the company. All countries in the world, especially those that are still developing in the field of information and communication technology, which are marked by a rapid increase in cyber crime, are exposed to cyber crime attacks. The government needs to take proactive steps to prevent cybercrime. This means that the private sector needs to be encouraged to help fight cybercrime by implementing and enforcing cybercrime regulations and strengthening cybersecurity (Falco, 2019).

In the evolution of digital transactions, which are increasingly sophisticated, have complex implications for human life and relations between countries (Lana, 2021). When it comes to cybercrime and high-tech crimes such as cybercrime, the law seems to be behind the scenes (Kaur & Ramkumar, 2021). With the development of the use of the internet, those who have computer skills and have certain goals can use computers and the internet to commit crimes or "mischief" that harms other parties.

The development of information and communication technology has created many breakthroughs. One of them is payment technology, remittance, international remittance or remittance, lending or lending, crowdfunding or crowdfunding, financial intermediary or intermediary, personal investment, financial planning, financial research, and financial services (Das, 2019).

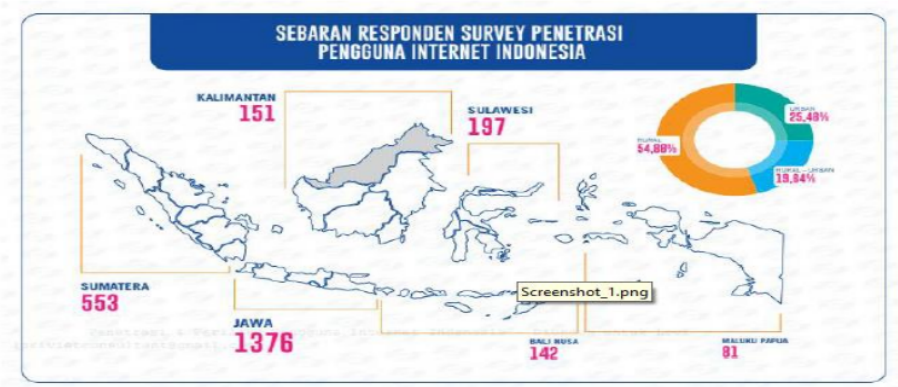
The purpose of this investigation is to identify the investigations carried out so far and provide an overview of the development of information systems against cybercrime, cybersecurity, and fraud. This survey is conducted by selecting, collecting, extracting and analyzing articles according to the survey questions to get results that cover all the selected articles. The results of this study provide an overview of cybercrime and cybersecurity in FinTech. It can be used as a theoretical reference, framework, and research model, providing insight and knowledge about the challenges of cybercrime and cybersecurity predictions, as well as providing opportunities for anti-fraud information systems and future research.

tuberculosis. Ronny R. Nitibaskara defines cybercrime as a crime committed on or on a computer network on the Internet (Sulisrudatin, 2014). But basically, the term cybercrime refers to crimes related to cyberspace and computer-based behavior. In simple terms, cybercrime is a term that refers to criminal activities in which a computer or computer network becomes a tool, target, or location of crime (Hayati, 2021). These include online auction fraud, check fraud, credit card (card) fraud, trust fraud, identity fraud, child pornography, etc. (Mom, 2021).

In Indonesia, regulations regarding electronic information technology are regulated in Law Number 11 of 2008 and Law Number 19 of 2016, which are changes from Law Number 11 of Electronic Information and Transactions (Sadino & Dewi, 2016). In 2018, it was shown that companies can be vulnerable to cyber attacks if they do not take basic security measures to protect their corporate data (Al-gasawneh, 2020).

Indonesia has the highest number of cybercrimes. Police Headquarters has announced losses from criminal banking activities targeting Indonesia's payment system. Cybercrime is a form of crime that occurs through the use of internet technology. In comparison, US computer experts Forester and Morrison describe computer crime as a crime in which the tool/weapon used to commit the crime is a computer (Wang et al., 2021).

**Table 1.1 Data on Internet Usage in Indonesia**




Source :(Fahlevi et al., 2019)

In Indonesia, internet users continue to grow, based on data from APJII (Association of Indonesian Internet Service Providers) in 2018. The number of internet users in Indonesia in 2019 was 132.7 million users or about 51.5 percent of Indonesia's total population of 256.2 million. This is the most important part of the Indonesian population who use this internet technology. Where 65 percent of the island of Java or about 86.3 million people and the lowest in Maluku and Papua 2.5 percent, around 3.3 million people.

The existence of cybercrime has become a threat to stability, so it is difficult for the government to balance the techniques of crime committed with computer technology, especially internet and intranet networks(Karina, 2019). Cybersecurity is now considered an important part of individuals and families, as well as organizations, governments, educational institutions, and businesses. Proper learning about online behavior and system protection results in reduced vulnerabilities and a safer online environment(Zhang & Malacaria, 2021).

*Cybercrime*based on conventional crimes as well as criminal acts and destruction of electronic media(Hamed et al., 2021). In 2018, the Police has handled more than 1,763 cyber crime cases. These include online auction fraud, check forgery, credit card or carding fraud, donfidence fraud, and identity fraud.(Securty, 2014). The objectives of cyber attacks cover four areas, including:(Siber et al., 2020):

a. Loss of integrity
b. Loss of availability
c. Loss of secrecy
d. Physical destruction, and
e. Cheating (Fraud)

**Table 1.2 Security Threat Risk Level**

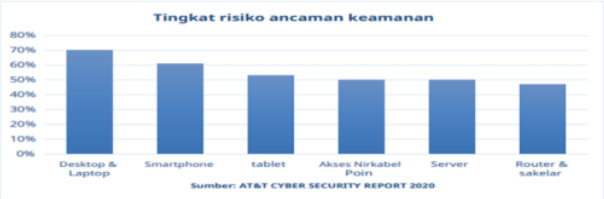



Figure : Table 1.2 Security Threat Risk Level(Surakarta, 2021)

Based on the graph above, it has been noted that countries and companies have spent a lot of money on cybercrime activities. Millions of dollars have been lost throug h cybercrime activities. The researchers would like to use the statistical data below to show the modes of penetration of cybercrime in 2020.

In addition to threats from external companies, there are also possible security threats from internal companies with the potential for fraud. The forms of fraud can be various, even sometimes the fraud does not use technology alone but focuses more on profits to enrich oneself or a group in the form of changes in the presentation of financial statements.(Thaifur et al., 2021). Types of fraud based on group violations are:

a. Employee fraud (fraud), is fraud committed by employees in a working organization
b. Management fraud (fraud), is fraud committed by management using financial state ments or fund transactions for various types of fraud, usually carried out to reduce stakeholder involvement in the organization.

**Table 1.3 Cybercrime Fraud Rate**

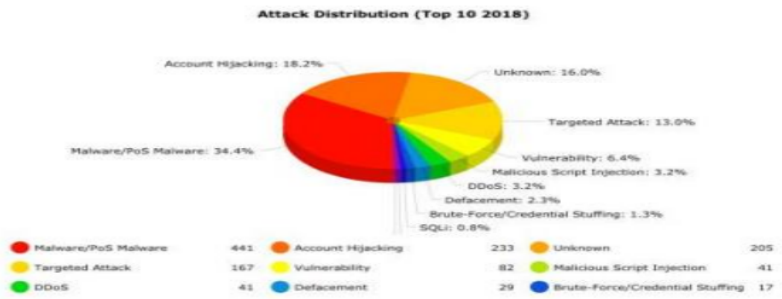



Figure 3: Cybercrime Fraud Rate(Jains & Gupta, 2020)

The picture above is the number of cybercrime frauds recorded during 2020

## 2. Literature review

2.1 Definition of Cyber Crime and Cyber Security

*Cybercrime*is a general term for a crime that attacks computer systems and internet networks for the purpose of data theft, financing, and distribution of malware, and in the field of information and communication technology, it is an illegal act as a modified version of a conventional crime. (Aravazhi, 2020). Cybercrime is an act carried out by

criminals to destroy corporate networks by stealing valuable data and documents, hacking them into bank accounts and transferring them to their accounts.

Investigation of these crimes requires cybercrime, which combines knowledge of criminology, psychology, sociology, computer science, and cybersecurity to gain a deeper understanding of cybercrime (Choi & Lee, 2018). Some of the main factors behind the rapid development of cyber crime are cyber crime tools, methods and media that are very easy to access and learn on the Internet: processing speed, data processing and analysis, Technology is developing rapidly in terms of bandwidth of the Internet and other Internet networks. Access to affordable activity and activity resources or servers.

To proactively fight cybercrime, cybersecurity such as defense measures against all forms of cybercrime and cybercrime remediation measures are needed. Cybersecurity is a means to protect computer systems from attacks and unauthorized access (Kaur & Ramkumar, 2021). With reference to the International Telecommunication Union (ITU), these cybersecurity measures include tools, policies, security concepts, etc. which can be used to protect the organization and user resources (Zheng et al., 2021).

## 2. 2 Definition of Cyber Fraud

Fraud, on the other hand, is a crime committed on a computerized system or internet network with the aim of manipulating financial information to generate maximum profit (Mao et al., 2021). Cyber fraud is a crime committed on a computerized system or internet network and aims to manipulate financial information for maximum profit (Hilal et al., 2022).

Hacking, phishing and malware affect cybersecurity compliance in the financial sector, according to various studies. Since most personal information and credit card data are stored and processed in these applications, cybercriminals prefer to commit crimes in e-commerce and online payment systems (Aravazhi, 2020). Cybercrime remains so unpredictable for e-commerce users that it reduces their trust in e-commerce. According to other studies, the development of e-commerce is hampered by a lack of compliance and weak consumer protection against cybercrime. For this reason, both regulators and business people need to take firm precautions, and the application of the law must continue to follow the evolution of cyber crime (Fahlevi et al., 2019).

## 2. 3 Types of Cyber Crime

### 2. 3. 1 Activity Based Cyber Crime

It can be seen that there are several types of cybercrime when viewed from its activities, namely as follows:(Zheng et al., 2021):

a. Carding usually shop using other people's credit card numbers and identities obtained illegally through data theft on the Internet. The term perpetrator is "carder" or sometimes referred to as cyber fraud, also known as cyberspace fraud.
b. Hacking means breaking into computer programs belonging to other people or parties. Hackers, on the other hand, are people who enjoy hacking computers, have a knack for writing and reading certain programs, and are crazy about security monitoring.
c. Cracking is a hack for a bad purpose. The term "cracker" is a black hat hacker. In contrast to "carders" who only look at credit cards, "crackers" look at customer deposits in various banks and other sensitive data centers for their own benefit. Both

break through other people's computer security, but "hackers" are more focused on the process. Focus crackers enjoy the results.

d. Tampering is the act of changing the website/website of another party, as recently happened to the Minister of Communication and Information Technology, the Golker Party, BI website, and KPU website in the 2004 General Election. Just for fun, to show skills, and to demonstrate the ability to write programs, there are also malicious acts of stealing data and selling it to other parties.
e. Phishing is an activity that aims to trick computer users (users) on the Internet into disclosing information about users' personal information (usernames) and passwords (passwords) on modified websites. Phishing is usually targeted at online banking users. Enter important user data and passwords.
f. E-mail is the unsolicited sending of messages and advertisements by e-mail. Spam is often referred to as bulk or junk email and is also referred to as "junk."
g. Malware is a computer program that looks for software vulnerabilities. Malware is usually created to infiltrate or damage software or operating systems. Malware comes in many types, including viruses, worms, Trojan horses, adware, browser hijackers, and more.

2. 3. 2 Cyber Crime Crimes Based on the Operandi

Meanwhile, the types of cybercrime based on their modus operandi are:(3, 2022 )

1. Unauthorized access to computer systems and services, intrusion A crime committed by illegally interfering with or attacking a computer network system without the per mission or knowledge of the owner of the computer network system.
2. Illegal content is a criminal offense when data or information that is wrong, unethica l, and can be considered illegal or offensive to public order and morals is posted on the Internet. For example, posting fake news or accusations that damage the dignity or self-esteem of others.
3. Data falsification is the crime of tampering with important document data stored as uncredited documents on the Internet.
4. *Cyber Espionage*is a crime that uses the Internet network to carry out spying activities agai nst other parties, by entering the computer network system of the target party.
5. Sabotage and cyber extortion, these crimes are carried out by sabotaging, destroying, or destroying data, computer programs, or computer network systems connected to the Internet. These crimes are usually committed by injecting logic bombs, computer viruses, or certain programs to render data, computer programs, or computer networ k systems unusable.
6. Intellectual property attacks, crimes that target the intellectual property rights of othe rs on the Internet. For example, imitating the appearance of a website that is illegall y owned by someone else, or spreading information found to be someone else's trad e secret on the Internet.
7. Privacy breach. These crimes are usually directed against a person's personal inform ation which is stored in a computerized personal data format and, if known to others , can cause serious or non-
serious harm to the victim, including: B. Credit card number, ATMPIN number.

## 2. 4 Characteristics of Cyber Crime

Based on some literature and practice, cybercrime has several distinctive characters compared to conventional crimes, namely:(Garcia-perez et al., 2022):

a. Such illegal activity without rights takes place online and it is difficult to determine which country has jurisdiction.
b. Actions are performed using any device that has an internet connection
c. These actions result in tangible and intangible losses (time, value, services, money, goods, self-esteem, dignity, confidentiality of information) which tend to be greater than traditional crimes.
d. The culprit is the person who controls the use of the Internet and its applications
e. These actions are often cross-border / cross-border

Crimes that are closely related to the use of technology based primarily on computers and telecommunications networks in some literature and practice can be grouped in several forms.

## 2. 5 Computers as Targets for These Crimes Are Carried Out By Selected Criminal Groups

Unlike crimes that use computers as tools, these crimes require technical knowl edge from the perpetrators. Therefore, as technology develops, so does the nature of cri me. This crime is relatively new in the history of computers and explains how an unpre pared society and the rest of the world can eradicate it. Many of these types of crimes a re committed every day on the Internet. Crimes that primarily target computer networks or devices include(Wall, 2008):

a. computer viruses
b. Denial-of-service attacks
c. Malware (malicious code)
d. Etc

## 2. 6 Computers as Tools

If an individual is the primary target of cybercrime, the computer can be considered a tool rather than a target. These crimes generally lack technical expertise. Human weaknesses are usually abused. It is difficult to take legal action against this variant, as the damage caused is primarily psychological and insignificant. This is a crime that has existed in the offline world for centuries. Before the development of high-tech equipment, fraud and theft existed (Chang, 2012). These same criminals are simply provided with tools that increase the potential for victims and make tracking and arresting more difficult. For crimes using other computer networks:

a. Fraud and theft of personal information (despite the increasing use of hacking and phishing malware and are examples of computer crime "as a target" and "computers as a tool").
b. Information war.
c. Phishing scam.
d. Spam.
e. Pornography, including harassment and threats. Sending email

In some jurisdictions, it is illegal to send large amounts of junk email for comm ercial purposes (spam). Phishing is mainly spread via email. Phishing emails may conta in links to other websites that are affected by the malware. It may also contain links to fake online banking and other websites used to steal personal account information.

## 3. Research Method

3. 1 Research Design

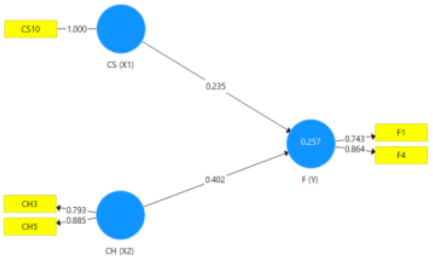
This survey method is a qualitative method and is a type of primary data from a survey collection. Primary data types are data obtained directly from survey subjects using survey methods. Secondary data is data obtained from documents from banks and other sources related to this survey. The sampling technique is analysis of the outer model (measurement model) and analysis of the inner model (structural model) using the SmartPLS 3 Multivariate Structural Equation Model (SEM) technique.

The population in this study are users of information technology in Jakarta and Tangerang. The research was carried out in Jakarta and Tangerang. The research will be carried out from March 2022 to August 2022 with the consideration of getting more appropriate respondents.

## 4. Results and Discussion

4. 1 Hypothesis Testing Results

**(Table 1. Measurement Model / Outer Model)**




Source : OutputSmartPLS, 2022

The measurement model on the convergent validity of the reflexive indicators is assessed based on the relationship between the item score / component score and the construct score calculated by PLS. For individual reflexive measures, it can be said to be high if it is correlated > 0.70 with the construct to be measured. However, for resear ch in the early stages of developing a measurement scale, a loading factor value of 0.50 – 0.60 is considered sufficient.

***(*Table 2. Loading Factor)**

| | CH (X2) | CS (X1) | F (Y) |
|---|---|---|---|
| CH3 | 0.793 | | |
| CH5 | 0.885 | | |
| CS10 | | 1.000 | |
| F1 | | | 0.743 |
| F4 | | | 0.864 |

Source : OutputSmartPLS, 2022

This study has a loading factor value > 0.70 so it can be declared valid. The first indicator on professional ethics there are 2 indicators, namely CH3 showing results of 0.793, CH5 of 0.885. The second indicator on independence has 1 indicator, namely CS10

with a result of 1,000. The third indicator has 2 indicators, namely F1 of 0.743, F4 of 0.864.

**(Table 3. Average Variance Extracted)**

| | Cronbach's ... | rho_A | Composite ... | Average Va... |
|---|---|---|---|---|
| CH (X2) | 0.589 | 0.617 | 0.827 | 0.706 |
| CS (X1) | 1.000 | 1.000 | 1.000 | 1.000 |
| F (Y) | 0.468 | 0.491 | 0.786 | 0.649 |

Source : OutputSmartPLS, 2022

Value of Average Variance Extracted (AVE) variable cyber security, cyber hardware, information systems against 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)**

| | CH (X2) | CS (X1) | F (Y) |
|---|---|---|---|
| CH (X2) | 0.840 | | |
| CS (X1) | 0.212 | 1.000 | |
| F (Y) | 0.452 | 0.320 | 0.806 |

Source : OutputSmartPLS, 2022

The Fornell-Larcker Criterion (FLC) value in the CS variable has the highest FLC value in the latent construct itself, which is 1,000 compared to the FLC value in other constructs of 0.840, 0.806. The highest FLC latent construct value in the CH variable is 0.840. Variable F has the highest FLC value in the latent construct of 0.806.

**(Table 5. Cross Loading)**

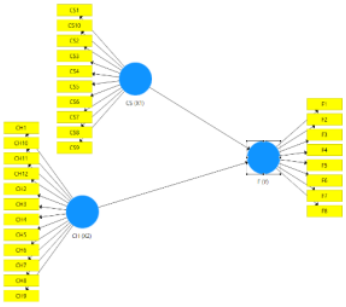
| | CH (X2) | CS (X1) | F (Y) |
|---|---|---|---|
| CH3 | 0.793 | 0.131 | 0.325 |
| CH5 | 0.885 | 0.217 | 0.425 |
| CS10 | 0.212 | 1.000 | 0.320 |
| F1 | 0.354 | 0.143 | 0.743 |
| F4 | 0.377 | 0.349 | 0.864 |

Source : OutputSmartPLS, 2022

Based on the table above, it shows that the value of the relationship between the variables and the indicators is higher than the 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

Structural model testing aims to see the R-Square value for each endogenous latent variable to be the predictive power of the structural model.

**(Table 7. Reliability Test Results)**

| Variable | Crobach's Alpha | Critical Value | Description |
|---|---|---|---|
| Cyber Security | 0,80 | 0,700 | Reliabel |
| Cyber Hardware | 0,79 | 0,700 | Reliabel |
| Fraud | 0,75 | 0,700 | Reliabel |

Source : OutputSmartPLS, 2022

The result of Cronbach's alpha reliability of cyber security instruments is 0.80, cyber hardware is 0.79, and fraud is 0.75. Of the three instruments that have Cronbach's alpha value > 0.7, namely cyber security and cyber hardware which are declared reliable or meet the requirements.

**(Table 8. Path Coefficient)**

| | CH (X2) | CS (X1) | F (Y) |
|---|---|---|---|
| CH (X2) | | | 0.402 |
| CS (X1) | | | 0.235 |
| F (Y) | | | |

Source : OutputSmartPLS, 2022

Cyber Security variable (X1) on Information System and Fraud variable (Y) has a path coefficient value of 0.235, which means that Cyber Security has a positive influence on Information Systems and Fraud. The Cyber Hardware variable (X2) has a path coefficient value of 0.402 on the auditor's performance variable (Y), which means that the auditor's experience has a positive influence on information systems and fraud.

**(Table 9. Reliability Test Results)**

| | Cronbach's ... | rho_A | Composite ... | Average Va... |
|---|---|---|---|---|
| CS (X1) | 1.000 | 1.000 | 1.000 | 1.000 |
| CH (X2) | 0.589 | 0.617 | 0.827 | 0.706 |
| F (Y) | 0.468 | 0.491 | 0.786 | 0.649 |

Source : OutputSmartPLS, 2022

Based on the table above, it shows that the Composite Reliability (CR) value for each variable is above 0.70. The cyber security variable has a CR value of 1,000, cyber hardware has a CR value of 0.827, fraud has a CR value of 0.786. 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... |
|---|---|---|---|---|
| CS (X1) | 1.000 | 1.000 | 1.000 | 1.000 |
| CH (X2) | 0.589 | 0.617 | 0.827 | 0.706 |
| F (Y) | 0.468 | 0.491 | 0.786 | 0.649 |

Source : OutputSmartPLS, 2022

Based on the table above, it shows the results of the study that the Cronbach Alpha . value(CA) for the cyber security variable, which has a CA value of 1,000 > 0.70, this variable has a high level of reliability. The cyber security variable has a CA value of 0.589 < 0.70, the fraud variable has a CA value of 0.468 < 0.70 so it can be interpreted that these three variables have a low level of reliability.

**(Table 11. T-Test – Statistics / Bootstrapping)**

| | Original Sa... | Sample Me... | Standard D... | T Statistics (... | P Values |
|---|---|---|---|---|---|
| CH (X2) -> ... | 0.402 | 0.421 | 0.076 | 5.314 | 0.000 |
| CS (X1) -> F... | 0.235 | 0.230 | 0.084 | 2.796 | 0.005 |

Source : OutputSmartPLS, 2022

Based on the table above, it can be seen that the cyber security variable (X1) has a P-Values value of 0.000, cyber hardware (X2) has a P-Values value of 0.05. It can be concluded that these two variables have an influence on fraud.

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

| | R Square | R Square A... |
|---|---|---|
| F (Y) | 0.257 | 0.242 |

Source : OutputSmartPLS, 2022

Based on the table above, it has obtained an R – Square (R2) value of 0.257 or (26%). This shows that the percentage of the fraud variableby 26% in other words, these

variables can be influenced by cyber security, cyber hardware, information systems by 26% while the remaining 74% can be influenced by other variables not examined in this study. 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.

**(Table 13. Construct Crossvalidated Redundancy Q – Square)**

| | SSO | SSE | $Q^2$ (=1-SSE... |
|---|---|---|---|
| CH (X2) | 200.000 | 200.000 | |
| CS (X1) | 100.000 | 100.000 | |
| F (Y) | 200.000 | 172.874 | 0.136 |

Source : OutputSmartPLS, 2022

The value of Q – Square on the endogenous variable is 0.136, which means that the amount of data diversity described in this research model is 13%. While the remaining 87% percentage is explained by other variables outside the research model. Therefore, this research model is declared to have met the requirements of goodness (model fit).

4. 2 Discussion of Hypothesis Testing Results

**(Table 14. Hypothesis Results)**

| Hypothesis | Statistics table | P. Value | Estimate | Results |
|---|---|---|---|---|
| H1 | C3-F | 2,750 | 0,005 | Received |
| H2 | CH-F | 5,310 | 0,001 | Received |

The results of data processing carried out to answer the results of the proposed hypothesis, it can be seen that there are two acceptable hypotheses. This shows that there is a significant effect between the independent and dependent variables.

4. 2. 1 Effect of Cyber Security on Fraud

Based on the results of hypothesis testing, it is known that the T - Statistics value is 2.796 and the P - Values that form the influence of cyber security on auditor performance is 0.005 < 0.05, so it can be stated that cyber security has an effect on fraud. This shows that cyber security can prevent fraud. This happens because cyber security is able to ward off all kinds of crimes that come from hackers.

4. 2. 2 Effect of Cyber Hardware on Fraud

Based on the results of hypothesis testing, it is known that the T - Statistics value is 5.314 and the P - Values that form the effect of auditor experience on auditor performance is 0.000 < 0.05, so it can be stated that cyber hardware has an effect on fraud. This shows that cyber hardware can prevent fraud. This happens because cyber hardware is able to back up all kinds of viruses that enter the hardware.

## 5. Conclusion

Based on data analysis and discussion results, it can be concluded thatBased on the hypothesis testing Test – T Statistics (Bootstrapping) thatcyber securityaffectfraud, cyber hardware has an effect on fraud. Based on the value of R - Square (R2) of 0.257 or (26%). This shows that the percentage of13variable fraudby 26% in other words13These variables can be influenced by cyber security, cyber hardware, information systems by 26% while the remaining 74% can be influenced by other variables not examined in this study.

# SINTA 4 Turnitin - CYBER HARDWARE FRAUD IN JAKARTA AND TANGERANG.id.en.pdf

ORIGINALITY REPORT

| 10% | 8% | 5% | 3% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | www.ijbel.com<br>Internet Source | 1% |
| 2 | journal.unnes.ac.id<br>Internet Source | 1% |
| 3 | Submitted to Strayer University<br>Student Paper | 1% |
| 4 | iosrjournals.org<br>Internet Source | 1% |
| 5 | Auliya Rahman Isnain, Rahmat Dedi Gunawan, Agung Deni Wahyudi, Suaidah, Dina Caesar Yani. "Analysis of The Effect of Promotion an Technology Acceptance Model on Purchase Interest in Tokopedia", 2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE), 2021<br>Publication | 1% |
| 6 | rjoas.com<br>Internet Source | 1% |

| | | |
|---|---|---|
| 7 | earnmoneycatalog.blogspot.com<br>Internet Source | 1 % |
| 8 | Submitted to University of Southampton<br>Student Paper | 1 % |
| 9 | journal.perbanas.ac.id<br>Internet Source | <1 % |
| 10 | Submitted to Anoka Ramsey Community College<br>Student Paper | <1 % |
| 11 | Ardiansyah, M. Rafi, Pahmi Amri. "Chapter 29 The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia", Springer Science and Business Media LLC, 2022<br>Publication | <1 % |
| 12 | Handayani, P.W., A.N. Hidayanto, A.A. Pinem, I.C. Hapsari, P.I. Sandhyaduhita, and I. Budi. "Acceptance model of a Hospital Information System", International Journal of Medical Informatics, 2017.<br>Publication | <1 % |
| 13 | Pajar Pahrudin. "Cybercrime in the Context of Cellular Telephone Scams", Jurnal Penelitian Pos dan Informatika, 2020<br>Publication | <1 % |
| 14 | 1library.net<br>Internet Source | <1 % |

| | | |
|---|---|---|
| 15 | Ida Hidayanti, Fadhliah M Alhadar. "Marketing Network Collaboration Capability in Improving SME Performance in Ternate City", Society, 2021<br>Publication | <1 % |
| 16 | network.bepress.com<br>Internet Source | <1 % |
| 17 | doaj.org<br>Internet Source | <1 % |
| 18 | Ikram Ullah Khan. "How does culture influence digital banking? A comparative study based on the unified model", Technology in Society, 2022<br>Publication | <1 % |
| 19 | lppm-unissula.com<br>Internet Source | <1 % |
| 20 | newinera.com<br>Internet Source | <1 % |
| 21 | Wenggedes Frensh, Mahmud Mulyadi. "Criminal policy on cyberbullying toward children", E3S Web of Conferences, 2018<br>Publication | <1 % |

| | | | |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | Off | | |