ISSN 2278-3091
Volume 8, No.1.1, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1981.12019.pdf
https://doi.org/10.30534/ijatcse/2019/1981.12019

A Hybrid Model for Information Security Risk Assessment

Sami Haji*[1], Qing Tan[2], and Rebeca Soler Costa[#3]**
[1,2]School of Computing and Information Systems, Athabasca University, Canada[1]
[3]Department of Educational Sciences, University of Zaragoza, Zaragoza, Spain[2]
[*]sami.haji@hotmail.com, [**]qingt@athabascau.ca, and [#]rsoler@unizar.es

ABSTRACT

Many industry standards and methodologies were introduced which has brought forth the management of threats assessment and risk management of information assets in a systematic manner. This paper will review and analyze the main processes followed in IT risk management frameworks from the perspective of the threat analysis process using a threat modeling methodology. In this study, the authors propose a new assessment model which shows that systematic threat analysis is an essential element to be considered as an integrated process within IT risk management frameworks. The new proposed model complements and fulfills the gap in the practice of assessing information security risks.

***Keywords*—**Risk Assessment, Security Assessment Framework, Threat Analysis, Risk Management.

1. INTRODUCTION

The ever-changing cyber activities evolved in a manner that circumvents the confidentiality, integrity and availability of control boundaries that are built in technologies. This raised the risk of unauthorized access, data manipulation and disruption of business information which has a severe business impact on organizations [1]. It is clear that cyber attackers are managing to stay ahead of protection means which has elevated the concern for safeguarding valuable information asset. For that reason, the protection of information has become an important endeavor for the top management of many organizations to gain appropriate assurances and operational visibility on the protection of resources and information. One of the steps in risk management frameworks, especially in the area of information security, is threat identification which is an essential element that contributes to the analysis of a risk to information Asset [2][3]. The process of threat identification and analysis against information asset provide a direction for carrying out an accurate risk assessment and implement appropriate countermeasures to mitigate the risks on resources and information. The nature of threat identification and analysis is complex and many standalone methods were introduced to provide guidance for addressing threats proactively. The scope of the methodologies of threat analysis is expanded and discussed in detail as part of the process of application development life cycle using threat modeling techniques [4]. However, this capability does not extend to the ongoing risk management practices in order to identify, analyze and evaluate threats appropriately. This limitation introduces a gap in the risk assessment and the precision of risk treatment planning in order to implement the relevant countermeasures that counteracts the identified risks.

The rest of this paper is organized as follows. Section II provides the problem statement. The standards, guides and methodologies are briefly surveyed in Section III. Section IV discusses the gap and findings in relation to the reviewed papers. The gap is complemented by proposing a hybrid model for information security risk assessment in section V. The proposed model is compared with the reviewed standards, guides and methodologies in section VI, which focuses on the threat analysis component. The case study in section VII shows a typical implementation of risk management and the missing gap in the threat analysis process due to the disconnection between risk management and threat modeling methodologies. The conclusion of future work is offered in section IX.

2. PROBLEM STATEMENT

One of the key processes in risk assessment is threat identification and analysis. In this research, we will attempt to answer the following questions

- To what extent do the processes of threat modeling affect the existing risk management framework practices?
- Will the adoption of threat modeling processes, as an integrated process of risk management, improve the risk identification and mitigation process?

3. III. BACKGROUND & RELATED WORK

A. Risk Management

The risk management frameworks outlined in this section of the research consist of management abstract layer approach to risk assessment. There are different approaches to each framework and for that reason a brief overview is given to each.

- ISO/IEC 27005 provides a standardized approach for information security risk management within an organization and it is a key requirement in information security management system (ISMS) [3]. The standard is applicable to organizations of all types given the generic outline of process flow for managing risks.
- NIST SP 800-37 is a guide that is made for the purpose of assisting federal information system and organizations in following a systematic approach of identifying, and evaluating risks to information systems [2]. The guide advocates that the risk assessment process is part of a larger risk management hierarchy within the organization. This resembles ISO/IEC 27005 in terms of making the entire cycle of information security risk management part of and an integrated process within the organization that is driven by a top down approach.
- The Risk Analysis and Management Method (CRAMM) provided government departments with a methodology for managing information security risks through a systematic review. The method has undergone multiple revisions and was adopted by Insight Consulting [5]. It was commercialized and made available to other organizations that are keen on implementing the CRAMM methodology.
- ISRAM method uses quantitative methods to risk assessment through mathematical calculation using a typical probability and impact equation based approach to deduce the severity of identified risk [6].

B. Threat Modeling

The threat modeling framework and methodologies are typically addressed at the operational level within the organization. The outcome of most methodologies is to technically assess the security issues using systematic methods which are not all identical. As a result, a brief overview is given to each.

- OCTAVE framework is designed to assist organizations in understanding the cyber threats targeting their asset and follow a systematic approach in addressing the associated risks. Currently, there are two approaches to OCTAVE. The first approach is designed for large organizations. The second approach is the simplified version for small organizations. The OCTAVE Allegro framework is the successor of the original OCTAVE method follows a multiple phase approach with multiple interrelated processes and sub activities [7].
- OWASP threat modeling is driven by the objective of embedding application security principles during the application development life cycle in order to ensure proper implementation of controls before the formal usage of the application and its resources. This results in avoiding cyber risks at the early stages of the application development which minimizes drastic changes to the application development at a later stage [4].
- PASTA is an application threat modeling process guide that follows a sequential approach to identify and analyze threats. This methodology uses a seven step approach to risk assessment and leverages an attacker's point of view on application technologies. This model is driven by business alignment at the early stages of the process to establish appropriate requirements that impacts the outcome of the decision making process [8].
- CORAS is a method for conducting risk analysis that uses unified modeling language (UML) in order to achieve a practical approach of model-based risk assessment. There are eight critical steps taken to complete the assessment in order to fulfill all the core elements of this method [9]. CORAS provides a way to demonstrate the cascading effect of a single vulnerability resulting to an incident.

4. RESEARCH GAP AND FINDINGS

The observed information security risk management practices are designed using a management perspective through an abstract layer that follows a structured process for assessing risks. One of the main interrelated processes is threat identification and analysis, which is not comprehensive in a manner that captures a systematic review and evaluation of threats. This limitation creates weakness in the risk assessment cycle, which impacts the decision making process. The decision making process impacts the implementation of the appropriate countermeasure and the resource required to protect the asset. On the other hand, the threat identification and analysis are expanded in threat modeling methodologies and frameworks which are designed to follow a technical process to risk assessment. This operational aspect of threat modeling shows that threat identification, analysis and evaluation is carried out in a systematic and structured manner that is comprehensive for managing technical risk. It is important to note that the operational process in the reviewed threat assessment cycle does not possess the risk management views for managing technical security risks.

Even though both practices differ from one approach to another, overlap and similarities exist among the processes. However, the common goal shared among the practices is the adequate protection of assets. The integration of threat modeling processes into risk management framework ensures that technical security risks are managed in a manner that aligns with the organization's practices and transferable to decision makers. Subsequently, improving the overall risk mitigation strategies and minimizes the disconnection between both practices and streamline the risk assessment process.

5. PROPOSED SOLUTION

The following proposed hybrid model shows the critical processes to information security risk assessment. The critical processes are linked based on the fundamental relationship between the definition of asset, vulnerability, threat and countermeasures to identify information security risks. The relationship model demonstrates the sequence of processes of a core risk identification, evaluation and remediation function at a conceptual level. The sequence of the relationship between the definitions is based on the Factor Analysis for Information Risk model [10]. The proposed hybrid model applies to information security at an abstract and the operational layer that fulfills the disconnection gap between management and technical approach to risk assessment due to the adoption of selected threat modeling processes for threat analysis. The following Figure 1 shows the proposed hybrid model which consists of a core principle to risk assessment.

It is important to note that the activities are formatted in a conceptual which serves as a guide that constitutes the entire process cycle. The development of a methodology is subject to further customizations depending on the nature and the requirement of the organization adopting the model.

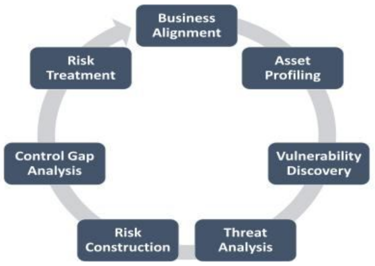

Figure 1: Proposed Hybrid Risk Assessment Model

A. Business Alignment

This stage has four activities which consist of the development of information security risk management and information classification policy, scope of risk assessment and protection measures, monitoring and communication strategy. The activities at this stage sets the expectation tone and the objective of risk assessment that aligns with the business objectives. The policy outlines the guiding principles and responsibility necessary to protect the information assets and the required measurement. The information classification policy sets the principles of the importance of restricted, confidential, internal information. This determination aids in the identification of the importance of the asset during the risk treatment stage. The scope and boundaries of the assessment determine the business functions that rely on the electronic services that are subject to the implementation of the policy. This determination guides the execution of the risk assessment during the execution cycle. Finally, the communication and monitoring strategy shows the collaboration of risk communication and the relationship with the stakeholders during and after the change of risk status. Typically, this takes place at the monitoring phase where the change in the environment or conditions elevates or reduces the severity of the security risks. The change of risk severity initiates the mitigation strategy and the subsequent management processes for the risk treatment and the associated decisions in order to reduce the severity of the risk to acceptable levels. This entire state considers the planning and context establishment of the risk management within the organization that aligns with the direction of business strategy. Therefore, business alignment is a key factor during the planning and establishment of information security risk assessment [11].

B. Asset Profiling

There are three main core activities to be implemented at this stage. First, the identification of the asset in the scope. The level of the asset identification is a service driven identification approach which is the collection of resources that provide a specific service to stakeholders. Second, the service ownership and the classification. The identification of the service owner followed by the classification of the services in terms of sensitivity. Finally, the identification and classification of the service lead to the decomposition process to identify the components that comprise each service such as software, information, platform, hardware. The depth of the decomposition depends on the service identification process. This process is subject to further customizations that aligns in a manner that fit the organization in question. This decomposition process leads to the identification of a specific weakness in the service. Therefore, the decomposition of the service determines the exact components that are subject to further vulnerability discovery process which subsequently leads to the applicable mitigation strategies. The asset profiling provide the decision makers with the depth of understanding the importance of the asset and the impact it has on critical functions [12].

C. Vulnerability Discovery

The the vulnerability discovery process takes presence to highlight the weaknesses in the component. In most cases, this is achieved through automated a query tool with built-in capabilities to understand the weaknesses in component or manual processes to uncover the weaknesses. However, it is important to note that query tools generate false positives that does not relate to the component or situation. In addition, many of the query tools do not consider the context of existing countermeasures in the setup of the network and infrastructure [13]. Therefore, the list of vulnerabilities generated by the query tool is subject to the mitigation strategies of existing control in the network. Finally, the alignment of a threat with a vulnerability generates a valid risk context that is subject to further analysis. This alignment determines the vulnerability with the matching threat to establish the context of exploitation. The presence of a vulnerability without a threat does not always lead to an exploitation process and therefore lacks the fundamental elements of risk identification.

D. Threat Analysis

The threat analysis stage consists of the development of a threat profile. The threat profile consists of the identification of a threat agent (actor), the discovered vulnerability and the threat scenario after matching the threat actor with the discovered vulnerability. The source of the threat actor comes from two main streams which are internal or external. The alignment of the threat actor with the discovered vulnerability builds the threat scenario that leads to the exploitation of the weakness in the component. The establishment of a threat scenario is necessary in order to build a threat tree. The threat tree will identify the channel and the method used to exploit the component to achieve the threat scenario. The development of a treat tree can follow either OWASP or AND/OR method that was developed by Bruce Schneier's
[14]. The establishment of a threat tree shows the possible entry points to achieve the threat scenario. The development of an attack tree on each scenario builds the intelligence required in order to establish an awareness for the risk construction stage and replicate the same threat scenario on other components that have similar attribute and conditions within the same scope.

E. Risk Calculation

There are two types of risk assessment methods which are qualitative and quantitative [15][16]. The qualitative risk assessment method describes the magnitude of a threat impact to the organization and the probability of risk occurrence which is expressed using a multiplication function. This description of probability and impact is typically rated using labels such as high, medium or low. Some of the discussed frameworks leverage numerical values to present the final risk rating after determining the rating of impact and probability. For instance, 3 signifies high, 2 is medium and 1 is low. The mathematical formula for calculating the final risk varies from one methodology to another. The following is an example of risk calculation based on a qualitative [17].

$$\text{Risk Value} = \text{Impact} * \text{Probability}.$$

In a typical scenario where a moderate probability of unauthorized access to the password file results in a high impact, produce an overall risk value of 6.

$$\text{Risk Value} = \text{Impact (3)} * \text{Probability (2)}.$$

However, the overall risk value of 6 does not indicate any importance without applying the final value to a risk grid to indicate the rating of the overall risk. Another method for obtaining the overall risk value is through a discussion based assessment where the assembled analysis team determines the overall risk value using judgement based assessment depending on the context of the risk. On the other hand, quantitative risk assessment method measures the risk based on monetary value. This is measured based on annual loss expectancy (ALE) which is calculated based on a single loss expectancy (SLE) multiplied by the annual rate of occurrence (ARO) [17].

$$\text{ALE} = \text{SLE} * \text{ARO}.$$

While both qualitative and quantitative methods are valid, a mature practice usually adopts one of the methods to regulate the risk assessment practice and ensure consistency and systematic assessment. It provides a clarity that is meaningful to decision makers to investigate the possible existing controls that mitigates the attack tree branches which is discussed in the next stage.

F. Control Gap Analysis

There are three main core activities in the control analysis stage. First, the review of existing countermeasures in place that mitigates the identified risks in the risk calculation stage. Upon the identification of existing controls, a measurement for analyzing the adequacy to mitigate the identified risk is required in order to ensure the acceptability of the residual risk. This is achieved using the following equation at a conceptual level [3][18].

$$\text{Outstanding Risk} = \text{Identified Risk} – \text{Existing Controls}.$$

This formula determines whether the existing countermeasure is sufficient in a manner that makes the outstanding risk acceptable. The acceptability of the outstanding risk is determined by the risk severity value scale discussed in the risk calculation stage. On the other hand, if the outstanding risk is not acceptable, a determination for the expected controls is required in order to achieve the acceptable level. This second activity for determining the expected controls is measured using the following at a conceptual level [3][18]

$$\text{Acceptable Risk} = \text{Expected Control Behavior} + \text{Existing Controls Behavior}.$$

The expected behavior is measured by a satisfactory appraisal of the risk after the implementation of the expected control in addition to the existing control. The expected control behavior is determined using a specific approach based on a strategic sequence to control implementation such as preventive, detective, corrective and finally compensating control. This sequence shows the priority of control selection to address the outstanding risk to ensure its reduction to acceptable levels. For example, a web application server that is vulnerable to SQL injection attacks is mitigated using a preventive control such as the implementation of input validation techniques [19]. However, it is important to note that the selection of the applicable controls reduces the identified risk to acceptable levels. Finally, the third activity is the gap in the existing countermeasure to address, the calculated risk that is deemed unacceptable. This gap is measured using the following formula at a conceptual level [3][18]

$$\text{Control Gap analysis} = \text{Expected Control} – \text{Existing Controls}.$$

The gap identified is the difference between the expected and existing controls. This gap leads to the risk treatment to mitigate the outstanding risk and the associated expected control selection activities.

G. Risk Treatment

The gap in the controls for the outstanding unacceptable risks identified requires a risk treatment plan. This makes the risk treatment stage subject to two main activities. First, the detailed planning of the expected control behavior using a standard or documented best practice index. This elevates the expected control behavior in a manner that is optimal and achieves the highest maturity. Second, the study of the expected control behavior through cost/benefit analysis [20]. The cost/benefit analysis, reviews the expected control behavior from financial, operational and legal feasibility. The operational feasibility reviews the after-implementation aspect of control, maintenance and the existing capability to ensure the expected control behavior. Finally, the legal feasibility is the review of the legal aspect of control acquisition, implementation and consequence. The three dimensions of cost/benefit analysis leads to the development of a structured plan in a manner that is meaningful to the decision makers. The final structured plan is documented and reviewed with the business process owners and service custodians. The implementation of the new controls depends on the capability of the organization. Alternatively, the absence of the capability within the organization leads to the acquisition of the expected control behavior. This activity solely depends on the communication strategies of identifying risks with the senior management of the organization. Typically, the resource of financial support is a key element to ensure the involvement of the relevant stakeholders. Therefore, it is important that the risk management language becomes the appropriate channel for elevating the outstanding risks and the associated risk treatment plans to obtain the consent of the decision makers on the suitable mitigation strategies. Thus, this stage connects the former activities with the risk management and information classification policy which is the first stage identified at the beginning of the proposed hybrid model.

6. COMPARISON OF THREAT ANALYSIS PROCESS

The context focuses on a threat agent taking advantage of a vulnerability residing in an asset that causes the exploitation process to occur [21]. This context establishment brings forth the improvement to the accuracy in identifying the relevant risks in the assessment process. The identification of a threat builds upon the source for deriving threat agents. The identification of threat agents takes on many forms such as Malware, insider threat or an external attacker. The threat agent in relation to the vulnerability discovered provides the opportunity to compromise the asset [17]. This logical relationship between the threat, vulnerability and asset pave the opportunity to assess the context as a result of the review of the conditions occurring. The occurrence of the condition confirms the potential of exploitation process. ISO/IEC 27005, NIST 800-35 and CRAMM provide a predefined list of threats that can be leveraged during the threat identification process in the risk assessment cycle. This predefined list of threats provides the direction for the establishment of a context which is obtained using a collaborative process through an interview or feedback mechanism. This discussion based approach using a predefined list has many advantages. First, it provides the stakeholders and the decision makers with the ability to review a larger scale of possible threats that targets the asset in question. Second, it provides a venue for raising the awareness to the decision makers on the possible danger that targets the asset. One of the disadvantages of using a predefined threat list is the endless possibilities of establishing risk context which raises the challenge in narrow the most important countermeasure. In addition, the identified possibilities do not always align with the vulnerabilities identified which impacts the establishment of a context. FRAP follows a meeting based discussion with the relevant business process owners and key stakeholders to identify the threat and establish the relevant context. This collaborative based approach to identify threat is not systematic and does not follow a proved methodology compared in OCTAVE, PASTA, OWASP and Microsoft. The latter methodologies identify threats using the STRIDE model to obtain the source required to establish the risk context. The actual establishment of the context is performed using threat tree and abuse case scenarios to provide granularity and precision to considering practical situations. Even though the methodologies do not all use the exact steps, the principles of in depth analysis of the threat scenarios are followed. One drawback to this approach is the lack of the involvement of business process owners, which increases the challenge to obtain the resources to mitigate the identified risks. Finally, the CORAS risk modeling approach identifies risks context using a modeling methodology involving the business process owner through a structured brainstorming sessions. This approach uses the business process flow as a model in order to establish threat scenarios that align with the model in question and to protect the targeted asset, but not the business process that operates the mission critical function in the organization. *The proposed model shows that threat analysis leverages some of the key processes followed in threat modeling methodologies while maintaining the principles of risk management in order to complement and provide an overall approach to risk assessment.*

7. CASE STUDY

The case study reviews the information that represents the processes followed through the results of the collection and analysis of the artifacts that are implemented. The artifacts reviewed present the opportunity to demonstrate a typical implementation of risk assessment to confirm the presence of a structured process. In turn, provides a comparison to with the proposed hybrid model to establish weaknesses that are subject to further improvement.

A. Information Security Policy

The reviewed standards, guides and methodologies this paper advocate the importance of information security policy as a top down approach for the implementation of risk management to mitigate risks on information assets. The artifact reviewed is the Information Security Policy Manual that is endorsed by the senior management of the institution. This policy manual contains a high level statement of management directives to reflect on the intention of protecting the institution’s asset. The policy manual dictates the development of *Information Security Framework Standards.* The standard reviewed shows the key processes in specific control domains such as physical security, access controls, network security and others. In addition, one of the statements reviewed in the standard references the use of *ITM Risk Management Framework Standard* which states the following: *“Information security risks will be identified and managed in conformance with the scope standard requirements set out in the ITM Risk Management Framework Standard”*

As a result, the *ITM Risk Management Framework Standard* is reviewed and shows the implementation of a risk management methodology. The methodology implementation is reflected in the IT risk register based on the following statement available in the *ITM Risk Management Framework Standard* which states the following: *"IT risk will be documented in an ITS Risk Register"*

This artifact is assessed in the risk assessment documentation stage. However, the entire sequence of the policy establishment in the institution in question shows a comprehensive deployment of information security policies. This is an essential stage that directs subsequent implementations that aligns with the directives of the management of the institution. Similarly, the business alignment stage in the proposed hybrid model argues the importance of setting the objective that is articulated in four main activities which are the development of information security risk management and information classification policy, scope of risk assessment and protection measures, monitoring and communication strategy.

B. Scope Statement

The scope statement in the *ITS Risk Management Framework Standard* states the following: *“It will apply to IT Infrastructure, Application and Service risk.”*

This shows that the IT risk management policy is applicable to all assets in the infrastructure, applications and IT services provided to the stakeholders.

C. Asset Inventory

The artifact that shows the list of services is named the *Application Catalogue* which shows a total of 112 services with sufficient information that captures the functionality of the service, the data owner and other information that is relevant to the institution in question. This approach resembles similar activities followed in the proposed hybrid model where the requirement of the asset profiling is identified to present sufficient information that supports the awareness of the service to the stakeholders and provide directions in analyzing the applicable vulnerabilities and threats. Similar the review service catalogue shows the criticality of the asset in terms of availability. It provides the opportunity to establish an institution-wide understanding of the service classification.

D. Vulnerability and Threat Assessment

The deployed vulnerability and threat assessment are combined using an automated query tool to identify the weakness in the computer network and relevant information asset. The realization of potential exploitation through the automated tool builds a repository of information that is subject to risk construction exercise. The proposed hybrid model shows importance of vulnerability and threat identification and analysis to establish a threat scenario that provides a direction to builds up the risk assessment phase.

E. Risk Assessment

The review of information security risk assessment is documented in the *ITS Risk Register* which contains three sections: risk identification, risk analysis, response planning and risk monitoring. Each section has multiple attributes. The description and content of the attributes were reviewed to establish the presence of the threat scenario as a result of vulnerabilities and threats analyzed at the previous stage. The content in the *ITS Risk Register* shows no identification of threat scenarios and associated risks or the impacted services. Instead, the information captured shows selected number of risks that are defined based on the risk surface only. Many of the reviewed standards, guides and methodologies throughout this research, discuss the importance of identifying assets and the relevant vulnerabilities and threats as part of the risk assessment process. This aids in the identification of more focused control implementation that is accurate and mitigates the risk identified. Finally, the *ITS Risk Management Framework Standard* fulfills the communication gap between bottom-up and top-bottom approach using a linkage between the *ITS Risk Register* and the enterprise risk assessment process as stated below: *"Risk reporting and assessment is consolidated"*

The potential vulnerabilities and threats are not identified and assessed in a manner that makes the control selection and implementation specific to the potential risks. This causes disconnection in obtaining the appropriate endorsement from senior management of the institution to allocate the budgetary allowance to mitigate the security risks.

8. CONCLUSION

The proposed hybrid model in this paper allows other researchers in risk management to examine the applicability of the proposed hybrid model in organizations of different sizes and complexity of operations. More importantly, it builds the foundation for carrying our further studies in the aim of systematically addressing information security risks while examining the growing threat landscape as a fundamental process in the risk assessment cycle.

REFERENCES

[1] A. S. Sendi, R. A. Barzegar & M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computer & Security*, Vol. 57, pp. 14-20, Mar 2016. https://doi.org/10.1016/j.cose.2015.11.001

[2] G. Stonerbumer, A. Goguen & A. Feringa, “Risk management guide for information technology system,” (2002). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[3] IEC/ISO 27005, "Information security risk management," *ISO International Organization*, 2011.

[4] OWASP, 2015. Application threat modeling. Retrieved from: https://www.owasp.org/index.php/Application_Threat_Modeling

[5] Z. Yazar, "A Qualitative Risk Analysis and Management Tool – CRAMM," *SANS Institute InfoSec Reading Room*, 2011.

[6] B. Karabacak, I. Sogukpinar, "ISRAM: information security risk analysis method," *Computer & Security*, Vol. 24, pp.147-159. 2005. https://doi.org/10.1016/j.cose.2004.07.004

[7] R. A. Caralli, J. F. Stevens, L. R. Young & W. R. Wilson, Introducing OCTAVE Allegro: Improving the information security risk assessment process, 2007.

[8] M.M. Morama, “Threat Modeling and Risk Management,” Risk Centric Threat Modeling, pp. 235–316, 2015.

[9] M.S Lund, B. Solhaug, & K. Stolen. "The CORAS Risk Modeling Language," *Model-Driven Risk Analysis*, pp. 47-72, 2011.

[10] C. Carlson, C. Hietala, J. Jones, J. Legary, M. Middleton, J. Tabacek, S. Weiman, C. Freund, J. Hutton, D. Musselwhite & B. Tomhave. Risk Analysis (O-RA). Open Group. 2013.

[11] A. Leitner, & I. Schaumuller-Bichl, "ARiMA - A New Approach to Implement ISO/IEC 27005" 2nd International Symposium on Logistics and Industrial Informatics, 2009. https://doi.org/10.1109/LINDI.2009.5258624

[12] M. R. Grimaila, & L. W. Fortson, "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," *IEEE Symposium on Computational Intelligence in Security and Defense Applications.*, 2007. https://doi.org/10.1109/CISDA.2007.368155

[13] H. Venter, J. Eloff, & Y. Li. "Standardising vulnerability categories," *Computer & Security*, vol. 27, pp. 71-83, 2008. https://doi.org/10.1016/j.cose.2008.04.002

[14] Schneier, Bruce, Attack Trees, Dr. Dobb's Journal of Software Tools 24, 12(December 1999): 21-29.

[15] S. Liu, R. Kuhn & H. Rossman, "Understanding insecire IT: Practical risk assessment," *IT Professional Magazine*, Vol. 11, no. 3, pp. 57-59, 2009. https://doi.org/10.1109/MITP.2009.62

[16] N. Shukla, & S. Kumar, "A comparative study on information security risk analysis practices,' *Special Issue of International Journal of Computer Applications*, pp 28-33, 2012.

[17] S. Harris, "CISSP: All-in-One Exam Guide" 6th Ed. McGraw-Hill, 2013.

[18] S. Bandopadhyay, A. Sengupta, & C. Mazumdar, "A quantitative methodology for information security control gap analysis," Proceedings of the 2011 International Conference on Communication, *Computing & Security* - ICCCS '11., 2011. https://doi.org/10.1145/1947940.1948051

[19] P. He, Y. Lv, Y. Yi, J. Cai, & Z. Da, "Study and design of database protection system for Sql attacks," *IEEE International Conference on Communication Software and Networks (ICCSN)*, 2015. https://doi.org/10.1109/ICCSN.2015.7296187

[20] R. Dewri, I. Ray, N. Poolsappasit, "Optimal security hardening on attack tree models of networks: A cost-benefit analysis," *International Journal of Information Security*, vol. 11, no. 3, pp. 167-188, 2012. https://doi.org/10.1007/s10207-012-0160-y

[21] Y. Gao, Y. Peng, F. Xie, W. Zhao, D. Wang, X. Han, T. Lu, and Z. Li, "Analysis of security threats and vulnerability for cyber-physical systems," *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology,* 2013. https://doi.org/10.1109/ICCSNT.2013.6967062