# GUIDELINES FOR THE PROTECTION OF COMPUTER CRIME THREATS IN THE INDUSTRIAL BUSINESS

**Komsan Machim, King Mongkut's University of Technology North Bangkok**
**Tanawat Jariyapoom, King Mongkut's University of Technology North Bangkok**
**Pairat Pornpundejwittaya, King Mongkut's University of Technology North Bangkok**

## ABSTRACT

***Aim:*** *This research investigates the characteristics of industrial business enterprises and develops guidelines for the protection of computer crime threats in the industrial business sector.*

***Methodology:*** *The model was discovered from the findings of both qualitative and quantitative of 500 questionnaires distributed to managers/administrators/ IT system controller of the industrial business public company that in stock market in Thailand. The data were analyzed by descriptive analysis categorized into light and heavy industries, and by Structural Equation Model (SEM) to conduct the model in compatible with the empirical data.*

***Finding:*** *The results reveal that: 1) guidelines for the protection of computer crime threats in the industrial business sector consists of 4 factors i.e. IT Governance, IT security system, IT resource and Security operation center. The managers/administrators/IT system controller gave very high importance on guidelines for the protection of computer crime threats in the industrial business sector at 4.23 on light industry and 4.31 on heavy industry respectively. The analysis of the importance on each aspect shows high importance on guidelines for the protection of computer crime threats in all factors 2) The development of SEM shows that the model fits with the empirical data at the 0.060 Chi-square probability levels, relative Chai-square at 1.177, goodness of fit index at 0.962 and root mean square error of approximation at 0.019. 3) The hypothesis results show the following influencing factors: IT governance has direct influence on IT security system at the statistically significant level of 0.001, security operation center at the statistically significant level of 0.001, and IT resources at the statistically significant level of 0.001. Security operation center has direct influence on IT Security System at the statistically significant level of 0.01 and Security operation center has direct influence on IT resources at the statistically significant level of 0.01.*

***Conclusion:*** *Guidelines for the protection of computer crime threats in the industrial business sector for Thailand comprises five main factors in very high important level on IT security system in industrial business of both light and heavy industries. The factors are ranked according to their important levels referred Linkert's scale as follows: IT governance, IT resource and Security operation center for heavy industries and factors are IT resource, IT governance and Security operation center for light industries in industrial business for Thailand. The evaluation of SEM in protection of computer crime threats in the industrial showed passing the criteria of the model fitting with the empirical data. It was found that Chi-Square Probability Level equaled 0.060, Relative Chai-square was 1.177, Goodness of fit Index was 0.962 and Root Mean Square Error of approximation was 0.019.*

**Keywords:** Simulation Model, Computer Crime, Cyber Security, Cyber Threats Management.

## INTRODUCTION

Nowadays, the advancement of potential technologies and science is playing an important role in driving, guiding and controlling various systems. A variety of information and data is connected through the internet network with computers. These becomes a widespread digital technology in response to the growth of the industrial business sector in terms of the accuracy and speed, and reduces barriers to overcome physical limitations of the business operations (Nsoh, 2015). Digital communication and data transfer are the primary targets of criminals. Data can be stolen from anywhere in the world within a few seconds. Cyber criminals infiltrate computer systems for financial benefits. When computers are connected to the Internet, they are immediately at risk of computer crime threats (Opara & Bell, 2011). Attacks or battlefields are no longer appeared in the cyber world. The cyber world itself can become a battlefield at all times and can increase violence with higher damage costs (Smith, 2017). Data is considered the main target of criminals (Rivard, 2014). In accordance with the cybercrime threats, Thailand is ranked as the number 8 out of 20 countries in the Asia-Pacific region. Therefore, it is urgently necessary to improve and develop certain ways to prevent all cybercrime threats. This study points out the problems and solutions.

Computer crime is a new form of crime occurring along with the development of information society. The crime is mostly based on internet technology which is different from the traditional features in several aspects such as changing from tangible thing into something intangible in the form of electronic data. The crime does not require physical abuse. When looking into the countries in the Asia Pacific region, the cybercrime threat of Malware was found at the highest level (Microsoft Security Intelligence Report, 2017) (Table 1).

**Table 1**
**THE SEQUENCE OF COUNTRIES THAT WERE AT RISK OF COMPUTER CRIME THREATS**

| No. | Country | Average (Q1: 2017) |
|---|---|---|
| 1 | Bangladesh | 26.87 % |
| 2 | Pakistan | 26.30 % |
| 3 | Cambodia | 25.70 % |
| 4 | Indonesia | 24.53 % |
| 5 | Mongolia | 24.23 % |
| 6 | Vietnam | 23.17 % |
| 7 | Nepal | 22.93 % |
| 8 | Thailand | 20.20 % |
| 9 | Philippines | 18.87 % |
| 10 | Sri Lanka | 18.07 % |
| 11 | China | 17.10 % |
| 12 | India | 15.33 % |
| 13 | Malaysia | 12.90 % |
| 14 | Taiwan | 10.67 % |
| 15 | Korea | 9.27 % |
| 16 | Hong Kong | 7.30 % |
| 17 | Singapore | 6.80 % |
| 18 | Australia | 4.50 % |
| 19 | New Zealand | 4.23 % |
| 20 | Japan | 2.20 % |

Note: Microsoft Security Intelligence Report, 2017.

Thailand was at risk of computer crime threats were ranked as the number 8 out of 20 countries in the Asia Pacific region with the percentage of 20.2 and the gap of risk was by 89% far away from Japan which was in the 20th rank. Under the trade phenomena in the digital economy era of Thailand, computer crime threats could be found as the threats in Thailand reported in every years. The rise in computer crime threats were shown in Figure 1.

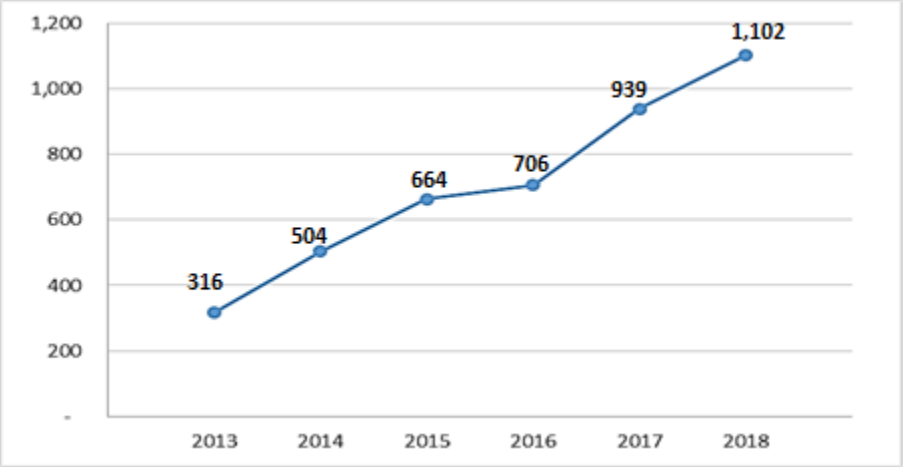


**FIGURE 1**
**STATISTICS OF THREATS BETWEEN 2013 TILL 2019 IN THAILAND**

When looking at the statistics in details, it can be noticed that the average threat rate increased every year between 2013 and 2018. The incidents of the threats had increased to 1,102 times compare to the threats in 2013. These rates were terrifying. The rates had the highly increasing trends overtime. The top 5 threats reported in Thailand are (1) Intrusion Attempts (2) Fraud (3) Intrusions (4) Malicious Code and (5) Information Security (Thailand Computer Emergency Response Team (ThaiCert, 2016), Electronic Transactions Development Agency (Public Organization, 2016). The evolution of computer crime can be due to the advancement of science and technology that causes the sequence of computer crime threats. The sequence of computer crime threats between 1997 and 2017 (InfoSec Institute, 2017). The crime has been spread around along with the growth of computer use. It causes the rise of computer crime threats and enhances the characteristics of cybercrime threats (Jennings, 2014). From the evidence mentioned above, it motivated the researcher of this research to study the ways of protection for computer crime threats in the industrial business sector under the situation of the rapid growth of information technology in the commercial economy of the digital age.

## IT Governance

An information technology management principle that drive the organization by setting information technology policies (Bello, 2016). Separation of duties Compliance with laws, regulations, legislation, computer regulations performs the work on the same basis, participate in work Integrity, fairness, transparency, verifiable (Jerman-Blažič & Tekavčič, 2012), including strict operational procedures in accordance with the policy (Al-Sa'eed et al., 2012) as well as controlling risks and in line with various levels efficiently, quickly and on time (Luftman et al., 2010). IT governance is a guide to better control the use of internal and external data, and

management should enforce IT governance to increase the efficiency of IT systems and risk management (Kooper et al., 2011). Important for management at the highest level of the organization to play a role in determining the behavior for the use and acquisition of IT (Weill & Ross, 2004)

## IT Security System

Protecting computer systems from theft, data loss And detect intruders that are harmful to the system according to information technology standards, set access rights, identity verification (Chenoweth et al., 2007) password setting use the licensed program virus removal program including managing and examining system vulnerabilities filter content that may be a threat collect evidence of connection to IT equipment, search, analyze, and monitor operations for data security and networking (Mukhopadhyay et al., 2011). It is a security system for information systems which has been set up as a policy to ensure the confidentiality, availability, and integrity of information and assets to prevent from hiring, adulteration, management or fraud (Smith & Jamieson, 2006).

## IT Resource

Modern organizations are increasingly exposed to information and strategic information systems. The need to protect important assets plays an important role in helping organizations develop a people-centered safety workplace by raising awareness (Rowley, 1996). Information security, employees and personal responsibility for safety and this research uses social network analysis methods to find out why employees are willing to share advice on information security, found that good security attitudes and participation in daily activities are good results (Dang-Pham et al., 2017). Human Resources are both hardware and software, starting with the screening of personnel, promoting internal and external support create and cultivate habits computer awareness of security awareness. The organization's secret is to promote computer security training (Auster & Choo, 1999). Make an operation manual place the road structure IT to support the growth of the organization (Grembergen & Haes, 2016).

## Security Operation Center

The Safety Operations Center (SOC) is a mid-level technical department that is continuously responsible for monitoring, analyzing, evaluating, and protecting the security positions of the organization. SOC personnel work closely with the incident response team, security analysts, and network engineers. Corporate managers using sophisticated data processing technology such as security analysis the filter threats and importance of assets to ensure that detect and analyze security problems quickly. Those techniques are part of a security strategy that needs to be countered because they rely on human factors, experience, and the judgment of security experts, using complementary technology to assess the risk impact and minimize attack areas (Demertzis et al., 2019).

## Objectives

Objective of this study is to develop simulation model for guidelines for the protection of computer crime threats in the industrial business sector.

## Hypotheses

In the light of the information obtained from the literature review, the research was designed into 5 hypotheses:

*$H_1$ Factor on IT governance has direct influence on IT Security system factor.*

Information technology governance is an important part of the process of creating and maintaining a framework to ensure that information security meets business goals. Applicable regulations achieving this benchmark is the goal of most organizations that need to be within the scope of the *"IT Governance Group of Excellence"* is a significant achievement and a path to a secure and secure network infrastructure (King, 2017). Modern organizations are facing increasing data and strategic information systems. It is necessary to protect these important assets as security-critical, which plays an important role in helping organizations develop (Dang-Pham et al., 2017).

*$H_2$ Factor on IT governance has direct influence on security operation center factor.*

The influence of IT governance forms on security control systems in industrial technology-based businesses is a key factor in the management's decision to monitor the selection of corporate governance modes (Kim & Kim, 2017). However, risk management is a strategic element for businesses that need to be systematically developed to stay current with technology and business innovation to support operational processes and bring technology to help reduce risks (Henry, 2016).

*$H_3$ Factor on IT governance has direct influence on IT resource factor.*

Good governance is of utmost importance and creates stability in controls in order to protect their environment from impacts and information technology security experts must secure data in order to define the best framework for organizations and personnel (Shah, 2017). In addition, information technology security systems are very important in the security of information which requires expertise of IT control measures and intentions of using IT with end users, as well as analyzing the relationship between performance expectations, focusing on user insight (Kassa, 2016)

*$H_4$ Factor on security operation center has direct influence on IT security system factor.*

Data analysis and threat Center are the risk of IT security affects the effectiveness of IT security (Waithe, 2016) and risk management also affects information security, information technology (Anzaldua, 2016).

*$H_5$ Factor on security operation center has direct influence on IT resource factor.*

The center of security or privacy and the efficiency of personal information protection are mostly in electronic form (Boustead, 2016). Nowadays, the use of information technology, computers and networks is becoming more prevalent. The crime of computer crime is increasing with the use of internet, computer, or technology as criminal crime. Including the enforcement of criminal offenses against these offenders in the organization (Wydra, 2015).

## METHODOLOGY

This study was designed as an inductive research with mixed methodology.

1. Qualitative Research using In-depth Interview technique with 9 experts including 3 experts in information technology management business organization managers, 3 experts in Security expert development government department and 3 independent scholars in information technology academic with structured interview in opened-end questions followed the concept of five latents which reviewed from theory and literature. The four latents comprised of 1) IT governance 2) IT security system 3) IT Resource and 4) Security operation center. These variables have been evaluated the index of the corresponding with objective or content using Item Objective Congruence (IOC) analysis that showed 0.60-1.00 value (accepted at >0.5). Finally we obtained the suitable 100 variables in 4 latents for try-out questionnaire that evaluated the reliability from Cronbach's Alpha statistic showed at 0.988 (accepted at >0.8) and discrimination both check-list and rating-scale question items (accepted at >0.3) using Standard Deviation (SD) analysis obtained 0.35-2.44 and Corrected Item-Total Correlation analysis obtained 0.31-0.87 respectively.
2. The quantitative research used questionnaire surveys with managers/administrators/IT system controllers of industrial business public companies in stock market in Thailand. Data was collected a period of seven months from 760 surveys. The 500 samples were selected (Comrey & Lee, 1992) for statistical analysis consist of 250 data by responding to heavy industries and 250 data from light industries. The research tools for quantitative survey questionnaires were. Data analysis was conducted through descriptive statistics by SPSS referred 5 Likert's scales (Tanin, 2020). Multivariate Statistical Analysis employed Structural Equations Model (SEM) by AMOS with evaluating the Data-model Fit in 4 levels including (1) Chi-square Probability Level over 0.05, (2) Relative Chi-square less than 2, (3) Goodness of fit Index over 0.90, and (4) Root Mean Square Error of Approximation less than 0.08.
3. The model of knowledge management strategy in industrial business approved by 7 experts using focus group analysis techniques in qualitative research.

## RESULTS

The results of this research in relation to the factors affecting and the simulation model of the guidelines for the protection of computer crime threats in the industrial business sector were further discussed as follows (Table 2):

**Table 2**
**MEAN AND STANDARD DEVIATION THE GUIDELINES FOR THE PROTECTION OF COMPUTER CRIME THREATS IN THE INDUSTRIAL BUSINESS SECTOR**

| Factors of simulation model of guidelines for the protection of computer crime threats in the industrial business | Heavy industry | | | Light Industry | | |
|---|---|---|---|---|---|---|
| | $\bar{x}$ | S.D. | Significant level | $\bar{x}$ | S.D. | Significant level |
| Overall | 4.29 | 0.38 | High | 4.31 | 0.31 | High |
| 1. IT governance | 4.31 | 0.37 | High | 4.30 | 0.30 | High |
| 2. IT security system | 4.36 | 0.35 | High | 4.32 | 0.35 | High |
| 3. IT Resource | 4.28 | 0.41 | High | 4.31 | 0.33 | High |
| 4. Security operation center | 4.23 | 0.49 | High | 4.30 | 0.39 | High |

1. The IT administrators of both light and heavy industries gave the importance on guidelines for the protection of computer crime threats in the industrial business sector by reporting 4 factors shown in Table 1. Table 1 presents factors in guideline of the protection of computer crime threats industrial business sector showing high importance of both light and heavy industries at 4.31 and 4.31 respectively. When considering in each aspect for heavy industry, the importance is on every factor with the highest on IT security system at 4.36 followed by IT governance at 4.31 then IT resource at 4.28 and Security operation center at 4.23 respectively. For light industry, the IT administrators gave high importance on every factor with highest on IT security system at 4.32 followed by IT resource at

4.31 then IT governance at 4.30 (S.D. = 0.30) and Security operation center at 4.30 (S.D. = 0.39) respectively.

2. The comparison of important level of guideline for the protection of computer crime threats in the industrial business sector between light and heavy industry using independent t-test statistic in SPSS statistical program showed the statistically significant non-difference between mean of factors important level of light and heavy industry.
3. The evaluation of structural equation modelling of the guideline for the protection of computer crime threats in the industrial business sector showed that the Chi-square probability level was at 0.000; relative Chi-square at 3.285, goodness of fit index at 0.553, and root mean square error of approximation at 0.068 which still could not pass the criteria of the SEM.

Thus, the researchers revised the simulation model by considering modification indices suggested by Arbuckle (2011). After the revision of the simulation model, it was found that Chi-Square Probability Level equaled 0.060, Relative Chi-square was 1.177, Goodness of fit Index was 0.962, and Root Mean Square Error of Approximation was 0.019 passing the criteria of the model fitting with the empirical data as shown in Figure 2.

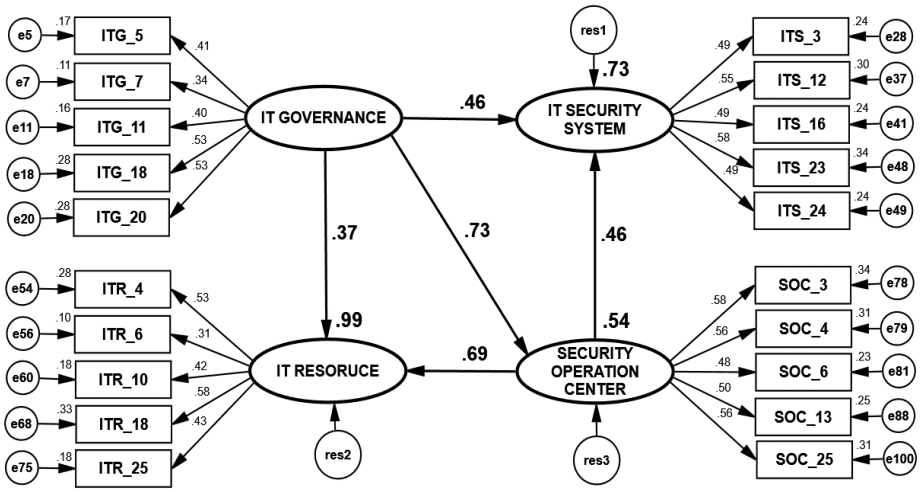


**FIGURE 2**
**GUIDELINES FOR THE PROTECTION OF COMPUTER CRIME THREATS IN THE INDUSTRIAL BUSINESS SECTOR**

From Figure 2, the analysis result of structural equation model of guideline for the protection of computer crime threats in the industrial business sector statistic values were factor loading in standardized estimate mode at hypothesis path analysis. The hypothesis 1 (H1) clarify the influencing factors: IT governance has direct influence on IT security system at the statistically significant level of 0.001 at factor loading 0.46. The hypothesis 2 (H2), clarify the influencing factors: IT governance has direct influence on security operation center at the statistically significant level of 0.001 at factor loading 0.73. The hypothesis 3 (H3), clarify the influencing factors: IT governance had direct influence on IT resource at the statistically significant level of 0.001 at factor loading 0.37. The hypothesis 4 (H4), clarify the influencing factors: security operation center had direct influence on IT security system at the statistically significant level of 0.001 at factor loading 0.46. The hypothesis 5 (H5), clarify the influencing

factors: security operation center had direct influence on IT resource at the statistically significant level of 0.01 at factor loading 0.69. Statistical analysis of structural equation model for guideline for the protection of computer crime threats in the industrial business sector in standardized estimate mode is shown in Figure 2 and summarized in Table 3.

**Table 3**
**STATISTICAL ANALYSIS OF STRUCTURAL EQUATION MODEL FOR GUIDELINES FOR THE PROTECTION OF COMPUTER CRIME THREATS IN THE INDUSTRIAL BUSINESS SECTOR IN STANDARDIZED ESTIMATE MODE**

| Variable | Estimate | | $R^2$ | P |
|---|---|---|---|---|
| | Standard | Unstandardized | | |
| **IT Governance** | | | | |
| IT Security System | 0.46 | 0.53 | 0.73 | *** |
| Security Operation Center | 0.73 | 1.03 | 0.54 | *** |
| IT Resource | 0.37 | 0.48 | 0.99 | 0.004** |
| **Security Operation Center** | | | 0.54 | |
| IT Security System | 0.46 | 0.37 | 0.73 | *** |
| IT Resource | 0.69 | 0.63 | 0.99 | *** |
| **IT Governance** | | | | |
| ITG_5 | 0.41 | 1.00 | 0.17 | |
| ITG_7 | 0.34 | 0.86 | 0.11 | *** |
| ITG_11 | 0.40 | 0.94 | 0.16 | *** |
| ITG_18 | 0.53 | 1.27 | 0.28 | *** |
| ITG_20 | 0.53 | 1.48 | 0.28 | *** |
| **IT Security System** | | | 0.73 | |
| ITS_3 | 0.49 | 1.00 | 0.24 | |
| ITS_12 | 0.55 | 1.32 | 0.30 | *** |
| ITS_16 | 0.49 | 1.05 | 0.24 | *** |
| ITS_23 | 0.58 | 1.29 | 0.34 | *** |
| ITS_24 | 0.49 | 1.19 | 0.24 | *** |
| **IT Resource** | | | 0.99 | |
| ITR_4 | 0.53 | 1.00 | 0.28 | |
| ITR_6 | 0.32 | 0.52 | 0.10 | *** |
| ITR_10 | 0.42 | 0.78 | 0.18 | *** |
| ITR_18 | 0.58 | 1.05 | 0.33 | *** |
| ITR_25 | 0.43 | 0.83 | 0.19 | *** |
| **Security Operation Center** | | | 0.54 | |
| SOC_3 | 0.58 | 1.00 | 0.34 | |
| SOC_4 | 0.56 | 0.98 | 0.31 | *** |
| SOC_6 | 0.48 | 0.82 | 0.23 | *** |
| SOC_13 | 0.50 | 0.90 | 0.25 | *** |
| SOC_25 | 0.56 | 0.95 | 0.31 | *** |

Noted: ***Significant level at 0.001; **Significant level at 0.01

Table 3 represents the estimate regression weight between factors of simulation model. Squared multiple correlations (R2) identify the statistical relation between variables and P-values as a statistical criteria for evaluating the significant level between variables. The results of latent variable analysis on observational variables can be explained as follows;

The factor loading of IT governance factor consists of the 5 sub-factors by following; (1) aware of the impact of information technology on stakeholders (ITG_18) of 0.53, (2) there are channels for communication and listening to information technology (ITG_20) of 0.53, (3) clearly separate the responsibilities of those involved (ITG_5) of 0.41, (4) transparency in

operations (ITG_11) of 0.40, and (5) executives in your organization are involved accountable and drive IT governance (ITG_7) of 0.34.

The factor loading of IT security system factor consists of the 5 sub-factors by following; (1) monitor operations and filter out potentially threatening content (ITS_23) of 0.58, (2) collect evidence, search, analyze, and present digital evidence in forensics tools (ITS_12) of 0.55, (3) application-level computer network security (application-level firewalls) (ITS_3) of 0.49, (4) protecting offline data that doesn't move over the network (ITS_16) of 0.49, and (5) a virtual private network that allows groups of sites to communicate with one another (Virtual Private Network: VPN) (ITS_24) of 0.49.

The factor loading of IT resource factor consists of the 5 sub-factors by following; (1) follow up and review the operational results. (ITR_18) of 0.58, (2) aware of the importance of budgeting in information technology (ITR_4) of 0.53, (3) people who resign from the IT staff organization will backup and check for the deletion of data or taking sensitive company information outside (ITR_25) of 0.43, (4) check software operating system To be ready for work (ITR_10) of 0.42 and (5) do not disclose the confidential information of the organization to third parties. (ITR_6) of 0.32.

The factor loading of security operation center factor consists of the 5 sub-factors by following; (1) the center for receiving complaints or crashes in information technology (SOC_3) of 0.58, (2) backup computer center to prevent data loss to prevent an emergency (SOC_4) of 0.56, (3) aware of the acceptance of information technology security from customers, partners and investors (SOC_25) of 0.56, (4) define a clear list of duties and responsibilities. Phone number used to contact in case of emergency (SOC_13) of 0.50, and (5) always log when accessing the central database (SOC_6) of 0.48.

## DISCUSSION

The organization management approach was an important way to prevent computer crime threats in the industrial business sector in the age of rapid changes of the technological environment and to obtain the long-term success. The results of this research were discussed in five different aspects as follows.

1. The results of the study revealed that when comparing the components of the protection guidelines of computer threats among the SME and large enterprises in overall aspect, it was not statistically significant at the level of .05 in accordance with the research on "*Factors influencing cloud computing adoption in small medium enterprises"*. The conclusion showed the small/medium/large enterprises had limitation of their own customers, the potential of cooperation with service quality, price mechanism, the application of personal, public or hybrid cloud program. Moreover, each organization provided the rights for the IT department to hire the external IT provider for the competitive business (Hassan et al., 2017). It was also consistent with *"Information technology reliability influence on controlling excellence"*. The conclusion showed employees of the organization acknowledged the reliability of the IT department. Therefore, users' experience, private opinions about were extremely important. Having an IT framework did not make the organization big or small. Because almost every organization implemented the IT control as well (Bieńkowska, et al., 2019).
2. The results of hypothesis showed that the IT governance component directly influenced the security center component with standardized regression weight of 0.73. This revealed that empirical data of the IT governance importantly affected the security center. It was important for running the business in accordance with the research on *"Cyber security of critical infrastructures"* which concluded that the updated systems of controlling, monitoring and storing the data were necessary for the of the accountability, management and distribution of the data. In the age of Internet of Things (IoT), the massive, complicated and easily distributed system was developed. Besides the new cybercrime

threats, the modern and low-cost system with high quality of detecting and identifying the threats must be considered. It was implemented for various ways of security. The attacks were severe and dangerous threats for businesses and the nation and it mainly affected the security operation center (SOC) and cyber emergency team (Maglaras et al., 2018). It was also consistent with the research on *"Primary Examiner-Nicholas Ulrich"* which concluded that when connecting the computer with the internet, the security system started to work regarding the control policy and the potential of the protection and computer maintenance. The effective system was important for the organization for computer security check and management. The products of security might include the security tools such as anti-virus tool, anti-malware tool, firewall tool, network tool, artificial security tool, email security tool, etc. Therefore, the dashboard of computer security system was used for the presence of computer outcomes. The dashboard was necessary for the security control center to show the viewpoint of organizational security.

3. The guidelines for the protection of cybercrime or computer crime threats in the industrial business sector for IT security was the highest average of 4.34 indicating the necessity of the IT security in accordance with the research on *"A safety/security risk analysis approach of industrial control systems"*: the industrial risk of cyber security ignorance and the other related risks affecting the system security could course the failure of the systems. Last year, the increasing cybercrime threats attacked several important targets more clearly. Therefore, the safety and security systems were the primary necessity (Abdo et al., 2018). It was also consistent with the research on *"Construction methodology of information security system of banking information in automated banking system":* the security was a form of strategic management of the IT. The system was used to prevent the cybercrime threats to save the bank data. The security system was the fundamental structure of data of both government and private sectors (Hryshchuk et al., 2018)
4. The guidelines for the protection of cybercrime or computer crime threats in the industrial business sector revealed that the IT governance – never violating the rights of others in operations was the highest average of 4.58 in accordance with the research on *"Block chain technology and its relationships to sustainable supply chain management"*: block chain database was transparent and reliable. Accessible data influenced the sustainable supply chain network, situation update and environment effectively. The human rights and performance could be fair, transparent and accountable-never violating the rights to work, controlling sustainable regulations and policy freely and implementing appropriately (Saberi et al., 2019). It was also consistent with the 11th National Conference on communication systems and networks on the topic *"Ensuring Responsible Outcomes from Technology"*, which focused on monitoring projects which the technology developers helped organizations with the confidence of responsibility, regulations and rights (Seth, 2019).
5. The results of relation analysis between the variables of the guidelines for the protection of cybercrime or computer crime threats in the industrial business sector revealed that the variables of relationships between monitoring performance and threats of text /information and the variables of virtual private network (VPN) allowing the sites to communicate with one another were at the highest level of .370 in accordance with the research on *"Classification of abusive comments in social media using deep learning"*, which concluded that behavior of hatred, impolite language, cyberbullying and private threats-it was necessary to sensor the inappropriate opinions and record the inappropriate websites and enhance the safety for the users. Therefore, it was necessary to classify and screen the contents causing the violence and threat (Anand & Eswari, 2019). And it was also consistent with the research on *"Detecting toxic content online and the effect of training data on classification conformance"*, which concluded that the detection of information threats or the classification of information threats, pornography and virus. Therefore, the effective detection was vital for the performance of organizations (Zhao et al., 2019).

## CONCLUSION

This research provided new knowledge from applying a mixed research method including a qualitative research with in-depth interview techniques, quantitative research with questionnaires and qualitative research with focus group discussions. The objectives of this study were: 1) to study the general operation of industrial businesses that focused on the prevention of computer crime threats, 2) to study the component of guidelines of protection for computer crime

threats in the industrial business sectors, and 3) to develop a structural equation model for guidelines on computer crime prevention in the industrial business sector. Population used in qualitative research with in-depth interview techniques were the experts who met the inclusion criteria and their qualifications must be clearly specified. For this method, there were a total of 9 experts included in this study. Moreover, respondents including both quantitative and quantitative research were those who were responsible for information technology systems in industrial business sector. The researchers then determined the sample size by using the research criteria for analysis of components or structural equation model which specified a very good sample size of 500 samples.

Therefore, the guidelines of protection for cybercrime or computer crime threats in the industrial sector is important in terms of the competitive advantage to industrial business sector.

## Suggestion for Further Study

The IT resource is the key to success of protection for computer crime threats in the industrial sector in the organization which is the most important discovery in this study. IT resources are important to driving IT security to achieve its goals, but new knowledge is also important. Therefore, senior leaders of the organization need to focus to attend in over countries seminars to bring knowledge back to apply and develop ways to prevent computer crime threats. The researchers recommend studying the attitude of senior management towards information technology system and a system to focus on threats.

## REFERENCES

Abdo, H., Kaouk, M., Flaus, J.M., & Masse, F. (2018). A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. *Computers & Security*, *72*, 175-195.

Al-Sa'eed, M.T.A., Al-Mahamid, S.M., & Al-Sayyed, R.M. (2012). The impact of control objectives of information and related technology (cobit) domain on information criteria and information technology resources. *Journal of Theoretical & Applied Information Technology*, *45*(1), 9-18

Anand, M., & Eswari, R. (2019). Classification of abusive comments in social media using deep learning. In *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*

Anzaldua Jr, R. (2016). *Does information security training change hispanic students' attitudes toward the perception of risk in the management of data security*. Northcentral University.

Auster, E., & Choo, C.W. (1999). Managing information for the competitive edge. New York: Neal-Schuman, 1996.

Bello, L. (2016). Re: duplication of corporate governance codes and the dilemma of firms with dual regulatory jurisdictions. *Corporate Governance*.

Bieńkowska, A., Tworek, K., & Zabłocka-Kluczka, A. (2019). Information technology reliability influence on controlling excellence. *International Journal of Digital Accounting Research*, *19*, 1-28.

Boustead, A.E. (2016). *Police, process, and privacy*. Unpublished doctoral dissertation, Pardee Rand Graduate School.

Chenoweth, T., Minch, R., & Tabor, S. (2007). Expanding views of technology acceptance: seeking factors explaining security control adoption. *AMCIS 2007 Proceedings*, 321.

Comrey, A.L., & Lee, H.B. (1992). A first course in factor analysis. 2nd Edn. Hillsdale, NJ: L.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, *67*, 196-206.

Demertzis, K., Tziritas, N., Kikiras, P., Sanchez, S.L., & Iliadis, L. (2019). The next generation cognitive security operations center: adaptive analytic lambda architecture for efficient defense against adversarial attacks. *Big Data and Cognitive Computing*, *3*(1), 6.

Grembergen, W.V., & Haes, S.D. (2016). Introduction to the IT governance and its mechanisms minitrack. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)*.

Hassan, H., Nasir, M.H.M., Khairudin, N., & Adon, I. (2017). Factors Influencing Cloud Computing Adoption in Small Medium Enterprises. *Journal of Information and Communication Technology*, *16*(1), 21-41.

Henry, M. (2016). *Exploring information technology: Why the use of information technology governance negatively influences revenue performance*. Unpublished doctoral dissertation, Capella University.

Hryshchuk, R., Yevseiev, S., & Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems.

InfoSec Institute. (2017). *Evolution in the World of Cyber Crime*. Retrieved on 28 June 2016 from http://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/

Jennings, K.W. (2014). Who are computer criminals?.

Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management*, *48*(6), 1031-1052.

Kassa, W. (2016). *Information technology security professionals' knowledge and use intention based on UTAUT model*. Unpublished doctoral dissertation, Capella University.

Kim, H.J., & Kim, B.K. (2017). Risk-based perspective on the choice of alliance governance in high-tech industries. *Journal of Management and Organization*, *23*(5), 671.

King, K.E. (2017). *Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management*. Unpublished doctoral dissertation, Capella University.

Kooper, M.N., Maes, R., & Lindgreen, E.R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International journal of Information Management*, *31*(3), 195-200.

Luftman, J., Ben-Zvi, T., Dwivedi, R., & Rigoni, E.H. (2010). IT Governance: An alignment maturity perspective. *International Journal of IT/Business Alignment and Governance (IJITBAG)*, *1*(2), 13-25.

Maglaras, L.A., Kim, K.H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., Maglaras, A., & Cruz, T.J. (2018). Cyber security of critical infrastructures. *Ict Express*, *4*(1), 42-45.

*Microsoft Security Intelligence Report* (2017). Retrieved from https://www.microsoft.com/thailand/piracy/cybercrime.aspx

Mukhopadhyay, I., Chakraborty, M., & Chakrabarti, S. (2011). A comparative study of related technologies of intrusion detection & prevention systems. *Journal of Information Security*, *2*(01), 28-38.

Nsoh, M.W. (2015). Information security systems policy violation: An analysis of management employee interpersonal relationship and the impact on deterrence. Unpublished doctoral dissertation, Colorado Technical University.

Opara, E.U., & Bell, R.L. (2011). The relative frequency of reported cases by information technology professionals of breaches on security defenses. *International Journal of Global Management Studies Professional*, *3*(2), 15-28

Rivard, J.P. (2014). *Cybercrime: The creation and exploration of a model*. Unpublished doctoral dissertation, University of Phoenix.

Rowley, J. (1996). *The basics of information systems*. Facet Publishing.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117-2135.

Seth, A. (2019). Ensuring responsible outcomes from technology. In *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*. IEEE.

Shah, A. (2017). Determination of ISRA framework using delphi methodology for small and midsized enterprises. *ProQuest LLC*.

Smith, B. (2017). Analytic, intelligence & response. *RSA Conference 2017*. Retrieved on 5 August 2018 form https://www.etda.or.th/publishing-detail/rsa-conference-2017.html

Smith, S., & Jamieson, R. (2006). Determining key factors in e-government information system security. *Information Systems Management*, *23*(2), 23-32.

Tanin, S. (2017). Research and statistics analysis by SPSS and AMOS. *SR Printing Mass Product*.

ThaiCert- Thailand Computer Emergency Response Team. (2016). https://www.thaicert.or.th/statistics/statistics-en2016.html

Waithe, E. (2016). *An analysis of enterprise risk management and IT effectiveness constructs*. Unpublished doctoral dissertation, Capella University.

Weill, P., & Ross, J.W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Wydra, C.A. (2015). *The evolution of criminal procedure for law enforcement in western pennsylvania and northern west virginia with the emphasis on cybercrime*. Unpublished doctoral dissertation, Robert Morris University.

Zhao, Z., Zhang, Z., & Hopfgartner, F. (2019). *Detecting toxic content online and the effect of training data on classification performance*. EasyChair.