Information Risk Management: Qualitative or Quantitative? Cross industry lessons from medical and financial fields

Upasna Saluja CISSP, CISA, BS 25999, ISO 27001
University of Technology, Malaysia
Kuala Lumpur, Malaysia
and
Dr Norbik Bashah Idris CISSP
University of Technology, Malaysia
Kuala Lumpur, Malaysia

ABSTRACT

Enterprises across the world are taking a hard look at their risk management practices. A number of qualitative and quantitative models and approaches are employed by risk practitioners to keep risk under check. As a norm most organizations end up choosing the more flexible, easier to deploy and customize qualitative models of risk assessment. In practice one sees that such models often call upon the practitioners to make qualitative judgments on a relative rating scale which brings in considerable room for errors, biases and subjectivity. On the other hand under the quantitative risk analysis approach, estimation of risk is connected with application of numerical measures of some kind. Medical risk management models lend themselves as ideal candidates for deriving lessons for Information Security Risk Management. We can use this considerably developed understanding of risk management from the medical field especially Survival Analysis towards handling risks that information infrastructures face. Similarly, financial risk management discipline prides itself on perhaps the most quantifiable of models in risk management. Market Risk and Credit Risk Information Security Risk Management can make risk measurement more objective and quantitative by referring to the approach of Credit Risk. During the recent financial crisis many investors and financial institutions lost money or went bankrupt respectively, because they did not apply the basic principles of risk management. Learning from the financial crisis provides some valuable lessons for information risk management.

Keywords: Risk, Risk Analysis, Risk Management, Information Risk Management, Qualitative and Quantitative Approach, Risk Management in healthcare, Financial risk management

1. BACKGROUND

The very fact that one is involved in business entails RISK. Global recession has given new dimensions & meaning to Risk. Definitely, this recession has pointed to the lacunae of Risk Assessment & Risk Management methodologies especially of financial institutions [1]. Risk is a subject of much discussion ever since its oversight is believed to have triggered the recent economic crisis. [2]

What you cannot measure, you can neither control nor improve. With an endeavor to have data driven objective assessment of risks, practitioners worldwide continuously seek to apply quantitative models, means to measure and manage risk where possible. There are a few quantitative models available to address information risk. These models are considered less customizable and often need the organization to go in for commercial off the shelf software which eventually turns out to be an expensive affair. As a norm most organizations end up choosing the more flexible and easier to deploy and customize qualitative models of risk assessment. In practice one sees that such models often call upon the practitioners to make qualitative judgments on a relative rating scale which brings in considerable room for errors, biases and subjectivity.

There is a need for a reliable and proven quantitative model for risk management which needs to be practical and easy to deploy. There are numerous mature disciplines which have engaged in assessing and managing risk for considerable period of time. The practice of risk management has indeed evolved and matured in some of these disciplines. There are definite lessons that the information security discipline can draw upon from such disciplines and their practices in managing risk.

This paper seeks to first touch upon commonly used models from both Qualitative & Quantitative Risk Assessment approaches and then brings out parallels in risk management practices from other disciplines like medical and finance, from which information risk practitioners can draw lessons.

Effective Risk Assessment is the need of the day. For security consultants, it is difficult to justify new business from a prospective client when no risk analysis has been done, to show the projected payback. For an individual company, since management typically about the bottom line, it is difficult to justify improvements in security

without proper financial analyses. For the IT systems administrators, it is a vicious cycle of firefighting for security issues when much more effective countermeasure proposals are beyond reach due to the lack of proper financial justification. Risk Management includes risk assessment and risk mitigation. In the domain of information management; analysis of risks pertains to loss of confidentiality, integrity and availability. Traditionally Information risk assessment tends to focus on risks in IT systems i.e. IT Risk Assessment, however recently, it has been established that Information Risk Assessment is vital which is much more comprehensive than IT Risk Assessment.

2. QUALITATIVE METHODS FOR RISK ASSESSMENT

Qualitative Risk Assessment which is more the norm does not operate on numerical data. The most common expression of qualitative risk is in terms of qualitative description of assets' value or service, determination of relative qualitative ratings for the frequency of threat occurrence and relative susceptibility for a given threat. Few Qualitative Risk Assessment methodologies discussed in this paper are FMEA/FMECA, NIST 800-30 and CRAMM.

FMEA (Failure Mode and Effects Analysis) and FMECA (Failure Mode and Effects Criticality Analysis) methods have been in existence from ages [3]. **FMEA** is an inductive (bottom-up) engineering analysis method. It is intended to analyze system hardware, processes, or functions for failure modes, causes, and effects. Its primary objective is to identify critical and catastrophic failure modes and to assure that potential failures do not result in an adverse effect on safety and system operation. It is an integral part of the design process and is performed in a timely manner to facilitate a prompt action by design organization and project management. FMEA is supposed to be one of the better methodologies since it provides a systematic evaluation and documentation of failure modes, causes and their effects. It categorizes the severity (criticality category) of the potential effects from each failure mode/failure cause. It provides input to the CIL (Critical Items List). It identifies all single point failures. The FMEA findings constitute a major consideration in design and management reviews. Results from the FMEA provide data for other types of analysis, such as design analysis of mission risk.

FMECA is similar to a FMEA; however, FMECA provides information to quantify, prioritize and rank failure modes. It is an analysis procedure which identifies all possible failure modes, determines the effect of each failure on the system, and ranks each failure according to a severity classification of failure effect. FMECA is a two-step process: Failure Modes and Effects Analysis (FMEA) and secondly Criticality Analysis (CA). MIL-STD-1629A, Procedures for Performing a FMECA, discusses the Criticality analysis can be done quantitatively using failure rates or qualitatively using a Risk Priority rating Number (RPN). CA using failure rates requires extensive amount of information and failure data. A RPN is relatively simple measure which combines relative weights for severity, frequency, and detectability of the failure. It is used for ranking high risk items.

The process of IT risk assessment according to **NIST SP 800-30** methodology [4] is divided into 9 basic phases:

- Selection of systems which are subject to evaluation
- Definition of the scope of evaluation, collection of needed information
- Identification of threats of evaluated systems
- Identification of susceptibility of evaluated systems
- Analysis of applied and planned mechanisms of control and protections
- Specification of probabilities of susceptibility usage by identification of the source of threats (probability is defined as: low, medium, high);
- Analysis and determination of incidents impact on system, data and organization (impact defined in three degree scale: high, medium, low)
- Determination of risk level with the help of a matrix – Risk Level Matrix – for the entire risk for identified threats. This matrix is created as a result of multiplication of probabilities of incidents occurrence (high probability receives 1,0 weight, medium – 0,5, and low – 0,1) and strength if incident impact (high impact receives 100 weigh, medium – 50, and low – 10). On the basis of matrix there is defined level of whole risk for every identified threat, determined as high for product from range (50,100], medium for range (10,50] and low for product from range [1,10].

CRAMM (CCTA Risk Analysis and Management Methodology) [5] has been accepted as the governmental standard for risk analysis and management. The process of risk management according to this methodology consists of three stages; asset identification and valuation wherein the goal is to identify and value assets, threat and vulnerability assessment in order to assess the CIA risks to assets and countermeasure selection and recommendation which identifies the changes required to manage the CIA risks identified.

This methodology uses dedicated software as an integral element supporting the three stages. The concepts of CRAMM applied via formal methods ensure consistent identification of risks and countermeasures, and provides cost justification for the countermeasures proposed [6].

3. QUANTITATIVE METHODS FOR RISK ASSESSMENT

Under the quantitative risk analysis approach estimation of risk is connected with application of numerical measures of some kind. These numerical values could be - the value of resources defined in dollar terms, the periodicity of threat occurrence in the number of instances, risk by the value of loss probability. These quantitative measures present the risk analysis outcome in the shape of indicators like a risk index of some sort. Some examples of quantitative methods in risk assessment include - Annual Loss Expectancy, Courtney's and Fisher's methods, ISRAM model etc [7].

Basic formula for IT risk assessment is -

$R = N \times L \times V$ where (R = Risk Score; N = Number of times the incident or accident is expected to happen in a defined period of time; L = Value of loss to an asset / information system because of a single incident of threat exploiting the existing vulnerability; V = Measures the possibility that a specific threat would exploit the existing vulnerability)

The most commonly used quantitative method for Risk Assessment is **Annual Loss Expected (ALE) model**. This involves calculation of single loss expectancy (SLE) of an asset. The SLE is calculated as the loss of value to asset because of a single incident. Then Annualized Rate of Occurrence (ARO) is calculated for that asset. ARO is an estimate that how frequently a threat would be exploiting vulnerability successfully. Subsequently, the Annualized Loss Expectancy (ALE) is calculated which is calculated as a product of single loss expectancy multiplied by the annual rate of occurrence. This tells the organization that how much an organization could estimate to lose from that asset based on the risks, threats, and vulnerabilities identified. In Risk Mitigation, different countermeasures are explored to address this risk which invariably leads to cost-benefit analysis to justify expenditure to implement / enhance countermeasures in order to mitigate risks faced by the asset. Sum of predicted annual losses provide Annual Predicted Loss of a company [8].

It is presented as ALE = ARO x SLE or ALE = (Probability of event) x (value of loss)

There exist many other models of IT risk evaluation and assessment, based on above method. In business it is imperative to be able to present the findings of risk assessments in financial terms. Robert Courtney proposed a formula for presenting risks in financial terms. The **Courtney's Formula** was accepted as the official risk analysis method for the US governmental agencies. The formula proposes calculation of ALE (annualized loss expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis). He emphasized on the approach that requires recognition that a control should not be implemented if it costs more than tolerating the problem. Further, no control should be implemented which is more costly or less effective or displaces less potential loss than does some other control [9]. **Fisher** proposed one of the first requirements oriented methods for information security design. He built on Courtney's checklist to develop a complete water-fall style design method [10].

4. POTENTIAL FOR LESSONS FROM OTHER EVOLVED DISCIPLINES

Risk Management across disciplines has been attempted both qualitatively and quantitatively. Quantitative Risk assessment has its inherent challenges since risks most often are not tangible. How do you quantify loss of an incident that has not occurred? Loss expectancy is believed to be one of the key measure in expressing risk quantitatively. The following sections describe approaches to Risk Analysis by bringing out the potential to derive lessons in risk assessment from other disciplines which have had a track record in managing risks, namely the medical and financial disciplines.

5. INFORMATION RISK MANAGEMENT LESSONS FROM THE DISCIPLINE OF RISK MANAGEMENT IN HEALTHCARE

Medical risk management models lend themselves as ideal candidates for deriving lessons for Information Security Risk Management. Since times immemorial man has struggled to fight disease, build better drugs as measures to augment the body's natural immune systems which fight disease and increase human survivability. The medical fraternity has constantly attempted to ward off the risks that the body faces in terms of diseases due to external factors and some intrinsic weaknesses (genetic defects, or other pre-dispositions) in the body. Since the medical fraternity needs to determine long term impacts of various drugs on fighting disease there is a considerable emphasis on empirical studies with well documented causal impact and associated effects. This empirical nature of the medical field and the constant endeavor on the part of practitioners to fight disease has led to considerably large body of data on risks faced by the body, probable causes of disease, diagnostics possible drugs and prevention measures As can be seen, the medical field lends itself wonderfully for understanding the gamut of identifying, analyzing, mitigating and managing risk. We can use this considerably developed understanding of risk management from the medical field towards handling risks that information infrastructures face. Take information assets to be patients, different incidents including hacking, malicious programs as diseases, while technical controls to mitigate risks could be considered as medicines and different processes, policies and practices can be considered as treatment protocols [11].

Over years a lot of data has been gathered in the medical field allowing for application of statistics and statistical

modeling. Application of the risk management principles derived from their use in medical field depends considerably upon knowledge of the probability distribution associated with successful attacks on information assets. Do we have such historical data available to us for us to derive probability distribution of attacks on information assets? The fact is that even today, we don't have enough real data to rely on. The solution to this non availability of data lies in use of sampling theory to arrive at statistically valid estimations of the probability distributions required.

In medical field, different groups of patients are studied by statistically analyzing the expected / observed results of usage of different medicines & different protocols. The statistical methods which are used in medical field could also be used in Information Technology provided adequate data on non-availability of assets / systems over periods of time is collected & analyzed. This would help derive statistically valid estimations for underlying probability distributions.

Field of medicine involves the complete drug development process for drug discovery, drug testing to drug marketing and mass production. Risk management which is looked at from learning perspective is "Clinical Trials" phase of drug development process. In this phase a target disease is chosen and a drug is tested for effectiveness against that target disease. The model used for drug effectiveness in clinical trials phase is the "Survival Analysis".

A target disease is chosen for study and one or more group of volunteers having the specific target disease condition are subjected to the drug for a specified period of time. These volunteers are monitored at regular intervals for their health condition to report for their response to target disease. And based on the data collected during this clinical trial, analysis is done about the effectiveness of the drug against that specific disease. Subsequently, the drug is tuned and another series of clinical trials are done till the formulation of drug matches the required levels.

Generally, survival analysis is a collection of statistical procedures for data analysis for which the outcome variable of interest is time until an event occurs. Time refers to years, months, weeks, or days from the beginning of follow-up of an individual until an event occurs; alternatively, time can refer to the age of an individual when an event occurs. Event refers to death, disease incidence, relapse from remission, recovery (e.g., return to work) or any designated experience of interest that may happen to an individual. In a survival analysis, we usually refer to the time variable as survival time, because it gives the time that an individual has "survived" over some follow up period. We also typically refer to the event as a failure, because the event of interest usually is death, disease incidence, or some other negative individual experience. However, survival time may be "time to return to work after an elective surgical procedure," in which case failure is a positive event. Most survival analyses must consider a key analytical problem called censoring. In essence, censoring occurs when we have some information about individual survival time, but we don't know the survival time exactly. The "Hazard Function" can be considered as giving the opposite side of the information given by the survivor function.

6. PARALLELS FOR INFORMATION RISK MANAGEMENT IN FINANCIAL RISK MANAGEMENT

The recent financial crisis and mortgage triggered downturn has brought to focus the failure of risk management across the financial industry. While the debate on regulation, over-regulation or deregulation continues, financial organizations are taking a hard look at their risk management practices and models. Finance industry has boasted of a fairly evolved set of risk management models and techniques. Credit risk in particular has had considerable work happening in defining the criteria, parameters and indicators of risk. Credit risk is risk resulting from uncertainty in a counter party's ability or willingness to meet its contractual obligations. Run up to the recent crises saw lenders throwing risk assessment to the winds and offering mortgaged loans to borrowers irrespective of their propensity or capacity to repay. Financial risk management discipline prides itself on perhaps the most quantifiable of models in risk management. Risks in Financial industry were naturally expected to be termed in dollar terms and the research and quantitative models developed in that manner.

Financial risk management has been a concern of regulators and financial executives for a long time. One of the key concepts in Financial Risk management is termed Value at Risk (VaR). VaR was a concept that gained ground sponsored by a large number of U.S. banks in the last two decades of the last century as the derivative markets developed. With VaR, banks developed a generic measure of economic loss that could equate risk across products and aggregate risk on a port-folio basis. VaR is defined as the predicted worst-case loss at a specific confidence level over a certain period of time. [14]. For a given portfolio, probability and time horizon, VaR is also defined as a threshold value such that the probability that the mark-to-market loss on the portfolio over the given time horizon exceeds this value (assuming normal markets and no trading in the portfolio) in the given probability level [15]. One of the key benefits of VaR-based risk management is the improvement in systems and modeling it forces on an institution. Per Philippe Jorion the greatest benefit of VAR lies in the imposition of a structured methodology for critically thinking about risk.

The measurement and reporting of Information Security Risks is still undeveloped as compared to that of Market

and Credit Risks. Credit Risk is the risk of loss of principal amount or a financial reward stemming from a borrower's failure to repay loan or meet a contractual obligation. Credit risk is closely tied to the potential return of an investment. Credit Risk is calculated by calculating expected losses that can arise at the time of default.

Expected losses = EAD (exposure at Default) × PD (probability of default) × LGD (loss given default) where EAD is an estimation of the extent to which a bank may be exposed to counterparty in the event of, and at the time of, that counterparty's default. EAD is equal to the current amount outstanding in case of fixed exposures like term loans. Probability of default (PD) is the likelihood of a default over a particular time horizon. It provides an estimate of the likelihood that a client of a financial institution will be unable to meet its debt obligations. LGD is the credit loss incurred if an obligor defaults. LGD is calculated by dividing total loss by exposure at default (EAD). For Example:- A bank has total exposure of Rs.100000. The probability of default is 10% and Loss at given default is 60% as 40% is recovered against the assets mortgaged by borrower to the bank to get a loan. So, Expected Loss = EAD × PD × LGD = 100000 × .1 × .6 = Rs.6000

This approach could be applied to Information Security with EAD corresponds to exposure of an asset to a particular threat, PD corresponds to rate of successful attack due to a threat exploiting vulnerability and LGD corresponds to percentage loss on an asset due to an attack.

7. MAPPING SOME OF THE LESSONS FROM THE FINANCIAL CRISIS TO INFORMATION RISK MANAGEMENT

During the recent financial crisis many investors and financial institutions lost money or went bankrupt respectively, because they did not apply the basic principles of risk management [17]. Firstly, risk appetite was not well stated in many firms. This is a key issue in Information risk management too. It is very often not clear how much residual risk is the management ready to take. Many senior management executives charged with taking decisions on risk appetite often skirt the issue rather than addressing it head on. Secondly, enterprise risk management was not well defined or used. Information Risk Management too needs to be viewed holistically as part of the larger business risk or the Enterprise risk framework. Where information risk management operates in a silo and does not roll up into Enterprise or Organizational risk management there is a chance that the overall import of it may be lost and business may not prioritize resources required to handle it well. Thirdly, relevant risk-management policies were not supported by top decision makers. In fact, risk management in many organizations appears to have been cyclical, peaking only after the crisis reached full-blown proportions. As many security practitioner report information security initiatives launched with overtly visible senior management support are more often likely to succeed than those without. Fourthly, the increasing complexity of structured finance created challenges in terms of efficient management and the dissemination of information. This relates to Information security directly where in more complicated the control greater is the difficulty in understanding the risk picture. In security too the KISS principle works well – Keep it Simple Simon. Lastly in the final analysis, more due diligence with respect to risk is absolutely necessary both for senior management and investors. In information security too it is absolutely vital that appropriate due diligence is exercised both for senior management and users [17].

8. CONCLUSION

The debate over qualitative and quantitative models in risk management continues to rage across disciplines with practitioners. Factors that have made practitioners choose the qualitative models over quantitative ones have included ease of deployment, customizability and cost of implementation. However, the drawbacks in qualitative models in terms of reliance on expert opinion, qualitative ratings with inherent biases and subjectivity, have led to a constant endeavor among researchers and practitioners to look for quantitative models that are easy to use and implement. Mature disciplines such as the medical profession and finance have long relied on risk management practices to prevent operational losses. Information Risk practitioners need to draw from other such disciplines where risk management practices have evolved and matured with time. Considerable more work needs to be undertaken to identify such opportunities for adoption of risk management models and customizing them to suit the ephemeral world of often "virtual risks" in the information risk management discipline.

9. REFERENCES

[1] The Financial Crisis and Lessons for Insurers , September 2009: http://www.soa.org/files/pdf/research-2009-fin-crisis.pdf

[2] Financial Risk Management: http://ayushveda.com/blogs/business/financial-risk-management-after-the-economic-recession/

[3] FMEA : http://www.fmeainfocentre.com/papers.htm

[4] NIST Sp 800-30: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[5] A Qualitative Risk Analysis and Management Tool – CRAMM: http://www.sans.org/reading_room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm_83

[6] CRAMM : http://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm

[7] Quantity RA step by Step: http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849

[8] Quantitative risk assessment : http://en.wikipedia.org/wiki/Risk_assessment

[9] Fisher & others RA models: http://www.tawileh.net/anas//files/downloads/papers/InfoAssurance-SSM.pdf?download

[10] Courtney's RA model: https://www-950.ibm.com/blogs/visible/entry/the_beauty_of_guesstimates?lang=en_us

[11] Quantitative Risk Assessment for Medical and Veterinary Public Health Officers and Researchers, Mar 2008: http://www0.sun.ac.za/sacema/BTC_QRA.pdf

[12] Some issues in the quantitative modeling portion of cancer risk assessment, Sept 2004: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6WPT-4DDP3CW

[13] Book - Medical Statistics at a Glance By Aviva Petrie, Caroline Sabin: http://books.google.co.in/books?id=upQ5tlFEc1sC&pg=PA45&lpg=PA45&dq=use+of+statistics+in+Risk+Analysis+medical&source=bl&ots=RM1k03LNZY&sig=XI6grLzJWXvbxGMvlGnnBlkWs14&hl=en&ei=uuGtTJafO42OvQOkkp3PBg&sa=X&oi=book_result&ct=result&resnum=10&ved=0CC0Q6AEwCQ#v=onepage&q&f=false

[14] Risk Management in Financial Services Industry: An Overview – Arjun C Marphatia & Nishant Tiwari http://public.intensum.eu/brochures/risk_management_fsg.pdf)

[15] Philippe Jorion, Value at Risk: The New Benchmark for Managing Financial Risk, 3rd ed. McGraw-Hill (2006). ISBN 978-0071464956 - http://en.wikipedia.org/wiki/VaR#cite_note-Jorion-0)

[16] Structured finance, risk management, and the recent financial crisis, by Georges Dionne http://www.iveybusinessjournal.com/article.asp?intArticle_ID=869)

[17] Challenges to Sustainable Risk Management: Case Example in Information Network Security, Pinto, C Ariel, http://www.allbusiness.com/finance/business-insurance-risk-management/4080361-1.html

[18] Quantitative Risk Analysis: http://www.statistics.com/ourcourses/risk

[19] The Financial Crisis and Lessons for Insurers , Sept 2009: http://www.soa.org/files/pdf/research-2009-fin-crisis.pdf

[20] Relative risk: http://en.wikipedia.org/wiki/Relative_risk

[21] Financial Risk Management - http://ayushveda.com/blogs/business/financial-risk-management-after-the-economic-recession/

[22] Enterprise Information Technology Security: Risk Management Perspective: http://www.iaeng.org/publication/WCECS2009/WCECS2009_pp1171-1176.pdf