Enhancement of Dynamic Risk Assessment Model for Telecommunication Infrastructure

***Gamal Abdel Nasir, **Ammar Yassir, ***Norafida Ithnan**

*Faculty of Computer Science and Information Systems, UTM University, Malaysia
**Department of Information Technology, CMJ University, Shillong, India
***Faculty of Computer Sciences, University Technology University, Johor, Malaysia

Abstract- A considerable amount of research has been conducted on information security in recent years. Limited attention has been paid to the intrinsic tradeoff between security and system usability within the current literature. The balance between protecting organizational assets and preventing access is always a difficult line and this represents an important distinguishing feature of the study of computer and information systems security. In this research, a new Dynamic Risk Assessment Model (DRAM) is proposed to secure any type of information i.e., organization information or information system. The main case study has been taken from one of the leading Telecommunication Organization which is based on my scope to the physical and logical types of information. Various dynamic and static models are investigated in order to find a suitable way of securing information which is processed either in physical or logical manner. There are different static and dynamic security risk assessment tools are available. Although, a dynamic security risk assessment tool is used to help in getting into the field of developing a new model for the telecommunication system. In DRAM, various dynamic and static models are compared with the help of data in form of diagrams and tables. As a result of these comparisons, a new dynamic risk assessment model is proposed to help telecommunication organizations to secure their information from any threats.

Index Terms- Information security, Dynamic Risk Assessment, Security risk assessment, Systems security

I. Introduction

Contracts for IT services include provisions that specify the scope, quality, and duration of the services to be delivered. When clients and providers of IT services enter into contracts, they expose themselves to a myriad of risks. The risk exposure of an individual firm is often defendant upon the provisions surrounding contract duration, service quality, and scope. While there has been a substantial body of research considering IT services contracts risk and agency issues (Clemons et al., 1993, Aubert, et al., 2005), there has been little research in quantitative-based IT services risk assessment and management in the telecommunications in particular.

Fundamentally, this research proposal seeks to answer the following question: How can firms apply quantitative and qualitative risk assessment methods and risk assessment theory to inform decision making in telecommunications services contract negotiation? I look at two specific contexts of IT services risk assessment models. First, I consider service-delivery risk faced by provider firms when offering customized, dedicated resources to a services contract. I then consider risk of information been processed physically or logically and how to secure them from different sort of attacks/risks. I am here demonstrating some of the current various models of risk assessment and by a clear comparison between them and by looking into the phases that they are covering which are risk identification, risk analysis and risk evaluation. As a researcher I believe that the basic main problem is that the information is at a risk which attacks the assets hence these assets have to be secured. And all this, according to this research, will be in a telecommunication organization where the scope will be on the physical and logical parts of the organization itself. Hence comes the type of information which may be classified into two parts i.e. organization information and information system information and for both there will be physical and logical forms. Then the research will proceed in finding out how to secure this information? Here it will look into the security tool which is taken as the risk assessment tool which in turn will have two types i.e. static and dynamic and the research aims at the dynamic one.

II. Objective of Research

Here the main objectives of this research will range from using existing tools of information security to develop a new Telecommunication Dynamic Risk Assessment Model in the near future which may:

1. Secure assets/information (been processed physically or logically) and keep them away from any kind of expected/unexpected risks that may attack them in the Telecommunication System.
2. Suitable for all types of information in the Telecommunication System as it must be easy accessible, low in cost and long in its life time.

III. Problem Background

It is a fact that the information where they have been stored or processed is at risk; hence I am aiming at producing a new developed model which will consider being as the most suitable model for the Telecommunication Organizations. Through this research I will be looking into finding a new model of securing the information finally the models of risk assessment will be looked into deeply and compared as a diagrammatical and tabular format will be formed for the dynamic risk assessment models and the static risk assessment models and hence as a result of this comparison the research will come out with a new dynamic risk assessment model which will be taken for the main case study in this research i.e. the telecommunication organization and this new dynamic risk assessment model may then been given a new name as telecommunication dynamic risk assessment model.

IV. Problem Statement

Basically the main problem is that there exists a risk which attacks the assets/information hence this assets/information has to be secured. And all this, according to this research, will be in a Telecommunication Organization. In order to address the research problems stated in the problem background section, this main problem hopefully will be solved by answering the following research questions:

1) What is the scope of the Dynamic Risk Assessment Model (DRAM) within the Telecommunication Organization?
2) What are the elements to be considered in measuring the DRAM?
3) What is the appropriate framework to measure DRAM based on context of Telecommunication Organization?

V. Research Scope

The research covers the organization information and the information system. It will be done based on the physical and logical information been stored or processed at a Telecommunication Organization. Also the feedback of this study will only focus on the side of the providers and recipients (in house providers and recipients). Therefore, the external Telecommunication System providers and external recipients are not involved in the survey and case study.

The frame work for the main problem is been stated as well as the suggested solution which leads to the main scope of the research and hence it reflects the overall objectives of this research. The frame work started from the point of stating the problem to the steps of solving it and the tool which could be used which according to this research the risk assessment tool and the dynamic one in particular. It also explains clearly the nature of the information and the source of it as it focuses on the telecommunication organization taken as the main case study from which the information may be driven. On other hand it shows the organization information and the information system information and the overlap or the intersection between them in term of common attributes on both

VI. Literature Review

Every organization is continuously exposed to an endless number of new or changing threats and vulnerabilities that may affect its operation or the fulfillment of its objectives. Identification, analysis and evaluation of these threats and vulnerabilities are the only way to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them. It has to be noted, that Risk Assessment is a process that in many cases is not (at least not adequately) performed, even if Risk Management is implemented. It is one of the main objectives of ENISA to generate awareness of this fact, but also to facilitate use of Risk Assessments by providing practical examples.

A. Identification of Risks

This is the phase where threats, vulnerabilities and the associated risks are identified. This process has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. It is very important that during this stage all risks are identified and recorded, regardless of the fact that some of them may already be known and likely controlled by the organization. The first step is to generate a comprehensive list of sources of threats, risks and events that might have an impact on the achievement of each of the objectives these events might prevent, degrade, delay or enhance the achievement of those objectives.

B. Analysis of Relevant Risks

Risk analysis is the phase where the level of the risk and its nature are assessed and understood. This information is the first input to decision makers on whether risks need to be treated or not and what is the most appropriate and cost-effective risk treatment methodology.
Risk analysis may involve a thorough examination of the risk sources with their positive and negative consequences also the likelihood that those consequences may occur and the factors that affect them and assessment of any existing controls or processes that tend to minimize negative risks or enhance positive risks (these controls may derive from a wider set of standards, controls or good practices selected according to a an applicability statement and may also come from previous risk treatment activities.)
The level of risk can be estimated by using statistical analysis and calculations combining impact and likelihood. Any formulas and methods for combining them must be consistent with the criteria defined when establishing the Risk Management context. This is because an event may have multiple consequences and affect different objectives, therefore consequences and likelihood need to be combined to calculate the level of risk. If no reliable or statistically reliable and relevant past data is available (kept for e.g. an incident database), other estimates may be made as long as they are appropriately communicated and approved by the decision makers. Risk analysis techniques include interviews with experts in the area of interest and questionnaires as well as use of existing models and simulations.

C. Qualitative analysis

In qualitative analysis, the magnitude and likelihood of potential consequences are presented and described in detail. The scales used can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risks. Qualitative analysis may be used as an initial assessment to identify risks which will be the subject of further, detailed analysis.

In quantitative analysis numerical values are assigned to both impact and likelihood. These values are derived from a variety of sources. The quality of the entire analysis depends on the accuracy of the assigned values and the validity of the statistical models used. Impact can be determined by evaluating and processing the various results of an event or by extrapolation from experimental studies or past data. As it is made clear from the above analysis, the specification of the risk level is not unique. Impact and likelihood may be expressed or combined differently, according to the type of risk and the scope and objective of the Risk Management process.

D. Semi-quantitative analysis

In semi-quantitative analysis the objective is to try to assign some values to the scales used in the qualitative assessment. These values are usually indicative and not real, which is the prerequisite of the quantitative approach. Therefore, as the value allocated to each scale is not an accurate representation of the actual magnitude of impact or likelihood, the numbers used must only be combined using a formula that recognizes the limitations or assumptions made in the description of the scales used. It should be also mentioned that the use of semi-quantitative analysis may lead to various inconsistencies due to the fact that the numbers chosen may not properly reflect analogies between risks, particularly when either consequences or likelihood are extreme.

During the risk evaluation phase decisions have to be made concerning which risks need treatment and which do not, as well as concerning on the treatment priorities. Analysts need to compare the level of risk determined during the analysis process with risk criteria established in the Risk Management context (i.e. in the risk criteria identification stage). It is important to note that in some cases the risk evaluation may lead to a decision to undertake further analysis.

The criteria used by the Risk Management team have to also take into account the organization objectives, the stakeholder views and of course the scope and objective of the Risk Management process itself.

The decisions made are usually based on the level of risk but may also be related to thresholds specified in terms of:

- consequences (e.g. impacts),
- the likelihood of events,
- The cumulative impact of a series of events that could occur simultaneously.

VII. Research Methodology

This research explains the research methodology to be used in order to meet the intent objectives of this study. As a matter of principle, the expected research work requires a combination of both quantitative and qualitative research methods, the reason behind that is the nature of people's perceptions to the Telecommunication and IT industry. Based on my scope to the physical and logical types of information hence throughout this research I will be investigating, analyzing and comparing between the various dynamic and static models in order to find the suitable way of securing those information which is been processed either in a physical or logical manner, using suitable security risk assessment tool. With a deep comparison between various dynamic and static models with a help of data been processed in the form of diagrams and tables and as a result of these comparisons a new dynamic risk assessment model will be found as an output of this research. For the data collection both primary and secondary data would be sampled according to the appropriate methods; analyzing data will depend directly on the concepts of ANOVA (Analysis of Variance), and Co – Variance, as the study is explorative in nature.

A. Security Planning and Policy

Assessing risk and making prudent decisions before the system is installed is the best approach. You can go a long way towards providing good security by establishing a security policy. A security policy is a written document that outlines what is permitted behavior on the system. Once written, it is reviewed periodically and distributed to all users of the system. No system can be fully secure, but with due diligence and attention to detail, many security threats can be mitigated.

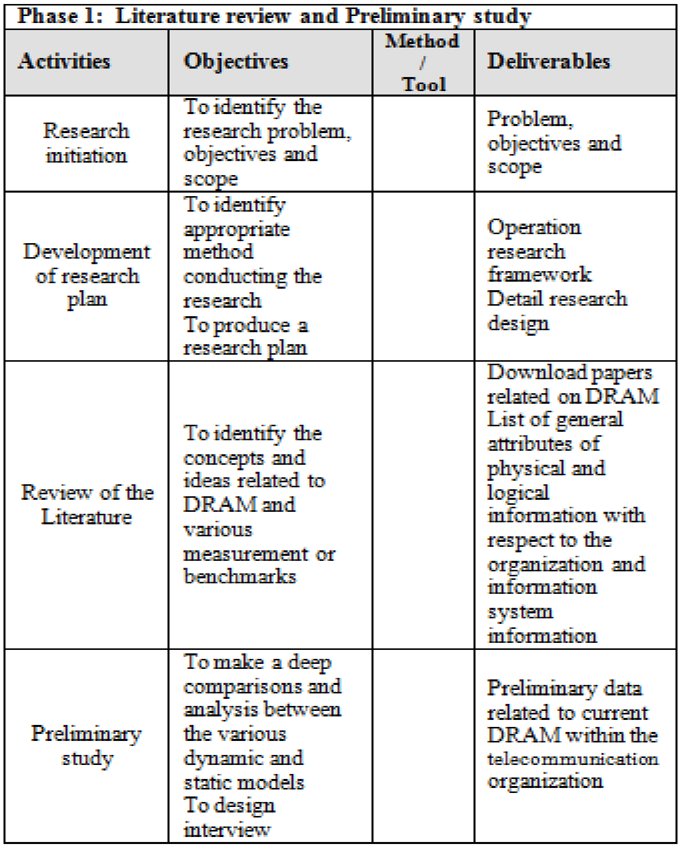
B. The difference of SRM from Other Security Solutions

Security Risk Management adds value to your existing or planned security investments. It provides advanced modeling and decision-support for the network operations and security teams. SRM enables you to maintain secure networks while reducing IT workload through continuous decision-support analysis and 'what-if' simulations. As a result, SRM complements your defense in depth strategy while adding value to your current or planned security investments.

C. Research Design

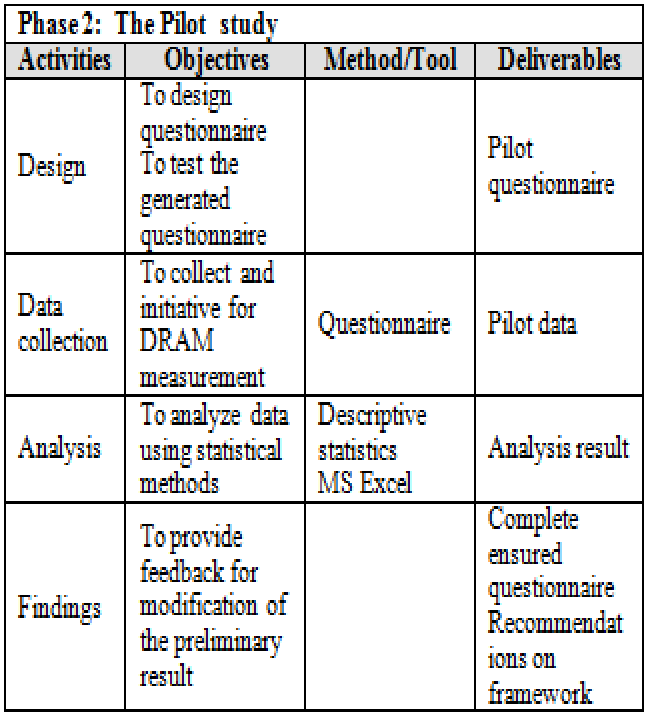
Since this is the initial stage of starting work on the research the research is structured in 3 different phases:
Phase 1: Literature Review and Preliminary study
Phase 2: The Pilot Study
Phase 3: The Case Study
The above phases are explained in the following tables:

TABLE 1
Literature Review And Preliminary Study



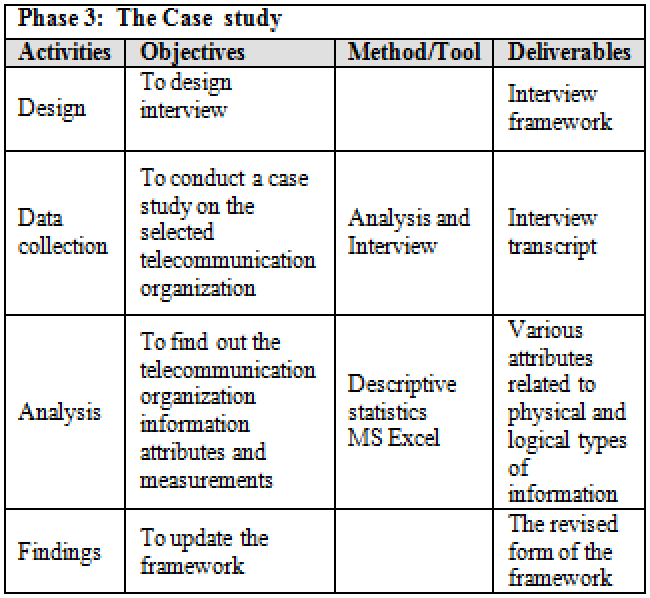
Phase 1: Literature review and Preliminary study			
Activities	Objectives	Method / Tool	Deliverables
Research initiation	To identify the research problem, objectives and scope		Problem, objectives and scope
Development of research plan	To identify appropriate method conducting the research To produce a research plan		Operation research framework Detail research design
Review of the Literature	To identify the concepts and ideas related to DRAM and various measurement or benchmarks		Download papers related on DRAM List of general attributes of physical and logical information with respect to the organization and information system information
Preliminary study	To make a deep comparisons and analysis between the various dynamic and static models To design interview		Preliminary data related to current DRAM within the telecommunication organization

TABLE 2
The Pilot study



Phase 2: The Pilot study			
Activities	Objectives	Method/Tool	Deliverables
Design	To design questionnaire To test the generated questionnaire		Pilot questionnaire
Data collection	To collect and initiative for DRAM measurement	Questionnaire	Pilot data
Analysis	To analyze data using statistical methods	Descriptive statistics MS Excel	Analysis result
Findings	To provide feedback for modification of the preliminary result		Complete ensured questionnaire Recommendations on framework

TABLE 3
The Case study



Phase 3: The Case study			
Activities	Objectives	Method/Tool	Deliverables
Design	To design interview		Interview framework
Data collection	To conduct a case study on the selected telecommunication organization	Analysis and Interview	Interview transcript
Analysis	To find out the telecommunication organization information attributes and measurements	Descriptive statistics MS Excel	Various attributes related to physical and logical types of information
Findings	To update the framework		The revised form of the framework

VIII. Preliminary Work and Results

A. Discussion & general study & research on Risk Assessments

The bellow shown research work is an initial, could be deep, study for various and different aspects of risk assessment which provide a broad knowledge and basic information on how the risk is assessed, with regard to the information security, as it occur in different areas where the information is been processed. Here a number of case studies for different types of organizations have been taken and foxed on each of them the main reason behind which I have taken this resource "along with some other relevant resources" as a basic of this initial research is to try to study and hence explain and find out the various concepts related to information security risk assessment this will be very clear and obvious as the study involves various types of organization as well as describing the different activities to be carried out when dealing with information security risk assessment tools and methods. The different types of organizations which have been pointed out in the source itself and based on which I will try to have my basic comparison and hence try to come to a useful result which may reflects which of the risk assessment methods is suitable in common for most organizations. In my basic and study I have tried to concentrate on the risk assessment concept and to have a general if not deep study on various aspects and necessary points which may be common in every type of organization with respect to information security risk assessment such as: Distinguishing Characteristics, Initiating a Risk Assessment, Conducting and Documenting the Assessment, Data Gathering Phase and Analysis Phase. Here the study been given by "GAO/AIMD-00-33- Security Risk Assessment" is focusing on the fact that risk assessment is an essential elements of risk management. In my own view this is may be true if only linked with the type of risk we assess and which method we fellow in order to assess the risk? As its mentioned in this resource i.e. GAO “ since risk and threats change over time it is important that organizations periodically reassess risk and reconsider the appropriateness and effectiveness of the policies and controls they have selected “. This has been clearly explained in the following Fig 1. I have included from the same source “GAO”. Here in my own view and analysis I would recommend if the point is clearly mentioned as the risk management needs a kind of a risk assessment which should be able to cover the threats or even go beyond that by safeguard the information from these types of risk by introducing the dynamic risk assessment as strong tool of risk assessment or reducing the risk even we can say eliminating it to the minimum. The figure as it is given in the source “GAO” is explaining about the risk assessment cycle which ranges from controlling the risk or managing it or even assessing it in different ways and manners. (Jean Boltz, Ernest Döring, and Michael Gilmore., November 1999) The risk will be assessed as the Centre will take the job of activating the cycle as per the risk level.

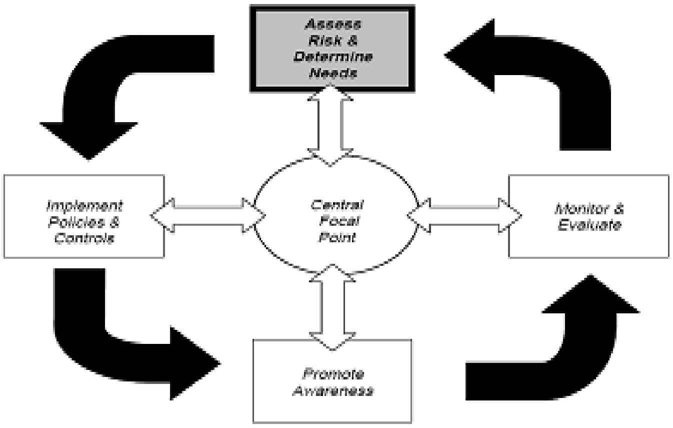


Figure 1 Risk Assessment Cycle

In my own view and according to several articles which I have referred mentioning about risk assessment I strangely believe that the above risk management cycle gives a general picture of how the risk has to be assessed based on managing it rather than introducing some models of risk assessment which ,in my own view, must be dynamic in nature so as to let the Centre of the organization be able to avoid any kind of threat in respect of its nature, time and level of occurrence as the dynamic risk assessment model will provide a solid solution and will act as a real trace for the threat which may be expected to happen or likely to be happened at any time during the cycle of information passing either through the network or even in stand-alone PC.

A. Sensitive/personal Information

Sensitive information stored on mobile devices or in background databases has to be protected. We refer to sensitive information in a broader sense here, i.e., any kind of personal information (e.g., name, date of birth), including biometric identifiers (e.g., facial image, fingerprints), as well as credentials (e.g., secret keys) and information about location. Location privacy is a particularly important issue here because mobile devices constantly communicate with their environment which might allow tracking of the user's movements. The bellow shown figure may explain the overall idea with regards to the part of problem statement and some of the research methodology which will be followed. With respect to the problem statement ,as shown in Fig 2, and how the risk as a main problem for the assets/information and the solution is that those assets in the telecommunication organization should be secured whether they are in a physical or logical format in order to reach a secured organization information and information system information as well. The model of how to develop a new Risk Assessment Model to secure that assets/information in the chosen telecommunication organization is also shown.

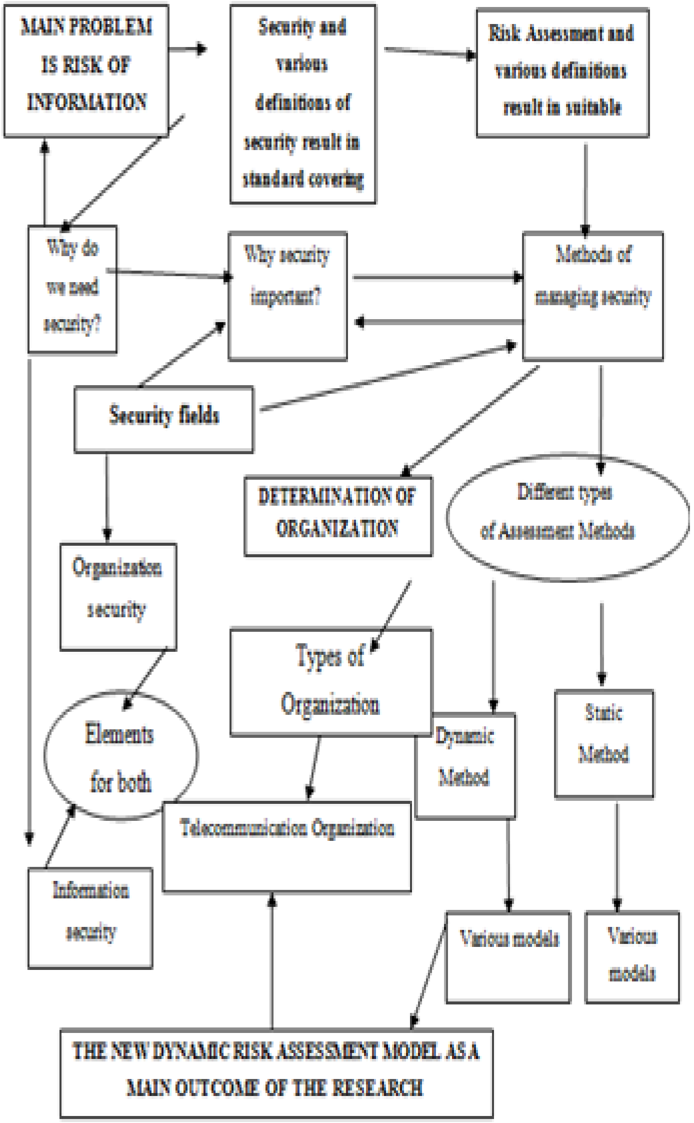

MAIN PROBLEM IS RISK OF INFORMATION
Security and various definitions of security result in standard covering
Risk Assessment and various definitions result in suitable
Why do we need security?
Why security important?
Methods of managing security
Security fields
DETERMINATION OF ORGANIZATION
Different types of Assessment Methods
Organization security
Types of Organization
Elements for both
Dynamic Method
Static Method
Telecommunication Organization
Information security
Various models
Various models
THE NEW DYNAMIC RISK ASSESSMENT MODEL AS A MAIN OUTCOME OF THE RESEARCH

Figure 2 Risk Assessment Model

IX. CONCLUSION

This research then concludes to the fact that the main problem is that the risk of information and this risk attacks the assets and hence the solution is to secure those assets in the telecommunication organization then the research passes through the point of how to secure that information and it suggests risk assessment tool as a mean of security for the information. The risk assessment tool is of two types static and dynamic and the focus in this research will be on the dynamic one. Then the research addressed the fact of where the information comes from? Here as per the title of the research the telecommunication system is the main source of the information. And on how to secure them the dynamic risk assessment model is recommended and to benchmark this literature review could be one of the sources as well as the organization itself. Finally the research reached to a main point of finding and discussing the various models of dynamic and static risk assessment methods and with further analysis and comparisons between both a new model may be found as a main outcome of this research and that model is a dynamic risk assessment model which could be suitable to be implemented in the main organization taken as a case study on this research. This new dynamic risk assessment model may be then called as a Telecommunication Risk Assessment Model.

REFERENCES

[1] Gerald V. Post a, Albert Kagan b. (2006). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. aEberhardt School of Business, University of the Pacific, 3601 Pacific Avenue, Stockton, CA 95211, United States.

[2] Sangkyun Kima, Hong Joo Leeb, (2006). A study on decision consolidation methods using analytic models for security systems. Computers and security – science direct – journal.

[3] Ray Bernard Ray Bernard Consulting Services (2007). Information Lifecycle Security Risk Assessment: A tool for closing security gaps. Computers and security – science direct – journal.

[4] Bogdan Ksie˛z_opolskia,*, Zbigniew Kotulskib,c (2006). Adaptable security mechanism for dynamic environments. Computers and security, science direct journal.

[5] Stuart P. Goringa, Joseph R. Rabaiottib, Antonia J. Jonesb,* (2007). Anti-keylogging measures for secure Internet login: An example of the law of unintended consequences aBushcraftUK, Newcastle Emlyn, UK bSchool of Computer Science.

[6] Katerina Papadaki (2008). Collaboration and Knowledge Sharing Platform for supporting a Risk Management Network of Practice. National Technical University of Athens AND Despina Polemi University of Piraeus Karaoli & Dimitriou 80 The Third International Conference on Internet and Web Applications and Services.

[7] Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, ISBN 0-471-38922-6.

[8] Bruce Schneier: Secrets & Lies: Digital Security in a Networked World, ISBN 0-471-25311-1

Authors

FIRST AUTHOR–Gamal Abdel Nassir Awad Ali Senior Lecturer & Deputy HOD, Department of Computing Science, Muscat College, Sultanate of Oman and currently a Ph.D. candidate in Information system, UTM University, Malaysia. He has published International papers in several Journals and attended International Conferences.
Email: dr.gamal.utm.security@gmail.com

Second Author–Ammar Yassir received the B.Sc. degree with Honors in Computer Science in the year 2002 from Future University, Sudan & Master in Business Administration and IT from SMU, India in 2006 & currently a Ph.D. candidate in IT, CMJ University, Shillong, India. He has published International papers in several Journals and attended International Conferences.
Email: **alfayumi@gmail.com**

Correspondence Author – Ammar Yassir, **alfayumi@gmail.com , Contact Number +96892024004**