ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 3, pp. 191-204
DOI:10.33168/JSMS.2022.0412

Security Risk Analysis for Information Asset

Muhammad Afif Fathullah, Anusuyah Subbarao

Faculty of Management, Multimedia University, Cyberjaya, Malaysia

anusuyah.subbarao@mmu.edu.my

Abstract. Information in its multitude of forms has been recognized as 'Information Asset'. Protecting information asset is a vital importance to an organization nowadays as it has become a key asset in any organization. As such securities to avoid the damage and leakage for information asset are vital. The best method to do this is applying a security risk model. The aim of this research is to find the prevalent risks that affect Intellectual Property (IP) and their corresponding threats, consequences, and probabilities. The research design used is the qualitative method, this is as information asset and security risk analysis are experts' fields it is imperative to have an in-depth discussion with the experts in these fields. This research will show the risks that have been found from the semi-structured interviews conducted and their corresponding threats, consequences, and probabilities. However, more research is warranted to get the views of other parties that are involved in IP such as IP Lawyers to get their perspectives and inputs.

Keywords: risk analysis, risk management, information asset, intellectual property, qualitative interview

1. Introduction

Information in its multitude of forms has been recognized as an asset to an organization nowadays comes to be established as “Information Asset” (Eachempati, 2017). These are bodies of information, defined and managed as a single unit so it can be understood, shared, protected and utilized efficiently (Rouse, 2013). As such, its importance has become more vital to most organization nowadays and has become a key asset in organization as we are in this technological age with the emergence of industrial revolution 4.0. As Information Technology evolves dramatically, new trends, such as Cloud computing, big data, Internet of Things has become more and more popular and been applied widely in to organizations. There are several key risk areas and threat to information asset such as change and decentralization of usage, depreciation, and organization footprints, as such there is a need for organizations to do security risk analysis on their information assets so that it can be analyze and any gaps in their protection can be found.

Information asset are not constant and tend to have short lifecycles Eachempati (2017) such as in the case of IP. As innovations are constant in this age, there will always be new products and there will be more intellectual properties. This is as even a new design can be filed as a new intellectual property. As such there will always be new information that needs to be added or remove.

Information asset can be classified based on their risk assessment and business impact analysis. There are multiple types on information such as intellectual property, organization information, and etc. Depreciation is a factor in an information asset based on the classification and category of information the asset represents, how accurate the information can remain over time (Eachempati, 2017). Information value increases in a direct relationship to the number of people who need the information in question.

A portion of information that an organization carries will leave an organization footprint which is a very important area that must be kept protected. This is as competitors can follow these footprints and hence an organization must preserve this information from the public domain.

This has increased the amount of information assets and thus has expended the range of the risks associated with these assets. Inevitably, this have given rise to new challenges to information assets protection such as piracy and IP infringement Hanafi et.al (2021) which has created a pressing need to establish a systematic security risk analysis for valuable information in an organization and to prepare countermeasures for contingencies that may happen.

In the field of information security, a lot of methods have been created to assess, control and mitigate their information assets to minimize information security risks such as the Conflicting Incentives Risk Analysis (CIRA), Information Security Risk Analysis Method (ISRAM), and etc. However, with the rapid evolution of technology

in the industrial revolution 4.0, unforeseen and unknown risks have emerged and can be found anywhere in an organization, no matter the field. This has created unseen gaps that haven't been seen before which has affected the security risk analysis of an information asset.

Information assets have financial value to all organization in the world. Management of business processes to use information system is a primary objective of any organization. This is as management of information asset such as IP is critical for an organization to sustain competitive advantage (Grimaldi et al., 2021). As such, as a key asset, reducing the risk of information compromise in an information asset is a high priority that must be secured by any organization. The best method to do this is by applying a security risk model that is relevant to the related information asset. The information system must satisfy the security purpose of confidentiality, integrity, availability, authentication, authorization, and non-repudiation in order to assure appropriate functioning of the business processes (Agrawal, 2017). The ultimate output to be gained from this paper is to pinpoint and analyze the risk factors that are related towards IP such as the threats, vulnerability, risk and consequences related to the information asset.

This paper will first discuss the related work in section 2. This is followed by a discussion of materials and methods used in this research in section 3. Followed by, the results and discussion of this research in section 4 and 5. Finally, the conclusion of this research is conferred is section 6.

2. Related Work

2.1. Information asset

According to Rouse (2013) "An Information Asset is a body of knowledge that is organized and managed as a single entity". Agrawal (2017) meanwhile says that "Information Asset is a broad expression and is in a perpetual cycle of change". Investopedia definition of an information asset is "organized information that is valuable and easily accessible to those who need it".

This is to say that information asset at its core is an asset that compromises of all forms of knowledge that are constantly evolving and progressing. It is also something that has value and that value is evaluated based on who needs it, how it can be use, and who has it

2.2. Benefit of information asset

The benefit of an information asset depends on its value as there are various categories of information asset. Batini et al., (2018) describe that "Information value has to be interpreted in terms of determinants such as information capacity, information utility, and the cost related to the design and maintenance of technologies adopted in information management initiatives".

As such some assessment have to be carried out to discover the value of an information asset. Their benefit can be small or tremendous to a person or organization. An example of an information asset that can have tremendous value is an IP for a smartphone design. This information asset can amass a sizable fortune for its owner if used correctly.

2.3. Information asset challenges

Information asset possesses challenges that are related to its quality and also in the context of its protection. According to Batini et al., (2018) "the higher the accuracy of information, the higher its usefulness and value" which is why the four dimensions of accuracy, completeness, currency and consistency must be evaluated to ensure the information asset quality.

According to Agrawal (2017) "reducing the risk of information compromise is a high priority" as such the protection given to an information asset must be substantial enough to avoid a compromise. This is challenge that must be faced by an information asset owner. This is as the owner has a stake in ensuring that the information asset is not compromised and its value is sustained in its lifecycle.

2.4. Information security risk analysis

Agrawal (2017) describe information security risk analysis as "the basis of information protection, risk management, and risk in the process of information management". While according to Business Dictionary security risk analysis refers to as a way to "find the inefficient place and providing improvement guidance to commissioner, thus enhance the information security defense". Eachempati (2017) meanwhile says that when an organization or person does an information security risk analysis they must "weigh how much to spend protecting each asset against cost of losing the asset".

The groundwork of the protection and risk management for information asset subsist of information security risk. It is done to find the feeble point of an information asset, providing guidance to the user and owner which will ultimately enhance the security of the information asset. When a security risk analysis is done, the funds spend must also be based on the information asset value as to make sure resources are spend on the right places.

2.5. Risk and threat

According to Market Business News risk in definition means "A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action". This means that risk though unavoidable in any category of information asset is something that can be mitigated by taking pre-emptive action.

Miller and Gregory (2016) define threats as "Any natural or man-made circumstances or event that could have an adverse or undesirable impact, minor or major, on an organizational asset". That is to say threats are circumstances or event that may affect and have an undesirable effect towards an information asset which is something that all information assets have both seen and unseen.

2.6. Risk classification

According to Business Dictionary the definition of a risk classification is "Grouping of different risks according to their estimated cost or likely impact, likelihood of occurrence and countermeasures required". This is to say that not all risk is equal and some have higher consequences and likelihood of happening than others.

Table 1 shows the levels of impact (consequences) while Table 2 shows the levels of likelihood and lastly Table 3 shows the level of risk. The formula for risk is likelihood x consequences. As such per the formula, the higher the likelihood of a risk happening and the bigger consequence of a risk are the factors taken into consideration when determining a risk classification of an information asset. An example would be a risk with an insignificant impact and rare likelihood can be classified with a low risk level. The purpose of Table 1 and 2 is to show the degree of likelihoods and consequences. Meanwhile Table 3 is to show the risk levels.

Table 1: Levels of impact (Consequences).

Levels Of Impact (Consequences)	
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Catastrophic

Table 2: Level of likelihood.

Levels Of Likelihood	
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

Table 3: Risk level.

Risk Level	
1	Low
2	Moderate
3	Significant
4	High
5	Extreme

2.7. Models and methods in information security risk analysis

There are various models and methods that are used for Security Risk Analysis. The security risk analysis models that are going to be discussed in this research are the CORAS security risk analysis method, IS Risk Analysis Based on Business Model (IS), and The Information Security Risk Analysis Method (ISRAM) method.

2.7.1. CORAS

According to den Braber (2007); Lund (2011) "CORAS are a model-based method for operating security risk analysis". Aegedal et al., (2002) describes CORAS as a qualitative approach to address information security risk. Agrawal (2017) characterize that one of the main aspirations of "CORAS is to establish a framework that employ approach for risk analysis, semi-formal methods for object orienting modelling and computerized tools for definite, unambiguous and efficient risk appraisal of security critical system". There are eight steps in this method. The CORAS model is shown in Figure 1.

Figure 1 depicts that in the ontology of CORAS that asset has value. Threat has intent and source, exploit vulnerability, leads to risk, which will ultimately affect asset. The target contains asset and has security specification which leads to security guidelines that conclusively reduces vulnerability. Vulnerability leads to risk which incorporate consequences and likelihood.

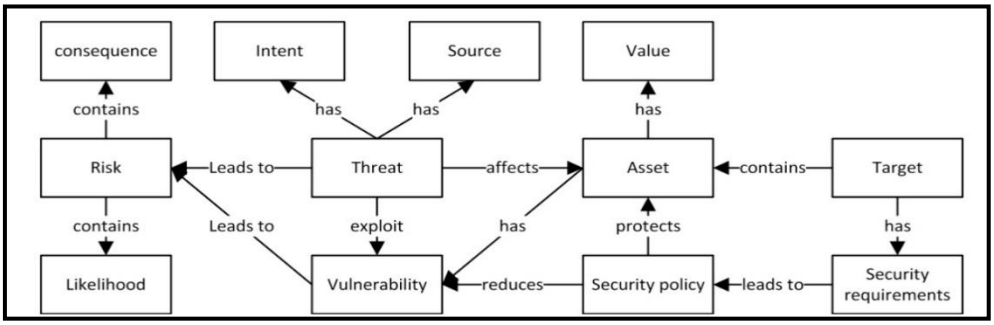

Fig. 1: CORAS model

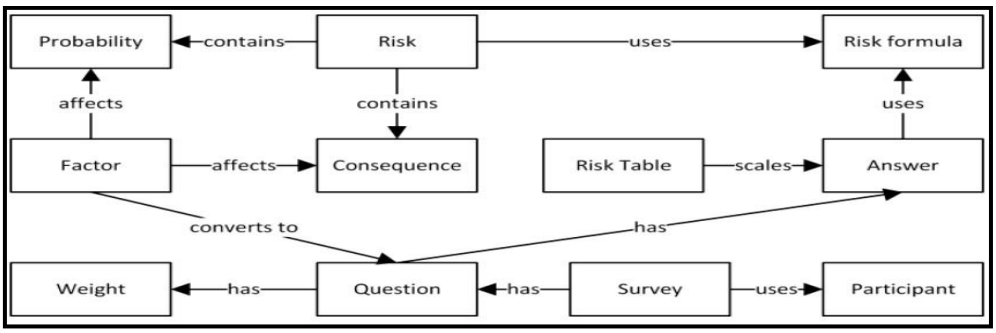

Fig. 2: ISRAM model.

The Information Security Risk Analysis Method (ISRAM) Karabacak and Sogukpinar (2005) is a model for risk analysis and are a study-based model adopted to inspect risk in information security which uses a quantitative method. Probability and consequence are the two primary attributes of risk to conduct two isolated and independent surveys. The method is deriving on risk entity shaped as a mix of probability and consequences of a security infringement

The risk aspect in "ISRAM is a numerical value between 1 and 25" (Karabacak and Sogukpinar, 2005). These numerical values are the value in which risk management determination are established as they correlate to a qualitative value of high, medium, or low value. It is designed as to analyze the risks at complicated information system by favoring participation of manager and staff. The ISRAM methods consist of seven steps. The ISRAM model is shown in Figure 2

Figure 2 depicts the ISRAM ontology with an overview of its elements. It identifies that risk contains consequences and probability with certain factors affecting them. These particular factors are transformed into questions and surveys completed by participants. The questions use weight in order to discover answer. Criteria that contribute to these factors are the direct association with the vulnerability and direct association with an important or critical asset. That led to the degree of influence to the probability or the result of infection. Ultimately, specifying how much the factor contributes to the risk criterion. Those factors with higher or more severe criteria have higher weight. The risk table then calibrates the response and, in addition to the risk formula, the results are transformed into a numeric value of the risk.

2.7.2. IS

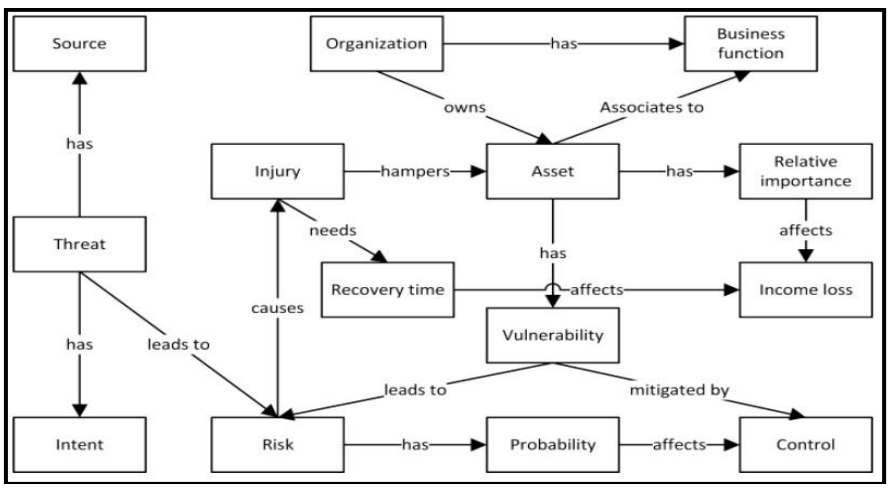

Fig. 3: IS model.

According to Suh and Han (2003) the IS method is a quantitative methodology developed by the Korea Advanced Institute of Science and Technology in 2002. This approach is divided into four phases. The first phase involves it using AHP (Analytical Hierarchy Process) in order to decide the relative requirement and consequence of particular business functions. This will be followed in the second phase, a conventional risk analysis procedure: Assets are defined and allocated to the business functions, resulting with the relative requirements of the asset. This is followed by a vulnerability and threat appraisal that will provide result to the certainty of risk probability in the third phase. In the final and last phase annualized loss expectancy (ALE) computation is organized to appraise the comprehensive loss because of business discontinuance. This method does not incorporate any instrument for re-examination of relevant protections for risk control. The IS model is shown in Figure 3.

Figure 3 depicts the ontology of the IS method. From the ontology it can be seen that asset is the first consequential contact point in the method. Organizations have various assets including information asset where every asset is associated to a business operation in the group. Risk assessment requires an overview of the vulnerability of the asset, and of threats having both source and intent. Risks may be capable of causing injury to the system that hinders the organization's assets Agrawal (2017). Injury requires recovery time; however, it leads to a loss of income. Risks are likely to have an effect on the control needed to reduce vulnerability.

2.8. Conceptual model

The researcher had constructed a conceptual model. The conceptual model in this research is an integration of three security risk analysis model which is the CORAS security risk analysis model Aegedal et al., (2002), ISRAM security risk analysis model Karabacak and Sogukpinar (2005) and IS security risk analysis model Suh and Han (2003) that is depicted in Figure 4.

As can be seen in Figure 4, the conceptual model was created based on the six common attributes that the three discussed model have. These are asset, threat, vulnerability, risk, likelihood/probability, and finally consequences.

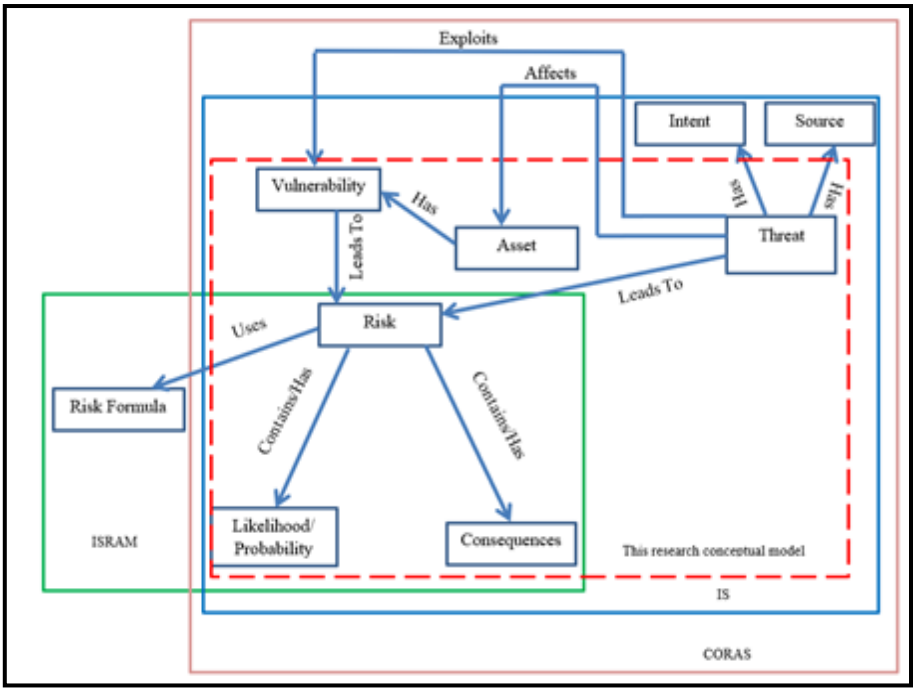

Fig. 4: Research conceptual model.

3. Methods

The main material used in this research from the risk management standpoint are the International Standard for Standardization (ISO) 31000 (ISO, 2018). This is as ISO 31000 provides direction on how companies can integrate risk-based decision making into an organization's governance, planning, management, reporting, policies, values and culture (Caufield, 2018).

The research philosophy being used in this research is intrepetivism (constructuvism) with qualitative method being used as the research design. Because of this, the methods that are being used in this research is the semi-structured interviews. Following these materials and methods, the researcher had constructed this paper research questions, which are: 1) What is risk and threats that must be analyzed associated to the related information asset in the connection of information security risk? and 2) What is the risk classification in information security risk depending on the risk associated to the related information asset?

Furthermore, the researcher had also set the research objectives for this research from the research questions which are: 1) To analyze the risk and threats in the related information asset in the context of information security risk and 2) To classify information security risk depending on the risks associated to the related information assets.

A list of keywords was used to search for literature that had helped the researcher to construct an interview instrument. Then, an initial interview instrument was created for this research was based on the literature found . Following the creation of the initial interview instrument two pilot interviews with two respondents from two different IP involvements were conducted with the respondents being an IP inventor and an IP intermediary respectively.From these interviews it was found that the questions were not suitable as it focus more on the risk of IP separated by types instead of the risk that can affect all of the IP types. This is why the interview instrument was amended and changed to focus more on the issue of risk in that affect the control area of an IP/Invention and risk that can cause an infringement to the IP/Invention.

The researcher had conducted several sub-processes during the interview process which are the pre-interview process, conducting the interview process, and the post-interview process. For the pre-interview process, the researcher had taken certain steps to find which Intellectual Property experts to interview and find their contact information. The first step was that the researcher had contacted the organization administration of which there are several experts in the field of IP and had asked for the experts contact information. From there the researcher had gone to the organization expertise website page in which the researchers had found the experts email. The last step in the pre-interview process was that the researcher had emailed the experts to ask for interviews.

Following that, during the conducting of interview process, the researcher had conducted the interview with the interviewees by first asking for their availability for an interview and then setting a date and time with the interviewee according to their availability. All of the interviews were held on online platforms Google Meet and Skype as the interviews were held during the Movement Control Order (MCO) period. The duration of the interview varied from interviewee to interviewee as each of the interviewee had different experiences and as such had told different point of view relating to IP and the risk associated with them with the shortest interview being 20 minutes and the longest interview being 45 minutes. Finally, during the post-interview process, the researcher had recorded the interviews given by the interviewees and compiled them to be analyze as to find out what are the risk and threats that must be analyzed in relation to IP in the connection of information security risk.

A total of seven interviews were conducted by the researcher for this research as can be seen in Table 4. Following the whole interview process, the researcher had used thematic analysis to analyze the statements gotten from the interviews. Thematic Analysis is qualitative research analysis method. It is a method for identifying, analyzing and reporting patterns with data [16]. Thematic Analysis allows the researcher a lot of flexibility in interpreting the

data, and allows the researcher to approach data sets more easily by sorting them into broad themes [16]. There are six steps in the thematic analysis process which are: 1) familiarize with the data; 2) generate initial codes; 3) search for themes; 4) reviewing themes; 5) define and name the themes; 6) produce report.

Table 4: Interviewees characteristic.

No	ID	IP Involvement	Years of Experience	Mode of Interview
1	I1	Intermediary	27	Google Meet
2	I2	Inventor	23	Skype
3	I3	Inventor	23	Google Meet
4	I4	Inventor	14	Skype
5	I5	Inventor	26	Skype
6	I6	Inventor	20	Google Meet
7	I7	Intermediary	8	Google Meet

4. Results

The results of the interviews are used to find both the results of research question 1 and 2 of this research. From the use of thematic analysis, it was found that the interviewees interviewed are mostly involved in the IP type of Patents and Copyrights. As such the risk and threats that have been found are in relation to these 2 IP types. Table 5 shows the risk and threats found from the interview.From the results found in phase 2 which were the risks and threat related the information asset (IP). The researcher has extended the information gain by finding each risk probability and consequences which is shown in Table 6.

Table 5: Risk and threat.

Risk ID	Risk/Theme	IP Type	Threats
R1	The Invention/work being stolen and pirated by other people	Patent/ Copyright	Internal and External (Depend on the intention)
R2	Infringement of others work/invention during the invention/creation process	Patent/ Copyright	Internal (Depends on the researcher and their collaborator)
R3	Work/Invention being stolen and modified during events such as exhibition and etc.	Copyright	External (Can be from the event organizer and participants)

Table 6: Risk threat, probability, and consequences.

Risk ID	Threats	Probability	Consequences
R1	Internal and External (Depend on the intention)	Depends on value and impact of invention and intention of the stealer	Depends on value and impact
R2	Internal (Depends on the researcher and their collaborator)	Depends on the researcher and colleague awareness	Depends on the value and impact of the invention and the researcher's reputation
R3	External (Can be from the event organizer and participants)	Depends on what the researcher displays during the events.	Depends on the value and impact of the invention/ creation.

5. Discussion

From Table 5, it can be seen that there are two risk that are associated with Patents and three risks associated with Copyrights. The similarities in the risk that affects both patents and copyrights are : 1) both can be stolen and pirated by other people and 2) infringement of other people works/invention can happen in both.

These risks constitute two of the risks found with the third and last risk affecting copyrights and that it is more specific with the risk being the work being stolen and modified during events such as an exhibition. By getting these results, the researcher had fulfilled research objective 1.

The discussion for research question 2 is on the probability and consequence of the risk founded happening. It was said by Evesti (2016); Chen and Song (2016) that "Risk combines the probability of threat realization and the impact/consequences of threat realization" as such these two measures are something that is needed for this risk analysis of information asset (IP). As such the consequences and probability of the risk happening is stated as can be seen in Table 6. It can be seen that the consequences and probability of all three risks are not set in stone but instead changes depending on the variables that affect them as stated in Table 6. This means that the risk for every IP is not the same and that depending on their variables, their risk is different. By getting these results, the researcher had fulfilled research objective 2.

6. Conclusion

6.1. Contribution to theory

Three key contributions to theory can be derived from this paper.

First, this paper had presented a conceptual model constructed from the common attributes shared between three security risk analysis model which were CORAS Lund et al., (2011), ISRAM Karabacak and Sogukpinar (2005), and IS (Suh and Han, 2003). It has shown that there are common attributes that are essential and is important to be considered for a security risk analysis. These six common attributes

are “Asset”, “Risk”, “Vulnerability””, “Threat”, “Consequences”, and “Likelihood/Probability”.

Second, through the interview analysis, this paper had shown what are the risk and threats that must be analyzed relating to the IP. This is relevant to the body of knowledge as it has shown that (1) the same risk can affect both copyright and patent even though they are of different IP types and (2) that threats for risk can originate externally or internally or even both for the same risk.

Third, this paper had shown that for the risk found which were R1, R2, and R3 that their likelihood/probability of happening and the consequences of these risk happening are not set in stone and are absolute but are instead depended on factors such as impact and value of invention, the intention of the stealer, researcher and their colleague awareness, and etc.

6.2. Future development

The results of research question 1 and 2 of this research has shown the researcher the risk associated with patent and copyright along with its threats, consequences, and probability. This had let the researcher to move forward in the research. Moving forward, the researcher hope that interviews with other IP parties such as IP lawyers can be held as they may have different inputs and perspective that can contribute to this study.

References

Abdullah, N. Hanafi, H. Nawang, N.I. (2021). Digital era and intellectual property challenges in Malaysia. *Social Sciences & Humanities, Pertanika*, 29(S2), 205-219.

Aegedal, J. O., den Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D., & Stolen, K. (2002). Model-based risk assessment to improve enterprise security. *Proceedings of Sixth International Enterprise Distributed Object Computing Conference*, 51-62.

Agrawal, V. (2017). A comparative study on information security risk analysis methods. *JCP*, 12(1), 57-67.

Batini, C., Castelli, M., Viscusi, G., Cappiello, C., Francalanci, C. (2018). Digital information asset evaluation: A case study in manufacturing. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 49(3), 19-33.

Business Dictionary. Risk Retrieved from http://www.businessdictionary.com/definition/risk.html

Caufield. J. (2018). How to do thematic analysis. *Scribbr*. V iewed 18 August 2020, https://www.scribbr.com/methodology/thematic-analysis/

Chen, H. & Song, Z. (2016). Secure information assets with data: An information security governance framework using orchestrated data analytics from a holistic

perspective. *International Conference on Computer Science and Electronic Technology (CSET 2016)*, 179-183, Atlantic Press.

den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps — A guided tour to the CORAS method. *BT Technology Journal*, 25, 101-117.

Eachempati, P. change management in information asset'. *Journal of Global Information Management (JGIM)*, 25(2), 68-87.

Evesti, A, Jordan, V, Latval, O. M, Sihvonen, M. & Toivonen, J. (2016). Security risk visualization with semantic risk model. *Procedia Computer Science*, 83, 1194-1199.

Grimaldi, M. Greco, M., & Cricelli, L. (2021). A framework of intellectual property protection strategies and open innovation. *Journal of Business Research*, 156-164.

ISO (2018). ISO 31000 Risk Management – Guidelines.

Karabacak, B. & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers & Security*, 24, 147-159.

Lund, M., Solhaug, B., & Stølen, K. (2011). A guided tour of the CORAS method. *Model-Driven Risk Analysis*, 23-43.

Market Business News. What is information technology or IT? Definition and examples. Retrieved form https://marketbusinessnews.com/financial-glossary/information-technology/

Miller, L. C. & Gregory, P. H., CISSP for dummies(5th Edition). New Jersey/United States of America: Wiley Brand.

Rouse, information asset, 2013, Retrieved from https://whatis.techtarget.com/definition/information-assets

Suh, B. & Han, I. (2013). The \IS\ risk analysis based on a business model. *Information & Management*, 41, 149-158.