ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

Changing Requirements of Information Security landscape

Upasna Saluja[1], Dr Norbik Idris[2]

PhD Student, Faculty of Computing, University of Technology (UTM), Malaysia[1]

Professor, Advanced Informatics School, University of Technology (UTM), Malaysia[2]

ABSTRACT:Information security risk assessment has gained importance as organisations' dependence on information has grown on the one handwhile the threat environment has become complex on the other hand. Traditional risk assessments are subjective and are have proven to be inadequate in addressing the growing complexity of identifying, analyzing and evaluating risks in recent times. Risk-related decisions are invariably based upon scores derived from rudimentary aggregation of qualitative ratings. A study of risk assessment practices over the last two decades revealed that effort has been made to make risk assessments as quantitative as possible. Literature review revealed rich potential for adaptations of risk assessment methods from other mature fields namely medicine and finance.The study proposes research and innovation requirement towards a new information security risk assessment model. This new approach should have a scientific foundation to assess and evaluate risks which should improve information security risk assessment approach by assessing risks in a more objective manner while giving due consideration to appropriate measurement unit for each specific risk area; while taking into consideration inter dependence among different risk areas.This paper lays a sound foundation for advanced innovation in the field of information risks.

KEYWORDS: Information Risks, Challenges, Information Security Risk Assessment, Qualitative, Quantitative

I. Introduction to Information Risks

Over the last three decades, organisations across industry sectors and across the world have been embracing IT to improve operational efficiencies and automate routine tasks [1]. Morteza et al [2] stated that IT has not only transformed the way business is conducted by organisations of all scales and varieties; it has also led to creating new business opportunities. Furthermore, IT has also been used by many business organisations, particularly SMEs to gain competitive advantage [3]. Organisations are finding that Information Technology is becoming a core enabler for them to deliver their services or products. A McKinsey report drives the point that technology can directly improve business performance by growing revenues through the use of technologies such as big data for cross selling across channels and reducing costs e.g. through automation and more efficient supply chains [4].

Today's organisations are producing or processing a lot of information as they go about their business. Information resides in various forms within an organisation. Information assets are all forms of equipment, storage devices, computers, IT systems, paper documents, files and even people who carry the organisational information. According to Chris and Dave [5], organisations are beginning to realize the value of information as a key asset. Many organisations even consider information as the most valuable strategic asset. In order to realise the complete potential of organisation's investments in technology and the optimisation of business performance, organisations are changing their focus from technology to information. According to the survey conducted by Cap Gemini in 2008, 80% of the organisations surveyed stated that information is a top-3 organisational priority [6].

The dependency on IT and information brings certain inherent risks. Yazar [7] stressed that while networked information systems have created many new opportunities for businesses, they have also introduced considerable risks in the process. Modern technologies such as cloud make these risks more complicated. Organisations face risks because the Information they depend upon can be accessed or modified in an unauthorised manner, destroyed, copied and even stolen. That is why it is imperative for organisations to safeguard the confidentiality, integrity and availability of information that empowers their business processes and systems. Information risks that organisations are dealing with

DOI: 10.15680/IJIRSET.2014.0310081

today can no longer be ignored or considered trivial by organisations whether they are from the public sector or from the private sector.

II. BACKGROUND TO INADEQUACIES IN INFORMATION SECURITY RISK ASSESSMENT

In earlier years, due to simplicity of the technology landscape and threat environment, the existing Risk Management Methodologies were successful in spite of being qualitative and subjective.

Currently, the technology landscape, regulatory requirements and threat environment that organisations operate in; are undergoing an unprecedented transformation which impacts the overall information security risks. This has leftthe existing risk management methods inadequate in satisfactorily addressing these risks.

III. TODAY'S CHALLENGE: LACK OF APPROPRIATE INFORMATION SECURITY RISK ASSESSMENT

Organisations seek to adopt newer technologies for growth and efficiencies without associated risks weighing them down. However, the very real and constantly worsening threat scenarios do not allow this luxury. With the changing technology landscape and the evolving threat scenario (as mentioned above), there is an urgent need to have an effective means to manage the risks that these changes and new technologies and complex threats are bringing.

This lack of a universally accepted risk management solution is validated from a very recently initiated global effort being conducted by the European Government organisation [8]starting from 2013, which seeks to critically examine the entire range of international risk management methods including frameworks such as ISO/IEC 13335-2, ISO/IEC 27001, ISO/IEC 31000, UK's CRAMM and US's SP 800-30 among others [8].

IV. RELATED STUDIES: EVOLUTION OF APPROACH IN ADDRESSING INFORMATION SECURITY RISKS

Analysis based on Literature Review of existing Risk Assessment approaches: A study of the various risk assessment methods has revealed that the key risk assessment methods deployed in information security field have evolved over the last two decades. There has been a gradual evolution in the kind of risk assessment methods over the years. Starting from purely qualitative approaches there have been attempts to transform the risk assessment approach more towards quantitative rather than qualitative techniques. The evolution of the risk assessment method was studied by the researcher and an analysis based on learnings is provided in the following sections:

1. **Initial Methods**: Qualitative Origin of Information Security Risk Management Methods

In the nineties, the requirement of information security risk management was felt across the world and international as well as regional institutions developed various methodologies, standards and guidelines to address risks. The research focused on studying the established methodologies from national endeavours such as US (NIST & OCTAVE), UK (CRAMM, BS 7799), and Asia [9] and international endeavour from International Standards Organisation (ISO 17799).

It was observed that in this initial phase, the approach was to assess risks qualitatively and the process involved organisations collecting qualitative data through surveys, questionnaires, and interviews. The analysis relied on expert judgment and involved basic computational maths based on qualitative categories namely low, medium and high.

2. **Interim Endeavours**: Towards Quantitative Information Security Risk Management Methods

In due course of time, the challenges in implementation and effectiveness of RA were realized. According to BS 7799, information was categorized in two separate categories namely 'Hard Copy Documents' and 'Information Assets', however, practically, impact was same to both the categories. Additionally, the foundation of these Risk Assessments were "assets", however, with advancement of technology, so many new type of intangible assets were being introduced into the environment, which had not been catered for earlier.

DOI: 10.15680/IJIRSET.2014.0310081

Additionally, previously the scope to define boundary of assets was easy when organisations worked within their own premises, but with time, it was realized that considering e-commerce, partner eco-systems, teleworking, mobility and Internet etc. it was difficult to draw the boundary of the organisation's assets under scope, since many activities were being conducted from outside the organisation's physical perimeter.

To handle these issues, risk management approaches started looking into quantification rather than qualitativeness. Researcher observed efforts in two directions. First, data collection efforts started to focus more towards gathering quantitative data. In this approach, endeavours were towards taking into account monetary loss during any incident or event. This estimation of monetary value of an asset, however, was never successful. In the second direction, attempts were made to transform qualitative data into quantitative data for analysis; e.g. High, Medium and Low categories were transformed into numeric scale of 15, 10 and 5. However, the results based on such mathematical calculations of transformed data were at times ridiculously impractical.

Recent years have seen increased emphasis on quantitative methods for risk assessment. ISO 27005 released in 2008 and updated in 2011, recommends that incident likelihood and consequences may be estimated in qualitative or quantitative manner. NIST standard SP 800-30 Revision 1 with its companion publications SP 800-37 and SP 800-39, leaves it to the organisation to select an approach that can be qualitative or quantitative. None of the methods, however, specify or provide guidance on what quantitative method can be used or how to approach the issue of bringing quantitative-ness into the risk assessment process.

Risk management has been criticized for being shallow rather being based upon scientific approach. Even major US government programs like FISMA which require organisations to implement risk management when managing IT systems has also been criticized for the lack of scientific rigor. Risk management appears more like a qualitative process that attempts to guess rather than predict the future risk on the basis of statistical formulations or evidence. The subjectivity in assessing the value of assets, the likelihood of threats occurrence and the significance of the impact has also been criticized [10].

3. **Recent Efforts**: Quantitative / Hybrid Information Security Risk Management Methods

Recent attempts to bring in quantitative-ness have focused on various approaches. Some of the prominent approaches like defining the loss in terms of dollar value, measuring Return on Security investment [11] are reviewed. It is evident from the quantitative approaches that the risk assessment approaches are focused on bringing in quantitativeness. Majority of these approaches have tried to collect quantitative data and attempted to assess risks in monetary terms. Even in these quantitative attempts key risk attributes such as threat likelihood and impact are still assessed in terms of rating scales or categorization in terms of low, medium and high categories. These methods have been around for a while but have not been widely adopted or accepted.

V. KEY ISSUE FOR ADDRESSING INFORMATION SECURITY RISKS

Organisations seek to adopt newer technologies for growth and efficiencies without associated risks weighing them down. However, the very real and constantly worsening threat scenarios do not allow this luxury. With the changing technology landscape and the evolving threat scenario (as mentioned above), there is an urgent need to have an effective means to manage the risks that these changes are bringing.

As mentioned in section III, this lack of a universally accepted risk management solution is underscored by the global effort of the European Governmental institution in 2013, which sought to critically examine the entire range of international risk management methods including frameworks such as ISO/IEC 13335-2, ISO/IEC 27001, ISO/IEC 31000, UK's CRAMM and US's SP 800-30 among others [8].

DOI: 10.15680/IJIRSET.2014.0310081

VI. Information Security Risk Assessment

The soul of Information Security Risk Management lies in Information Security Risk Assessment which consists of three phases namely Risk Identification, Risk Analysis and Risk Evaluation. The following sections explain all these three components in detail.

1. Risk Identification

Risk Identification is the foundation of Information security Risk Assessment in which current or potential information security risks are identified. Generally, it starts with the consideration of all the assets under scope, followed by listing of all the applicable threats to information assets while considering possible vulnerabilities.

Issues with existing Risk Identification:Today, risk practitioners are dealing with organisations of all sizes, including multinational companies which are having thousands of employees scattered all over the globe. In such organisations, any asset centric approach for risk identification is neither practical nor effective. With the current trend of outsourcing, many business processes of the organisation are outsourced. When a large amount of the organisations' business processes are outsourced to third parties, an asset centric Approach is very challenging to execute. Along similar lines, when organisations proceed towards adopting cloud technologies, many organisations resort to pay per use methods. In such situations, organisations do not necessarily own the information assets in which their data resides. Looking for an "asset owner" in these cases does not have any meaning.

In a typical information security risk management scenario, Risk Identification is an exercise which endeavours a listing of potential threats relevant to the business at a given snapshot of time. Such exercises in risk identification lack the depth of time which could have helped in understanding of the overall threat landscape capturing the trend over time.

Furthermore, risks are typically identified through discussions with internal stakeholders who may or may not possess the full context or data about the potential threats that merit attention of the organisation. For the scenarios, where data is not available, generally the risk situation is gauged based on assessors or asset owner's judgment, which is quite subjective in nature.

With these changing trends, the organisations need to transition away from an asset-centric risk assessment approach as they need to capture diverse risks in a more comprehensive and less subjective manner.

2. Risk Analysis

Risk Analysis constitutes the most important phase of information security risk management in which risk levels are analyzed for various identified risks. Existing Risk Analysis methods face the issues outlined below.

Issues with existing Risk Analysis:When it comes to risk analysis, the existing methods rely on simple non-scientific processes. These processes involve some forms of qualitative judgments where experts assess and rate various threats and vulnerabilities and assign asset values based upon qualitative ratings. These ratings and scores are in turn used to derive an overall risk score based on some rudimentary calculation.

The existing approaches for risk analysis consider diverse risks in silos whereas the fact is that in IT environment, Info Sec risks are not independent of each other; rather, they have cascading effect on other risk areas in the environment.

Additionally, when one tries to assess risks across diverse factors such as governance framework, technical network security attacks and physical exposure to thefts, current risk analysis techniques measure all the different risk areas using the same common yardstick. Doing so results in the risk analysis losingpreciseness of analysis.

DOI: 10.15680/IJIRSET.2014.0310081

3. Risk Evaluation

The objective of Risk Evaluation is to assess the level of risk in the light of the defined criteria, in order to take a decision about the approach for addressing that risk. Risk evaluation aims to determine how significant are the specific risks estimated through the Risk Analysis phase.

Issues with Risk Evaluation:Information Security Risk Assessment methods today include rudimentary methods for risk evaluation. These typically involve an organization's defined criteria for qualitative prioritization which is termed as Risk Evaluation Criteria. The risk scores that are typically used in the Risk Evaluation exercise are subjectively assigned estimated values or ratings with no effective scientific foundation. Rather, it is more of a guesstimate than a confidence inspiring scientific derivation. According to Peter et al [12], there is a dearth of model to evaluate information security risks quantitatively. So the evaluation criteria in use in current methodologies is also a subjective method relying on qualitative ratings.

Subjectivity – An issue with Information Security Risk Assessment: The existing information security risk assessment approaches are subjective in nature with risk managers largely rely upon expert judgment to make assessments that remain open to individual's interpretation due to lack of objectivity. Let us look at the picture shown here. What do you see? Are there two faces or a vase. The answer depends on a person's perception. This explains how different people can look at the same scenario in more than one way.

According to Smock, one of the well-known and accepted drawbacks in Risk Assessments is the challenge of subjectivity impacting the quality of results of risk assessment [13]. Subjective risk assessments tend to see a general lack of confidence among the stakeholders there by also negatively impacting the adoption of risk assessment. Due to subjectivity in the risk assessment process, similar risk assessments performed by other assessors may yield inconsistent results.

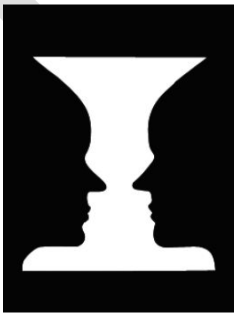

Figure 1: Subjectivity

VII. Need of the Day

Considering the above mentioned aspects of information security risks, it is highly recommended that considerable innovation be taken up to develop an approach for managing information security risks with special focus on three core phases namely Risk Identification, Risk Analysis and Risk Evaluation.

VIII. Innovation Required Based Upon Risk Assessment Approaches from Established Fields

While risk assessment is an evolving discipline in information security field, this topic is applicable across many fields and has been significantly practiced in an evolving manner in fields such as medicine and finance. However, lessons from the evolving application of risk assessmentin other fields have not apparently been adopted in information security field.

When looking at potential scientific methods that could work for information security risk assessment, the researcher discovered that there has been relevant work in other fields such as medicine e.g. development of rigorous models to study the spread of infectious diseases. These models are indeed relevant in cyber security [14] and lessons can be drawn from these models for information security. Daniel J Ryan in a presentation entitled "Statistical Analysis in Information Assurance" at The Naval Post-Graduate School Monterey, California in Jan, 2005 also highlighted the potential of drawing lessons from statistical models used by the medical community in measuring the value of proposed drugs and drug protocols. [15].

With considerable complexity and interdependence existing for large scale information systems, it is clear that important lessons need to be learned from other industries where similar complex situations have been handled successfully. In May 2008, the US State department invited industry experts, academia, scientists and policy makers to consider potential lessons from across industries such as biological immune systems, ecosystems and risk

DOI: 10.15680/IJIRSET.2014.0310081

management in financial markets. The workshop encouraged exploring information security from a metaphorical perspective towards exploring innovative and novel approaches from medical and finance fields [16].

Information security field has been using biological metaphors such as virus and worm since long ago and there is considerable potential in drawing upon biological approaches in order to develop models for addressing information security problems [17].

These developments highlighted the potential for the field of information security risk assessmentto draw suitable lessons from established fields especially medicine and finance[18].

IX. Requirement To Innovate a Scientific Approach for Risk Analysis

Joanne [19] in her article “A Scientific R&D Approach to Cyber Security”, brings out a clear need to implement a science-based approach to information security management with a strong technical basis which emphasizes that statistical methods are beneficial to address challenges in Information Security.

Similarly, Deborah Frincke from the US Department of Energy mentioned in “A Science-Based Approach - Transforming DOE Cyber Security” that in the quest of finding sustainable solutions to problems in information security, there is a need for mathematical foundation for defining and modelling challenging problems [20].

In a direct reference to use mathematics and statistics in cyber security, Juan et al in their paper entitled Mathematical and Statistical Opportunities in Cyber Security have concluded that the field of cyber security presents a rich set of new research opportunities in the area of mathematical or statistical sciences [21].

Even Charlie Catlett, CIO of Argonne National Laboratory clearly stated that Mathematics and Computational Science is largely unexplored by cyber security community [20] in a report submitted to Department of Energy in the US titled “A Scientific Research and Development Approach to Transform Cyber Security”.

Furthermore, Daniel and Bruce from Sandia National Laboratories working on a United States Department of Energy project have reported that the threat scenarios today demand that information security management needs to be transformed.. Mathematics and statistics can play a key role in understanding the cyber environment and designing solutions, which in turn would help in transforming information security [14]. In particular, the authors highlighted the value that statistics brings about in terms of data analysis especially in the presence of missing values.

All the above mentioned points highlight that mathematics and statistics are two disciplines that hold considerable promise in developing the appropriate risk assessmentapproach that overcomes the existing limitations of rudimentary, largely qualitative methods of risk analysis.

X. Proposed Innovation

Referring to the above sections, the following table outlines the key differences between the existing Risk Assessment approach and the proposed Risk Assessment approach based on innovation after conducting more appropriate study.

Table 1: Comparison between Proposed and Conventional Risk Assessment Approach

Aspects	Conventional RA Approaches	Innovation of Novel RA Approach
Guess work	Convention Risk Assessment approach nurtures guess work.	RA approach to be based on real observed scenarios where guesses have no place.
Time Factor	Assessment is based on partial knowledge of environment due to the assessment represents risks only for a snapshot of time.	Assessment should be based on complete knowledge of environment gained by observing the organization’s environment over a span of time.

DOI: 10.15680/IJIRSET.2014.0310081

Risk Calculation method	Risk Score which is essentially a function of likelihood and impact, is calculated according to rudimentary mathematics.	Risk Score should be calculated by scientific/ statistical / mathematical analysis of information.
Concurrent analysis	Conventional Analysis considers one threat at a timein siloes whilein the real world risks are not independent of each other.	Innovation should cater for considering all risk simultaneously and not one at a time.
Objectivity	Existing Risk Assessments approaches are subjective in nature and hence assessor's knowledge, experience and biasplay a significant part in risk analysis.	Risk Analysis should be done objectively so that it does not get impacted by assessors' knowledge, experience and bias.
Interdependence	Existing approaches consider each information risk as independent of the other.	Novel Risk Assessment approach should not consider each risk as independent and in fact cater for interdependence among different information risks that practically exists between risk areas.
Data Collection	Conventional Risk Assessment approaches collects data in a uniform manner in spite of diversity in risk areas.	New approachshould capture preciseness of informationby collecting data in the most appropriate manner and units of measurement considering the context of risk area.

XI. CONCLUSION

Innovation is the need of the hourin the vital area of Information Security in order to address the following question. "How Information Security Risk Assessmentcan be improved by incorporating scientific methods for managing Information Security Risks? The new Information Security Risk Assessmentapproach should be more scientific and less subjective in nature which in turn facilitates better risk-related decision making.

REFERENCES

1. Viswanath Venkatesh, M.G.M., Gordon B. Davis and Fred D. Davis, *User Acceptance of Information Technology: Toward a Unified View*. MIS Quarterly, 2003.
2. Morteza Ghobakhloo, T.S.H., Mohammad Sadegh Sabouri and Norzima Zulkifli *Strategies for Successful Information Technology Adoption in Small and Medium-sized Enterprises* 2012.
3. S. Moghavvemi, F.H., Tengku Mohd Faziharudean Tengku Feissal, *COMPETITIVE ADVANTAGES THROUGH IT INNOVATION ADOPTION BY SMES* 2012.
4. Willmott, P. *The do-or-die questions boards should ask about technology*. 2013.
5. Chris Higson, D.W., *Valuing Information as an Asset*. 2009.
6. Capgemini, *The Information Opportunity 2008*. 2008.
7. Yazar, Z. *A qualitative risk analysis and management tool*. GSEC 2002 [cited Version 1.3.
8. Security, E.U.A.f.N.a.I. *Survey of Risk Management Methods, Frameworks and Capability Maturity Models for the EU Network Information Security Platform*. 2013.
9. (MAMPU), M.A.M.a.M.P.U., *The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM)*, P.M.s. Department, Editor. 2005.
10. Katsicas, S.K., *Computer and Information Security Handbook*. 2009: Elsevier Inc.
11. *<ROSI.pdf>*.
12. Hoh Peter In, Y.-G.K., Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim. *A Security Risk Analysis Model for Information Systems*. in *Third Asian Simulation Conference, AsianSim 2004*. 2004.
13. Gary Stoneburner, A.G., and Alexis Feringa, *Risk Management Guide for Information Technology Systems* 2002(NIST Special Publication 800-30).
14. Daniel M. Dunlavy, B.H., and Tamara G. Kolda, *Mathematical Challenges in Cybersecurity*. 2009, Sandia National Laboratories: US.
15. Ryan, D.J. *Statistical Analysis in Information Assurance*. 2005.
16. Thomas H. Karas, J.H.M., and Lori K. Parrott *Metaphors for Cyber Security*. 2008.

17. Robert C. Armstrong, J.R.M., Frank Siebenlist, *Complexity Science Challenges in Cybersecurity*, in *SANDIA REPORT*. 2009.
18. Idris, U.S.a.N.B., *Information Risk Management: Qualitative or Quantitative? Cross Industry Lessons from Medical and Financial Fields.* Risk Management and Cyber-Informatics, 2011.
19. Wiel, J.W.a.S.V., *Statistical Analysis and Visualization for Cyber Security*. 2009, Quality and Productivity Research Conference.
20. Catlett, C., *A scientific research and development approach to cyber security.* . 2008.
21. Juan Mezay, S.C.a.D.B., *Mathematical and Statistical Opportunities in Cyber Security*. 2009.

BIOGRAPHY

Upasna Saluja has a Masters in Statistics and is pursuing her PhD in Computer Science with specialization in Information Security, from University of Technology, Malaysia. She is an Information Risk professional having rich experience in Information Security, Business Continuity and Disaster Recovery Management. She is currently working in Operational Risk and Compliance for Australia and New Zealand Banking Group, after having worked in companies like Thomson Reuters and HP. She has industry leading security certifications such as CISSP, CISA, CRISC, ISO 27001 and BS 25999. She has over 20 publications to her credit. She won a best paper award for her paper "Information Risk Management - Qualitative or Quantitative? Cross Industry lessons from the medical and financial field" at The 8th International Symposium on Risk Management and Cyber-Informatics: RMCI 2011, held in Florida, USA.

Norbik Idris is Professor of "Software Engineering & Information Security" at Advanced Informatics School, Universiti Teknologi Malaysia. He is also Founder of the SCAN Group of companies with a niche on information security. He is a CISSP and CISM.

DOI: 10.15680/IJIRSET.2014.0310081