Guidelines on the Prevention of Offenses under Thailand's Computer-Related Crime Act for Industrial Business

RUNGROJ SUBANJUI, SUNEE WATTANAKOMOL, THANIN SILPCHARU
Faculty of Business Administration,
King Mongkut's University of Technology North Bangkok, Rayong Campus,
19 Moo 11 Nongrarok, Bankai, Rayong 21120,
THAILAND

Abstract: - The objective of this research was to develop guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business. This research was conducted both qualitatively and quantitatively. Quantitative data were obtained from a questionnaire survey with 500 IT executives in the industrial sector. The data analysis employed descriptive, inferential, and descriptive statistics. The results found that guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business can be prioritized in all four components as follows: 1) morality ($\overline{X}$ = 4.21), 2) workforce ($\overline{X}$ = 4.18), 3) internal control ($\overline{X}$ = 4.16), and 4) punishment ($\overline{X}$ = 4.14). The hypothesis testing revealed that large, small, and medium-sized industrial businesses gave a significant difference to guidelines for the prevention of offenses under Thailand's computer-related crime act at a statistically significant level of 0.05. The results of the developed structural equation modeling showed that all values were above the evaluation criteria and consistent with the empirical data. The chi-square probability level value was 0.092. The relative chi-square was 1.134. The conformity index was 0.960. The root index of the squared mean of the error estimation was 0.016.

Key-Words: - Thailand's computer-related crime act, prevention guidelines, offenses, industrial business, structural equation modeling.

Received: October 9, 2022. Revised: March 28, 2023. Accepted: April 21, 2023. Published: May 5, 2023.

1 Introduction

In the information age, it is undeniable that the Internet has played a role in daily life and society in many areas. Roles in the field of communication such as interpersonal mediation, negotiation between groups, expressing opinions, and business interests. The Internet has become an important tool to stimulate interest in discussions of public issues, especially, in the midst of conflicting ideas. Hence, the Internet has grown immensely in popularity, and the number of Internet users has increased rapidly, [1]. It is also a new medium where users have the freedom to customize their content and usage patterns. The Thai government must prepare for Internet misuse, which could harm and affect the Thai economy, society, and security, as well as the people's peace and morals. As a result, the Ministry of Digital Economy and Society issued and enforced "Thailand's computer-related crime act" to be able to supervise and control the behavior of people using the Internet more effectively and fairly. Thailand's new computer-related crime act was drafted by the National Legislative Assembly on December 16, 2016, and was published in the Government Gazette on January 23, 2017, entitled "Thailand's computer-related crime act (No. 2) B.E. 2560" (Computer Act B.E. 2560), [2].

The Royal Thai Police, [3], has disclosed the statistics of cases under the Computer Crime Act B.E. 2550 from 2010 to 2016, with a total number of 1,432 cases, of which 531 were arrested and prosecuted. The highest number of cases was in 2016 with 474 cases, followed by the year 2015 with a total of 379 cases.

When the offenses were classified based on the Act, the highest number of cases, 549, was the importation of fake or false computer data (Section 14(1)), followed by 119 cases of the importation of obscene data (Section 14 (4)), 99 cases of importing edited images of others into a computer system (Section 16), and 96 cases of accessing a computer system incorrectly (Section 5). The trend of offenses related to the Computer Act is increasing every year (Fig. 1).

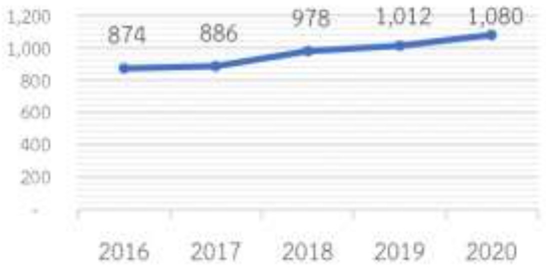

Fig. 1: Statistics of offenses against Thailand's computer-related crime act, [4].

Therefore, the researcher was interested in developing guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business. This is because Thailand's latest computer-related crime act can make industrial business workforces more likely to commit computer-related crimes, either by sharing information, expressing opinions, or ingesting false information on social media. The purpose is to explore preventative guidelines to prevent the workforce in industrial business from committing crimes according to Thailand's computer-related crime act.

1.1 Research Objectives

1) To explore the components of guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business
2) To develop a structural equation model for guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business

2 Literature Review

2.1 Thailand's Computer-Related Crime Act

Thailand's computer-related crime act involves 21 sections. It was enacted to amend Thailand's computer-related crime act, which is intended to impose provisions on offenses and punishments for the culprit or any person who breaks down or does something with the computer system, computer data, or uses a computer system as a tool to commit an offense, [5]. Thailand's computer-related crime act generally refers to crimes in information technology that are different from traditional crimes. At the present, the original offense is somehow related to the computer system, which in turn may not be the type of offense that requires separate theories and principles from the original offense, [6-7]. The same approach has been adopted in Thailand as Thailand's computer-related crime act. It has made certain offenses punishable under existing law. If it is an offense that involves a computer system, it is also a computer-related offense under the meaning of Thailand's computer-related crime act.

To understand the context and differences between traditional and new offenses arising from information technology, they can be summarized in Table 1.

Table 1. Comparison of traditional offenses with Thailand's computer-related crime act, [8].

Traditional offense	Thailand's computer-related crime act
1. There is a common norm and understanding in society about the offense.	1. There is no consistent norm of understanding.
2. Behaviors tend to occur in the present and depend mainly on physical factors.	2. Behavior is not dependent on any moment or suddenness.
3. Most of the behavior takes place in a specific and distinct area.	3. Behaviors are independent of any area. It can be transnational or global behavior. If there are limitations, it depends on internet access and language.
4. Behaviors tend to be associated with offender-based instead of victim- or nature-based offenses.	4. Behaviors tend to be associated with offence-based instead of the offender or the victim.
5. Severe fraud tends to be linked to worker culture.	5. Behaviors cover a wide range of issues and focus on civil law rather than criminal law. It will likely be a white-collar crime.

Wall, [8], described the Internet as a means of committing crime. The Internet has had a significant impact on both social and criminal behavior, particularly modernity's discontinuities for time and space separation. People's behaviors do not depend on the context of the local social environment, and developed knowledge does not longer depend on customs, [9]. Now, it is too early to assess the impact of the Internet on modern behavior; however, at least it can be known that the Internet offers people more freedom, choices, and maximum benefits.

2.2 Concepts and Theories Related to Workforce

Behavior is a response to environmental stimuli through cognitive and learning processes. It can be divided into overt behavior and covert behavior, [10]. This study examined the overt behavior of the workforce in industrial business to identify guidelines on the prevention of offenses under Thailand's computer-related crime act. The study was under the concept of employees' participation in work planning, organizational optimization, a shift from commanding to brainstorming for problem-solving, and creating a win-win situation for both the enterprise and the workforce. The workforce at all levels is an organization's priority. With the full participation of the workforce, it will enable them to use their knowledge and abilities to benefit the organization. In addition, if the workplace is a place full of happiness, employees will be happy and willing to work as well as doing something that benefits the organization and society, [1 1] , and workforce skills are a key factor in driving a business towards its goals, [12]. Several studies revealed that organizational performance entirely depends on the input rendered by the workforce. Committed and highly motivated employees help to improve the growth of any organization. The commitment and general productivity of employees are enhanced by different situational factors at the workplace. Managers or leaders are so influential concerning the behavior and level of commitment exhibited by employees when executing different operations or activities of an organization, [13].

2.3 Concepts and Theories Related to Morality

Morality is a principle and rule of decency in social life. Morality can be divided into individual morality, social morality and mondial morality. Individual morality is an awareness of good principles, which is inward, embedded in humans which will affect the way of thinking and action. Morality arises from within, not by being forced from without. Morality is an attitude of the heart that is revealed in outward actions. Social morality is reflected of individual morality in seeing social reality, namely the way individuals see others as human beings who have the same value and dignity. While morality mondial is morality that is universal and applies anywhere and anytime, related to justice, humanity, independence and so on, [14]. Morality means deciding to do something in moderation. Each person will derive rationality from logic and knowledge (wisdom), as well as a profound understanding from practical expertise. (Option, decision, and action) to be appropriate, [15]. If people can control their minds (souls), inappropriate behavior can be controlled, which is called self-control. When people do not know how to control themselves, they become intoxicated with pleasure and lust, which are considered bad, [16]. Globalization is a phenomenon that increases the likelihood of an offense and spreads beyond the traditional scope of crime. Criminals have a wider range of crimes, which has led to more scrutiny and enforcement of laws that need to be adjusted, [8].

2.4 Concepts and Theories Related to Internal Control

The objectives of internal control in information technology are not different from those of other organizations' internal control. In other words, internal control for information technology is designed for reasonable assurance. It means that the organization will be able to achieve its objectives in terms of effective operation, reliability of financial reporting, and compliance with applicable laws and regulations, [17]. Computer network technology opens the door to new businesses, collaborations, communication channels, and the allure of bait, [8]. A system of internal control is a way to supervise or monitor financial management. With a good internal control system, an organization will be able to operate well. The implementation of the internal control system is integrated into all parts of the company's activities. It is not a separate part of the activity, nor is it added to the activities that have been arranged. This is reflected in the existing components of the internal control system, [18]. Management designs and implements control components to provide reasonable assurance that all activities are controlled to achieve the company's goals, [14].

2.5 Concepts and Theories Related to Punishment

At present, the traditional offense involves a computer system either way, [6]. It may not be the offense that requires separate theories and principles from the original offense, [7]. The same approach has been adopted in Thailand's computer-related crime act, which defines certain types of crimes as acts under existing law. If it's a computer-related crime act, it must be Thailand's computer-related crime act. In addition to the economic and social changes, the Internet has also affected the fundamental concepts of criminal and civil behavior. Moreover, the scope of public law and private law has been changed due to the uncertainty of what behaviors using the Internet or computers are considered offenses under traditional law, [19]. Small offenses were originally not significant enough to carry out the original law, but when they happen on the internet, the perpetrator can take such action against multiple victims. As a result, it has become a criminal behavior that is required by the new law. Cybercrime traces are disappearance of disappearance phenomena, which means every time an electronic transaction takes place, an individual could leave some informational trace that can be tracked and enforced by law, [8].

3 Research Methodology

3.1 Composition Synthesis

From the above concepts and theories, the researcher can summarize guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business into four components: 1) Workforce, due to the workforce's lack of knowledge and understanding of the use of information technology, 2) Morality, due to the organization's lack of inculcation of morality, ethics, and empathy, which makes the workforce misbehave on the Internet, 3) Internal control, as a result of the infringing workplace environment, 4) Punishment because punishment is not so severe or stringent, so people have no fear of wrongdoing. The research conceptual framework is shown in Fig. 2.

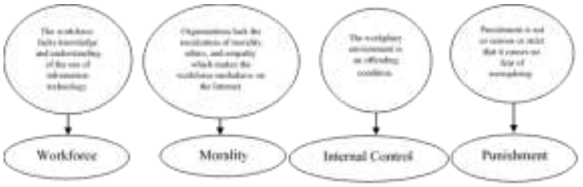
The workforce lacks knowledge and understanding of the use of information technology
Organizations lack the inculcation of morality, ethics, and empathy which makes the workforce misbehave on the Internet
The workplace environment is an offending condition
Punishment is not so serious or strict that it causes no fear of wrongdoing
Workforce
Morality
Internal Control
Punishment

Fig. 2: Conceptual framework

3.2 Population and Sample

The population in this study included 70,410 executives who were responsible for information technology in industrial businesses, [20], which were divided into two types; small and medium businesses (up to 200 workforces) and large businesses (more than 200 workforces). Comrey and Lee determined the size of 500 samples at a very good level, [21]. So, this research was made up of 250 cases from small and medium businesses and 250 cases from large businesses.

3.3 Research Tools

The questionnaire was developed with a 5-point Likert scale to provide an appropriate choice for respondents, [22]. Then, a draft questionnaire was evaluated by five experts with the Index of Item-Objective Congruence (IOC) method. The IOC results ranged from 0.60-1.00, where the optimal value was 0.50 and above, [23]. After that, the questionnaire was tried out with 30 samples, which are like the population. To assess the correlation and reliability, checklist-style questions were analyzed with discrimination, and scale-style questions were analyzed with Standard Deviation (S.D.). The results found that the discrimination was between 0.83-1.44, and the reliability of the entire questionnaire was 0.99, which is greater than 0.9. It can be concluded that reliability was at a very good level, [24]. Finally, the questionnaire was used for collecting data.

3.4 Data Analysis

Data analysis used both descriptive and inferential statistics that were analyzed using SPSS, while a structural equation model was analyzed using AMOS. The evaluating criteria for the data-model fit comprised of 4 values: 1) The chi-square probability was higher than 0.05, 2) The relative chi-square was less than 2.00, 3) The conformity index was higher than 0.90, and 4) The root index of the squared mean of the error estimation was less than 0.08, [25].

4 Results

The results of the important level of each component of the guidelines on the prevention of offenses under the computer-related crime act for industrial business using descriptive statistics found that:

1) For the workforce component, overall, entrepreneurs prioritized the workforce at a high level ($\bar{X} = 4.18$). When considering each item, "encourage the workforce to pursue lifelong learning

behaviors and develop up-to-date IT skills" had the highest value ($\bar{X}$ = 4.34).

2) For the morality component, overall, entrepreneurs prioritized morality at a high level ($\bar{X}$ = 4.21). When considering each item, "support morality instilling in computer ethics" had the highest value ($\bar{X}$ = 4.35).

3) For the internal control component, overall, entrepreneurs prioritized internal control at a high level ($\bar{X}$ = 4.16). When considering each item, "information technology emergencies were tested at least once a year" had the highest value ($\bar{X}$ = 4.28).

4) For the punishment component, overall, entrepreneurs prioritized the punishment at a high level ($\bar{X}$ = 4.14). When considering each item, "determined the level of punishment for the workforce's fear of committing a computer crime" had the highest value ($\bar{X}$ = 4.36).

Table 2. The level of importance when classified by business size

Components	t-value	P-value
The level of importance overall	-1.77	0.08
1. Workforce	-1.20	0.23
2. Morality	-1.56	0.12
3. Internal Control	-1.87	0.06
4. Punishment	-1.86	0.06

Table 2 shows the level of importance of the guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business both overall and for each component. When classified by business size, they were not significantly different at the 0.05 level.

For the model development, the model was improved by considering the modification index values derived from the AMOS with theoretical academic principles to eliminate some improper observational variables one by one, then repeat all processes until a model with all four statistical values (the chi-square probability, the relative chi-square, the conformity index, and the root index of the squared mean of the error estimation) meets the criteria. The results of the structural equation model are as follows:

5) The components of guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business consisted of four components: workforce, morality, internal control, and punishment. All four of those components were derived from the relevant literature review. Therefore, it revealed that the model was consistent with the empirical data with the values of p-value = 0.092, CMIN/DF=1.134, GFI = 0.96, and RMSEA = 0.016 with statistical significance at 0.001 and all values were above the criteria. The observational variables and structural equation model are shown in Table 3 and Fig. 3, respectively.

Table 3. Observational variables

Abbreviation	Description
Workforce	
WKF7	Provide a budget to organize prevention activities against Thailand's computer-related crime act
WKF12	Provide experts to teach the prevention of Thailand's computer-related crime act
WKF15	Promote the IT Code of Conduct in the workforce as a corporate culture
WKF20	Require the employee to log in before every use of the computer and log out after every use
WKF24	Praise for those who follow the rules of the Computer Crime Act and do not create disgrace for the organization
Morality	
MRT5	Executives are responsible and drive good governance.
MRT10	The organization's information operations should be transparent, honest, truthful, and trackable.
MRT17	Develop a collaborative network with external authorities related to morality and ethics.
MRT20	Raising awareness of comments made through online channels that may harm others
MRT22	Encourage the use of copyrighted software.
MRT25	Advertising of products through online channels must not be distorted or exaggerated.
Internal Control	
INC5	Set up a specialized agency with the skills and information needed to keep an eye on and look into Thailand's computer-related crime act.
INC8	Provide new digital tools or devices

Abbreviation	Description
	that increase efficiency in preventing Thailand's computer-related crimes.
INC11	There should be a tracking system for Thailand's computer-related crime act that operates with speed, timeliness, and efficiency.
INC21	Forward information on Thailand's computer-related crime act to the relevant authorities, report any problems encountered, and request guidelines to prevent recidivism
INC24	Adopt AI (artificial intelligence) as a guide for making decisions about how to solve Thailand's computer-related crime act.
INC25	Disclose the results of the investigation to the relevant authorities as a case study and preventive measure in the future.
Punishment	
PNM3	Define the severity of punishment for the workforce to fear computer-related crimes
PNM5	Apply the penalties set out in Thailand's computer-related crime act and prosecute both civilly and criminally
PNM8	Cooperate with government officials to check the information to make sure the organization is running correctly
PNM11	Improved punishment for offenders is needed to keep up with new situations
PNM19	There should be maximum punishment if employees impersonate the agency to commit computer crimes.

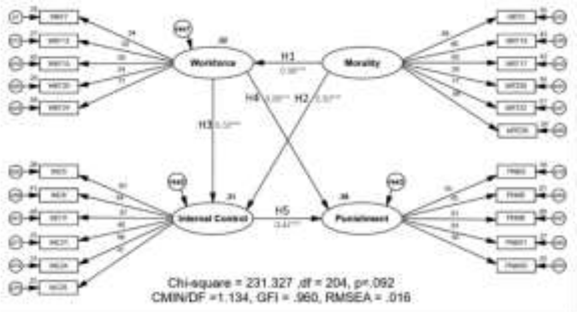
Workforce
Morality
Internal Control
Punishment
H1
H2
H3
H4
H5
Chi-square = 231.327 ,df = 204, p=.092
CMIN/DF =1.134, GFI = .960, RMSEA = .016

Fig. 3: Structural equation modeling

Figure 3 revealed the results of the overall influence of latent variables in the structural equation model of guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business in Standardized Estimate mode. The model consists of four latent variables, one exogenous latent variable (Morality), and three endogenous latent variables (Workforce, internal control, and punishment). Morality had a statistically significant direct influence on the workforce and the internal. The workforce had a statistically significant direct influence on the internal control and the punishment. The internal control had a statistically significant direct influence on the punishment component. The highest weight for overall influence was morality, which influenced the workforce both directly and collectively to the workforce with the standardized regression weight at 0.56.

5 Discussion and Conclusion

The results of the research using descriptive statistics and structural equation model can be concluded that:

1) Morality had a statistically significant direct influence on the workforce component at the 0.001 level. The standardized regression weight was 0.56. It was consistent with McNeely's, [26], research on the political implications for morality on STEM workers. The findings concluded that morality in social identity and behavior affected the performance of science, technology, engineering, and math (STEM) workers. Therefore, developing a STEM workforce is an important consideration for meeting current and future social needs and challenges. Monteverde, [27], studied the future of workforce care, morality flexibility, and health care ethics education, which was to prepare the medical workforce to deal with the stress and fatigue of studying. It was concluded that morality studies demonstrate health care potential. It contributes to the mental and physical health of the medical workforce for better performance. Hader's research, [28], measured employee honesty by examining behavioral traits such as honesty, ethical standards, morality, labor integrity, and management practices. It has been found that supporting morality in words and actions can encourage employees to remain loyal to the organization and retain highly skilled workers who remain more committed and morally responsible.

2) Morality had a statistically significant direct influence on the internal control component at the 0.001 level. The standardized regression weight

was 0.30. It was consistent with Fernandhytia and Muslichah, [29], who studied the effects of internal control on morality and personal ethics on accounting fraud tendencies. In conclusion, increasing personal morality could be achieved by applying the correct morality to daily activities. It could prevent fraudulent accounting practices. It also had a significant negative impact on accounting fraud trends. Kurniawan and Azmi, [30], studied the effects of morality in managing accounting fraud with internal control. The analysis found that executive morality influenced accounting fraud trends. The results revealed that internal control had a significant positive influence on management's relationship with the tendency to commit accounting fraud. Wantanakomol and Silpcharu, [31], summarized the structural equation modeling for anti-corruption guidelines in the industrial business and found that one of the contributing factors to corruption was the ethical factor associated with the individual's morality. A person with low morals and little internal control might be persuaded to commit fraud. A person with a high level of morality, internal control, or non-internal control wouldn't influence the decision to commit fraud. Puspasari and Suwardi, [32], studied the effects of personal morality and internal control on the tendency to commit fraud and found that a person with low morality was more likely to defraud their accounts when they didn't have internal control.

3) The workforce had a statistically significant direct influence on the internal control component at the 0.001 level. The standardized regression weight was 0.32. It was consistent with Kalogiannidis, Kontsas, and Chatzitheodoridis’ research, [33], that confirmed the influence of proper managerial styles on the general productivity of employees in an organization. The results showed that managerial styles are an important part of every organization. Therefore, managers should continuously focus on applying the most appropriate styles that are employee-centered, such as participatory and democratic management styles. This helps to improve employees’ performance and consequently the performance of the whole organization. Do, [34], who said in part of his research on employee health that the personal health of employees played an important role in ensuring the quality of performance. If the employees were unhealthy, there was a weakness in the health of the employee, the internal control would be ineffective. Akhmetshin, Vasilev, Vlasova, Kazakov, Kotova, and Ilyasov, [35], studied improvements in organizational management functions and suggested that to improve the internal control system to be more efficient, personnel management was the key element. Therefore, the organization should be constructed according to the specified functions and integrated into the internal control system. Wilkens, Ruiner, and Küpper, [36], studied flexible management with highly qualified employees and concluded that a knowledge-driven workforce affected effective internal control.

4) The workforce had a statistically significant direct influence on the punishment component at the 0.001 level. The standardized regression weight was 0.28. It was consistent with Berns' research, [37], that found a person with moral order was immune to punishment. Saleilles, [38], said that the principle of appropriate punishment for the offender is to assign appropriate punishment to the offender because people have an unequal capacity to take individual responsibility, and some people should be sentenced or not punished at all. Punishment based on this concept focuses directly on the offender and aims to improve and cultivate the habits of offenders so that they will be good citizens. Punishing the offender for disastrous purposes may be inappropriate and cannot lead to better behavior on the offender's part.

5) Internal control had a statistically significant direct influence on the punishment component at the 0.001 level. The standardized regression weight was 0.44. It was consistent with Kasmawati, Sudarya, and Zakaria's research, [39], which was a survey of an airport employee. The analysis showed that internal control affected both rewards and punishments. The research by Hu, Weng, and Wang, [40], studied the effects of internal control on quality in China and found that companies should disclose management and audit reports on internal control. The goal was to ensure various companies' reliability through reporting because even minor deficiencies in internal control would affect administrative penalties such as fines or lawsuits. Wang, [41], studied the relationship between bank performance and internal control. The research found that the bank's negative performance affected the punishment for the bank's executive directors.

6) The level of importance of the guidelines on the prevention of offenses under Thailand's computer-related crime act for industrial business

when classified by business size was not significantly different at the 0.05 level. It was consistent with research by Kumari, [42], who said that machine learning (ML) is being used by all industries to prevent cybercrime. Over time, it has been shown that ML can solve problems and can be used in industries of all sizes and types based on IT security. It was also in line with research by Williams and Levi, [43], who surveyed European industries of all sizes against the computer-related crime act. It found that all industries prioritized reducing computer crime risk by taking proactive measures aimed at increasing public awareness. Some relevant study can be found in [44].

6 Suggestions

1) Aside from the budget, other factors influence how each organization manages information technology because implementing any information system in the organization can be risky. Therefore, it is important to add information security systems, educate on the prevention and monitoring of unauthorized use of information technology, and take preventive steps to avoid the misuse of information technology by users.

2) Morality and ethics should be instilled at a young age by creating a curriculum or content that fosters morality and ethics among students. It is to calm the mind in order to bring about attitude and awareness, and it is to be absorbed through practice until it becomes a habit. Importantly, it must be done continuously in a good atmosphere. Thus, educational factors should be studied in further research.

3) The current industrial sector lacks comparative data research to implement key guidelines for improving the capacity of organizations to formulate guidelines for the prevention of computer-related crimes. Future research should conduct comparative research on the prevention of other types of computer crimes to develop appropriate and directional guidelines for the long-term prevention of computer crimes.

References:

[1] Thepronglong, W. (2009). *Supervision of the content of political web boards after the promulgation of Thailand's computer-related crime act B.E. 2550. Thesis for Communication Arts, Master of Science, Department of Journalism, Department of Journalism, Faculty of Communication Arts, Chulalongkorn University.*

[2] Ministry of Digital Economy and Society. *computer-related crime act*, 2019, Available at http://www.mdes.go.th, Access on 21 October 2019.

[3] Royal Thai Police. *Statistics of cases according to the* Thailand's computer-related crime act*B.E. 2550 (2010-2016)*, 2019, Available at http://www.hightechcrime.org/public, Access on 21 October 2019.

[4] Office of Planning and Budget. *Statistics of offenses against the* Thailand's computer-related crime act *B.E. 2550 and 2560*, 2021, Available at https://oppb.coj.go.th/th/page/item/index/id/4, Access on 5 November 2021.

[5] Electronic Transactions Development Agency. (2019). *The essence of the Computer Crime Act*, 2019, Available at https://ictlawcenter.etda.or.th/files/files/main-point.pdf, Access on 25 October 2019.

[6] Brenner, S. W. Is there such a thing as 'Virtual Crime'?. *California Criminal Law Review, 4*(1), 2001.

[7] Basu, S., & Jones, R. Indian Information and Technology Act 2000: review of the regulatory powers under the Act. *International Review of Law, Computers & Technology, 19*(2), 2005, pp. 209-230.

[8] Wall, D. S. The Internet as a conduit for criminal activity. *Information technology and the criminal justice system. Pattavina*, 2015, pp. 77-98.

[9] Giddens, A. *The consequences of modernity*. John Wiley & Sons, 2013.

[10] Chanaim, S. *General psychology. 11. Bangkok: Thai Wattana Panich*, 1991.

[11] Maitreesophon, B. Communications for the Industrial Sufficiency Economy Movement (TIS 9999) in fostering morality, ethics and behavior modification at the individual level. *Humanities & Social Sciences, 34*(1), 2017, pp. 147-167.

[12] Wattanakomol, S. & Silpcharu, T. Second-order confirmatory factor analysis of auto parts manufacturing industry management guidelines

for sustainable success. *Uncertain Supply Chain Management, 10*(3), 2022, pp. 905-912.

[13] Tewari, S., Gujarathi, R., & Maduletty, K. Leadership styles and productivity. *Asian Social Science*, *15*(4), 2019, pp. 115-118.

[14] Wahyudi, S., Achmad, T., & Pamungkas, I. D. Village apparatus competence, individual morality, internal control system and whistleblowing system on village fund fraud. *WSEAS Transactions on Environment and Development*, *17*, 2021, pp. 672-84.

[15] Mckeon, R. *The Basic Works of Aristotle : Ethica Nicomachea, tr. W.D. Ross.* New York : Random House, 1931.

[16] Plato. *The Republic.Translated by Alan Bloom*. New York : Basic Book Press, 1968.

[17] Ditkaew, K. The effect of cost management quality on the effectiveness of internal control and reliable decision-making: Evidence from Thai industrial Firms. *Advance in Social Education and Humanities Research, 211*. 10th International RAIS Conference on Social Sciences and Humanities (RAIS 2018), 2020, pp. 60-69.

[18] Mardjono, E. S., & Chen, Y. S. Earning management and the effect characteristics of audit committee, independent commissioners: Evidence from Indonesia. *International Journal of Business and Society*, *21*(2), 2020, pp. 569-587.

[19] Wilton, C. Sony, Cyber Security, and Free Speech: Preserving the First Amendment in the Modern World. *UC Davis Bus. LJ*, *16*, 2015, p. 309.

[20] Department of Industrial Works. *Industrial factory statistics in 2021*, 2021, Available at http://reg3.diw.go.th/webdiw/static-fac/, Access on 30 December 2021.

[21] Silpcharu, T. *Research and statistical analysis with SPSS and AMOS. 18 th edition. Nonthaburi : Business R&D Ordinary Partnership.*, 2020.

[22] Joshi, A., Kale, S., Chandel, S. & Pal, D.K. Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, *7*(4), 2015, p. 396.

[23] Turner, R. C., & Carlson, L. Index of Item Objective Congruence for Multiple Objective Measures. *Unpublished manuscript, University of Arkansas*, 2002.

[24] George, D., & Mallery, P. *SPSS for Windows step by step: A simple guide and reference. 11.0 update* (4th ed.). Boston: Allyn & Bacon, 2003.

[25] Arbuckle, J. L. IBM SPSS Amos user's guide. *Amos Development Corporation*, 2016.

[26] McNeely, C. L. *The Implications of Morality Politics for Effecting Inclusion in the STEM Workforce*, 2021.

[27] Monteverde, S. Caring for tomorrow's workforce: moral resilience and healthcare ethics education. *Nursing ethics, 23*(1), 2016, pp. 104-116.

[28] Hader, R. How do you measure workforce integrity?. *Nursing management, 36*(9), 2005, pp. 32-36.

[29] Fernandhytia, F., & Muslichah, M. The effect of internal control, individual morality and ethical value on accounting fraud tendency. *Media Ekonomi Dan Manajemen, 35*(1), 2020, pp. 112-127.

[30] Kurniawan, P. C., & Azmi, F. The Effect of Management Morality on Accounting Fraud with Internal Control as A Moderating Variable (Study in Pemalang Regency). *Riset Akuntansi dan Keuangan Indonesia*, *4*(2), 2019, pp. 177-185.

[31] Wantanakomol, S. & Silpcharu, T. Strategy for Preventing Corruptions in Industrial Business Organizations with Delphi Technique. *Academy of Strategic Management Journal, 20*(3), 2020.

[32] Puspasari, N., & Suwardi, E. The effect of individual morality and internal control on the propensity to commit fraud: Evidence from local governments. *Journal of Indonesian Economy and Business: JIEB, 31*(2), 2016, p. 208.

[33] Kalogiannidis, S., Kontsas, S., & Chatzitheodoridis, F. Managerial Styles and Employee Performance. An Empirical Study from Bank Sector Employees in Greece. *WSEAS Transactions on Environment and Development*, *17*, 2021, pp. 1234-44.

[34] Do, T. P. The impact of workforce health on earnings quality. *Available at SSRN 3949160, 2021.*

[35] Akhmetshin, E. M., Vasilev, V. L., Vlasova, N. I., Kazakov, A. V., Kotova, X. Y., & Ilyasov, R. H. Improving management functions at an

enterprise: levels of the internal control system. *Calitatea, 20*(171), 2019, pp. 39-43.

[36] Wilkens, U., Ruiner, C., & Küpper, M. Flexible arrangements with the highly qualified workforce: antecedents and effects of different contract policies in knowledge-intensive firms. *Journal of Business Economics*, *8 3* (8), 2013, pp. 837-861.

[37] Berns, W. *For capital punishment: Crime and the morality of the death penalty*. New York : Basic Books, p. 91, 1979.

[38] Saleilles, R. *The individualization of punishment (Vol. 4)*. Little, Brown, 1968.

[39] Kasmawati, K., Sudarya, A., & Zakaria, Z. Effect of Reward and Punishment, Compensation, Leadership, and Workplace Skills on Employee Work Discipline at Mopah Class I Airport Management Unit. *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences*, *4*(4), 2021.

[40] Hu, J., Weng, Y. C., & Wang, F. (2021). The effect of the internal control regulation on reporting quality in China. *Borsa Istanbul Review*, *21*(4), 2021, pp. 394-404.

[41] Wang, T. C. *A study on the relationship between bank performance and internal control through punishment cases of FSC, 2019.*

[42] Kumari, M. Application of Machine Learning and Deep Learning in Cybercrime Prevention—A Study. *Int. J. Trend Res. Dev*, 2019, pp. 1-4.

[43] Williams, M. L., & Levi, M. Cybercrime prevention. In *Handbook of crime prevention and community safety*, pp. 454-469. Routledge, 2017.

[44] Petra Dostálová, Gabriela Králíčková, "Use of the CPTED Methodology (Crime Prevention through Environmental Design) and Fire Protection Principles in the Design of the New Form of Gas Stations and Their Surroundings", WSEAS Transactions on Business and Economics, vol. 19, pp. 2007-2014, 2022.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Rungroj Subanjui carried out the conceptualization, methodology, project admistration, resources, visualization, writing, and editing.
- Sunee Wattanakomol has implemented the methodology, investigation, and review.
- Thanin Silpcharu has implemented the methodology, supervision, and review.

All authors discussed the results and contributed to the manuscript.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflict of interest to declare.