International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010
1793-8163

Parameter Extraction for Measurement of the Effective Information Security Management - Statistical Analysis

Abhishek Vaish and Shirshu Varma, *Member IEEE , IAENG,*

***Abstract*— this paper critically analyzes the current well defined practice to manage the risk for information security managements that contains numerous flaws in terms of valuation of risk due to the fact that the parameter to measure risk is not established accurately. Critical parameter plays an integral part to establish an effective information security management system. Risk can only be measured properly if the parameter for data collection is precisely identified. Hence, the present work basically, considers the Information Security Management System (ISMS) parameters as the subject of study that will assist the organization to reinforce the security management at a very low cost. Based upon the statistical analysis of the responses received, the interventions in each area of the information security and management have been prioritized. The statistical analytical study finally claims that the identified interventions shall not only give a complete facelift to the way in which information security and management system are operative and managed today but also assist them in sustaining quality as demanded by society and other stakeholder.**

***Index Terms*—Risk Management, Information Security Management, Critical parameters, Security Evaluation.**

I. Introduction

The current digital era had exposed the organization to variety of event that brings negative outcome like reputation, financial loss, productivity etc. A system that can be dedicated to track the organization capability to sustain & withstand the uncertainty of risk of various kinds and to hover around with precise navigational devices plays an integral role in the success of the organization. This navigational process is possible only if a robust system is developed and deployed to the organization which may be known as information security management system. The recent research shows that the enforcement of ISMS in the organization is growing rapidly as can be clearly with the survey conducted by the ISO in the 2007 which depicts a growth of 33 % in 2007 compare to 2006 and a total of 5797 certificate and 7732 respectively were issued to the organization in 70 countries [1]. Additionally the observation recorded in one of the survey conducted by Comptia shows that 80 % of the respondents are of the opinion that the breach in security system is due to the lack of I.T Security, knowledge and lack of training [2], Additionally if we look at the quantum of loss in $ Value "$168,000 in last year's report to $350,424 in this year's i.e. 2007[FBI/CSI,2007]. The fundamental problem behind this gap i.e. high information security initiative and increase in the security incident draws attention toward understanding root cause behind the problem and one of the problem root is surfaced deep with the evaluation of the ISM, that can be possible only if the parameters that are capable to address the organization need for making it sustainable to be identified and explored correctly & precisely. Through this research work we are trying to investigate the critical parameter representing the ISM and to prioritize it through statistical analysis the final results will be the identified parameter that can be used for evaluation of the ISM.

The new result will minimize the cost drastically and will also assist the organizations to identify the vulnerable area must faster than the traditional methods. The parameters evolved helps to measure risk and its association with critical factor of ISMS. [15]

Indian Institution of Information Technology, Allahabad, India.

II. Related Work

The need for the measurement of the information security management has been envisaged since 2002 in the work of Siponen [6] that has acknowledged the need of an adequate maturity measurement. Additionally, the scale used for the measurement can handle the software capability that has many criticisms to it.

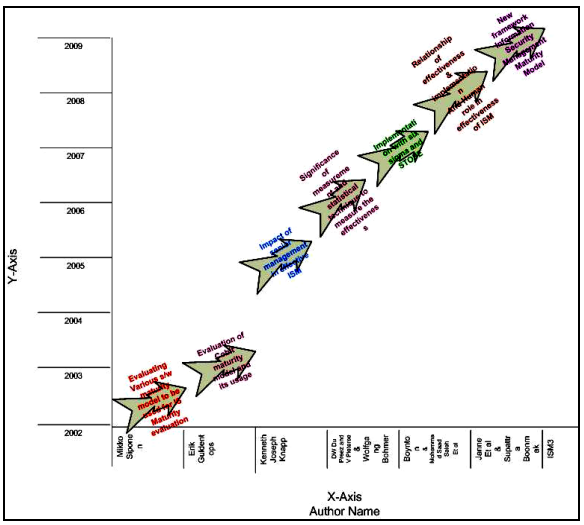

Fig. 1 published (2002-2009). Source at http://amrita.edu/cyber-workshop/proceedings/icscf09_submission_101.pdf /Fig2

Evaluation of the effectiveness of the Information security management has various perspective and techniques that has

been started up with up with the work of Blackey et al [17] where the parameter used for the evaluation of the ISM were related to the financial aspects and the objective for the measurement is to monetize the loss with the particular incidence. However, the results were not validated. Similarly in the work of Hong et al [18], the work was related with presenting a risk management approach to implement ISM using integrated theories. In the work of Bohmer[19], the measurement used to evaluate the effectiveness were on the basis of scope of the ISM that includes the coverage of the business process, the controls operationalization and the completeness of the security policy. The selection of the parameters was qualitative and was not validated. One of the ways to ascertain the ISM is through compliance measurement of the standards and best practice available Preez et al [9]. The author in his work had presented few statistical techniques with the merits and demerits and finally presented a new derivation to calculate the compliance ratio in lines with the arithmetic mean. The work can be utilized as the framework that can be used to compute the compliance score of the organization based on IS0 17799 standard but does not have the capability to predict and forecast the areas of missing control and the scale used in the work doesn't have much of choice to the respondent's organization to express the true status of the ISM The trustworthiness of the standard itself is an issue. ISO/IEC 17799 certification can give organizations or their interest groups a false sense of security Wiander [15]. Baker Et Al, 2007[20] attempted to provide a much sophisticated technique to evaluate the ISM, the parameters used in the measurement were the NIST classified controls i.e. Technical Operational, Management and ANOVA test has been used to understand the organizations control deployed schema. The result shows that the organizations are allocating more fund on the technical control and less on the management control which subsequently been addressed in the work of Knapp Et al [21] proposed a theory and to measure the effectiveness of information security management and emphasized the significance of the implementation on effectiveness. The parameter used for the measurement were related with the management control aspects like understanding the user behavior, policy enforcement, top management role with effective information security management. The result shows that top management support helps in the enhancing the effectiveness of the ISM. Code of ethics should be developed, this will help to develop good human behavior and plays an important role in the reduction of the risk, the study also gives a strong foundation by saying that experience does not affect the development of the code of the ethic and all can participate for this Boonmak[22]. Similarly, in the work of Hagen et al [13] the measurement consideration was implementation effectiveness and the parameter used for the measurement are security policy, Procedure & control, Tools and method, Awareness creation. However, the parameter identified were on the basis of the implemented security measures by the organization and not on the basis of the identifying the parameter in isolation. The result of the findings may not have comprehensive parameter as the objective for the evaluation was to measure the security performance not the parameter extraction. The lack of evidence to identify the critical factors and indicators make the management of information system a tough challenge Torres et al [16]. Figure 1 depicted below highlights the major development in the area of Information security management implementation and allied areas.

III. Research Design

The investigation has been conducted with the data set collected by floating a questionnaire consist of 14 questions derived with the analysis of critical data point(parameter) used by the auditor to measure the security posture of the organization. The questionnaire had been floated among the subject matter experts and the results were complied to perform various statistical tests with a sample size of 130 domain expert respondents.

IV. Analysis & Findings

The current study endeavored to explore the parameters that are critical in terms of their performance and evaluation for the measurement of the effectiveness of the information security management. Based on the literature review it can be seen that the measurement of ISM is highly dependent on the motivation behind the measurement i.e. "what is to be measured?" and "how to measure?" Vaish Et al [23] . The literature review reveals the fact that various framework has been used for the measurement of the information security effectiveness from the perspective of the security performance and majority of the framework either have select the parameter for measurement based on literature survey or based on the patter of the control deployed in the organization. The existing work has their own strengths and weakness. However, if the identification of the parameter is done merely on the basis of the byproduct of some other measurement it may bring risk to the entire framework. Hence, in our work we may attempt to extract the parameter with the objective to extract the parameter those are critical for the measurement of the Information security management. Further, after identification of the core constituent areas with the associated information management and security issues, a questionnaire comprising of 14 questions was designed specially and sent generously to the persons of related fields. These basically include academicians and persons from industry. The persons were requested to priorities the process as per the efficacy and impact. In all about 130 responses were received comprising of both academia and industry person, and these were subjected to statistical analysis and the result was summarized. Thus, in this paper the ratings given by the respondents were subjected to the statistical analysis of the probability distribution function and the distribution function is plotted.

Finally to priorities the parameters, the moment of the distribution measure like - central tendency, dispersion, skewness and Kurtosis were evaluated. Thus, with the help of these statistical parameters out of 14, 6 information security and management optimized parameters were identified and calculated.

The 14 information security management parameters defined in the survey are as follows:

1) Identity and access management as an integral part of the

implementation of the information security management system.
2) Preserving evidence, investigation technique and tool as the integral part of ISMS.
3) Ability to put policy into practice.
4) Effectiveness of the information security management system.
5) Possibility of the regular communication with the stakeholder.
6) If information security management system is not effective, will it bring risk to the organization?
7) If the scope is not defined properly, the security considered will be ineffective (Y3).
8) Effective risk management activities to contribute the success of the information security management (Y6).
9) Impact of inadequate human and other resources and knowledge to observe the quality of the information security management system (Y5).
10) Without proper technological control whether the organization can be secured from all kind of information system risk or not (Y2).
11) Whether senior management commitment plays an integral part for the implementation of ISMS (Y1).
12) Is identifying the business process for the information security is the right way to protect the information asset (Y4).
13) Is information security management system implementation is only required to achieve the certification from the accreditation body?
14) Is information security is simple antivirus software and firewall implementation?

Out of these 14 information security management system parameters the respondent statistical measure are as follows:

TABLE 1

Statistical Measures					
S.No	Parameter	Mean	Variance	Skewness	Kurtosis
1	Access Control	5.67	6.20	-0.176	4.00
2	Incidence Response	4.26	5.52	-0.402	**5.52**
3	ISM Governance	6.28	5.41	-0.487	5.41
4	Auditing Findings	5.43	6.00	-0.602	4.00
5	Communication & Correspondence	6.25	5.66	-0.611	5.66
6	Ineffective ISM	6.33	5.36	-0.610	5.36
7	Scope defined	6.42	6.91	-0.293	11.76(Y3)
8	Risk Assessment	5.91	6.05	-0.307	9.35(Y6)
9	Adequate knowledge and Human Resource	6.43	8.22	-0.259	9.77(Y5)
10	Technological Control Implementation	6.68	7.87	-0.842	11.87(Y2)
11	Senior Management Commitment	6.39	5.26	-0.62	15.26(Y1)
12	Business Process And Asset Classification	6.17	6.76	-0.59	10.76(Y4)
13	International Certification	6.45	4.62	-0.61	4.62
14	Anti Virus	6.49	5.12	-0.83	5.12

Based on the responses received we can see that all the parameter were having are closely related with the information security management and this may be a clear sign of the fact that how the field information security covers multidimensional and requires a thorough analysis to estimate the correct parameter representing the object.

Further on, the depicted table reveals that the calculation has been done with respect to mean, variance, skewness and kurtosis. Further, the prioritization of individual parameters like scope defined, risk assessment, adequate knowledge and human resource, technological control, senior management commitment and business process are all negatively skewed this emphasize that the priority has to be done on the basis of fourth statistical moment i.e. kurtosis. Also, it has been observed that the mean and variance differ very slightly for all the defined parameters the numerical value ranges from 5.26 to 6.42 for mean and 5.62 to 8.22 for variance. Therefore the central dispersion tendency of the parameters is less for defining the peak value or prioritizing the output.

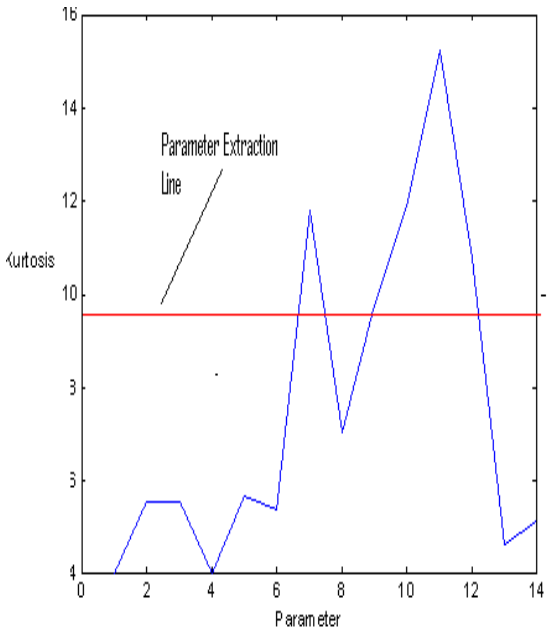

Fig 2.Depicts the kurtosis value Vs parameter extraction Graph

The depicted graph (Figure 2) claims to provide the extracted parameter. The red line "Parameter Extraction line" is derived with the kurtosis upper and lower values i.e. 15.26 for the parameter "Senior Management Commitment" and 4.0 for the parameter "Access Control" respectively. The centroid of the two score is computed with the equation (1)

$$C = (\text{Upper}+\text{Lower})/2 \quad (1)$$

$$= (15.26+4)/2 = 9.63$$

The value for deriving out the parameter considered to be successful parameter for calculating the effective ISMS is 9.63using equation (1). The parameter under the consideration for measurement should have fourth ordered of statistical moment i.e Kurtosis greater than equal to 9.63

rounded off to 9.6.

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} = \frac{1}{\sigma}\phi\left(\frac{x-\mu}{\sigma}\right) \quad (2)$$

Where

$f(x)$ = probability density function
μ = mean

And cumulative distribution function is calculated using equation (2) and (3) respectively.

$$\frac{1}{2}\left[1 + \operatorname{erf}\left(\frac{x-\mu}{\sigma\sqrt{2}}\right)\right] \quad (3)$$

The distribution plot of both probability distribution function and cumulative distribution functions are as follows that has been computed using equation (2):

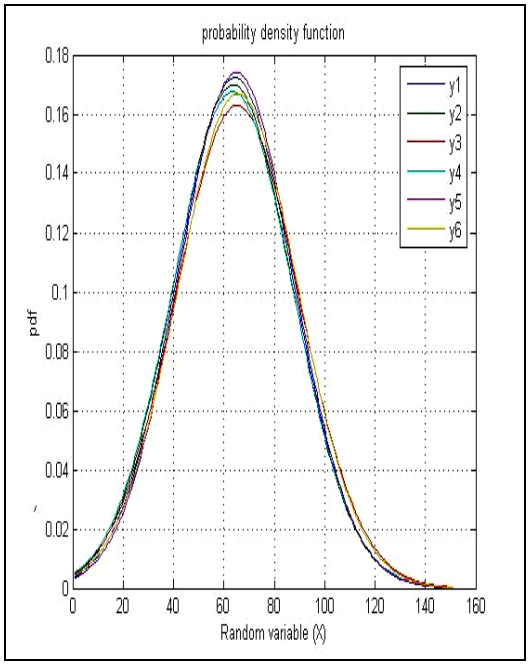

Fig 3 Probability Density Function of the depicted parameters

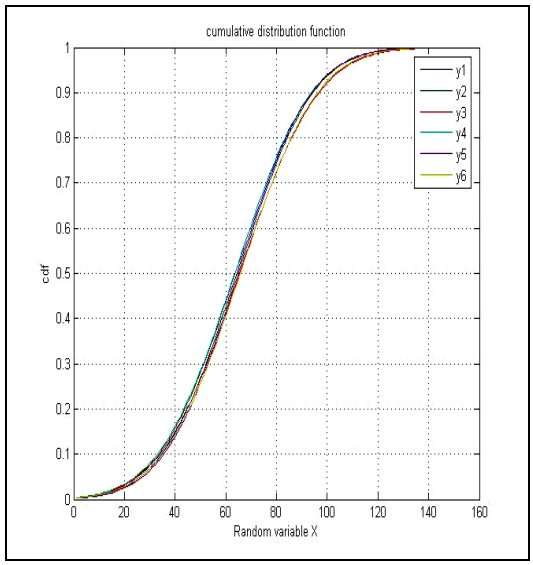

Fig 4 Cumulative Density Function of the depicted parameters

Fig 3 and 4 represents a Normal Probability Distribution Function plot from MATLAB Ver.7, (calculate using equation 1) for the 6 prioritized parameters of the information security management in terms of its pdf and cdf.

With the help of these (pdf) and (cdf) plots we basically can define

1) Database of the information security and management parameters on approved procedures & practices for all the prioritized parameters.
2) This basically allows us to centralize continuous variable values with its mean.
3) It allows also the results of a transformation to have a standard normal distribution.
4) With the different values of the mean and variance the normal distribution is a large family with the about 6 parameters and also they have some common properties.
5) With the help of values of the respondents the parameters are plotted that basically reflects the current understanding of the unique aspects of network security parameters user information, and the relationship between predictors and the network security related response variables.

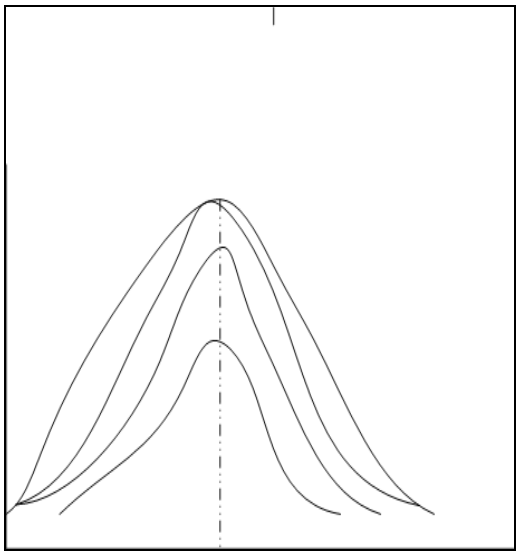

Fig 5 Probability Density Function of the depicted parameters

Now the survey here clearly indicates that that the statistical interviewers are very effective in achieving the desired objective for each o the sub goals. It has also revealed that the central tendency of the parameter emphasized less relative affect to the respondents, which clearly emphasized that the importance of the respondent data is related to accountability, monitoring and assessment of the parameter. Thus, with this measure the parameters are as follows:

1) If the scope is not defined properly, the security considered will be ineffective.
2) Effective risk management activities to contribute the success of the information security management.
3) Impact of inadequate human and other resources and

knowledge to observe the quality of the information security management system.

4) Without proper technological control whether the organization can be secured from all kind of information system risk or not.
5) Whether senior management commitment plays an integral part for the implementation of ISMS.
6) Is identifying the business process for the information security is the right way to protect the information asset.

Hence, the prioritization of these 6 parameters out of 14 provides also the predictive and feedback monitoring issues with other related activities. It involves finally the innovative and independent thinker to become an integral part for the implementation of ISMS.

Now further, in order to know whether the independent constituent can be measured for the achievable quality. The correlation coefficient among the prioritized 6 parameter has also been evaluated. For, in order to evaluate the*correlation coefficient*, using equation (3):

$$r = \frac{n\sum xy - \left(\sum x\right)\left(\sum y\right)}{\sqrt{n\left(\sum x^2\right) - \left(\sum x\right)^2}\sqrt{n\left(\sum y^2\right) - \left(\sum y\right)^2}} \quad (4)$$

Where

r = correlation coefficient
n= number of scores
∑xy= sum of the product of the scores
∑x=sum of X-scores
∑y=sum of Y-scores
∑x2 = Sum of the squared X-scores
∑y2 = Sum of the squared Y- scores

For the analysis of inference we shall be using the concept that if the correlation is negative, we have a negative relationship among the parameters, if it is positive, the relationship is positive. Further after evaluating the coefficient of correlation among these prioritized 6 parameters we shall also be performing the significance test of correlation.

TABLE 2

Parameter	X(Y1)	Y(Y6)	XY	XX	YY
1	67	3.6	195.0	4489	12.96
2	68	4.4	299.2	4624	19.36
3	71	4.3	305.0	5041	18.49
4	69	3.8	262.2	4761	14.44
5	68	3.6	244.8	4624	12.96
6	67	3.6	241.2	4489	12.96

Solving the above for the correlation between Y1 and Y6 is .62(using the above equations) which no doubt is very strong which clearly depicts the strong relationship between Y1 and Y6.

V. Conclusion

Organizations are finding it difficult to measure the health of the ISMS of their organization due to the problem of scaling. The results shown here can be very useful for the organization to use and measure the effectiveness of the ISMS. The current result shows that out of 14 important parameters 6 i.e. Scope defined, Risk Assessment, Adequate knowledge and Human Resource, Technological Control Implementation, Senior Management Commitment, Business Process and Asset Classification have the value that is beyond the lower threshold calculated by using equation (1). Also, the correlation test using equation (4) computes the score between Y1 and Y6 is .62 and prove to claim a correlation between the two upper and lower kurtosis values parameter this can be interpreted that the parameters indentified are precise to calculate the effectiveness of the ISMS.

References

[1] ISO Central Secretariat, "The ISO Survey of Certification 2007" available at www.iso.org
[2] ComTIA, available at http://www.trainingpressreleases.com/newsstory.asp?NewsID=582
[3] Garry Dinne, "The Second Annual Global Information Security Survey", Information Management & Computer Security Year:1999 ,Volume:7 Issue:3 Page:112 - 120
[4] LSEC "IT Security Management: Standard for Today's Businesses" , 2006 available at http://whitepapers.techrepublic.com.com/abstract.aspx?docid=378491
[5] Jerry Bryer, "Critical Success Factors for SOX Implementation" , available at http://www.anexinet.com/pdfs/SOX_successfactors5-2006.pdf
[6] Mikko Siponen , "Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria", Information Management & Computer Security,Year:2002 ,Volume:10 Issue:5,Page:210 – 224
[7] Kenneth J. Knapp, "A Mediation Model Of Managerial Effectiveness In Information Security: From Grounded Theory To Empirical Test "International Journal of Information Security and Privacy, Year 2007,Volume 1, Issue 2, Page: 37-60.
[8] Wolfgang Bohmer, "Evaluation of the Quality of an Information Security Management System (ISMS) available at http://www.ansatt.hig.no/erikh/boehmer.ppt.
[9] D W du Preez and V Pieterse, "CALCULATING COMPLIANCE STANDARDS" available at http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/32_Paper.pdf.
[10] Mohammad Saad Saleh, "Using ISO 17799: 2005 information security management: a STOPE view with six sigma approach", International Journal of Network Management, Year: 2007, Volume 17, Issue 1, Pages: 85 – 97.
[11] Brian C. Boynton, "Identification of process improvement methodologies with application in information security", Proceedings of the 4th annual conference on Information security curriculum development, Year:2007, Article No. 28 .
[12] Supattra Boonmak, "Influence of Human Factors on Information Security Measures Effectiveness under Ethic Issues" Submit to 8th Global Conference on Business & Economics, Year:2008, ISBN : 978-0-9742114-5-9.
[13] Janne Merete Hagen, "Implementation and effectiveness of organizational information security measures", , Information Management & Computer Security,Year:2008 ,Volume:16 ,Issue:4 ,Page:377 – 397.
[14] ISM3 Consurtium, "Maturity And Capability Levels Mapped" available at"http://www.ism3.com/index.php?option=com_docman&task=cat_view&gid=1&Itemid=9
[15] Timo Wiander "Implementing the ISO/IEC 17799 standard in practice– experiences on audit phases". ACM International Conference Proceeding Series; Vol. 328 archive Proceedings of the sixth Australasian conference on Information security – Year:2008 Volume 81 table of contents Wollongong, NSW, Australia SESSION: Contributed papers: protocols and practices table of contents Pages 115-119
[16] Jose M Torres, Jose M Sarriegi, Javier Santos and Nicolás Serrano "Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness" Springer Berlin / Heidelberg Volume 4176/2006 Year:2006, Pages 530-545

[17] Bob Blakley. The measure of information security is dollars. In Proceedings of The First Workshop on Economics and Information Security (WEIS2002), May 2002.
[18] Kwo-Shing Hong, Yen-Ping Chi, Louis R. Chao, Jih-Hsing Tang " An integrated system theory of information security management" Journal Information Management & Computer SecurityYear:2003 Volume:11 Issue:5 Page:243 – 248
[19] Wolfgang Bohmer, "Evaluation of the Quality of an Information Security Management System (ISMS) available at http://www.ansatt.hig.no/erikh/boehmer.ppt.
[20] Wade H. Baker and Linda Wallace. Is information security under control?: Investigating quality in information security management.IEEE Security and Privacy, 5(1):36–44, 2007.
[21] Knapp, Kenneth J.; Marshall, Thomas E.; Rainer, Jr., R. Kelly; Ford, F. Nelson" Information Security Effectiveness Conceptualization and Validation of a Theory: International Journal of Information Security and Privacy,Year: 2007 Vol. 1, Issue 2 pages 37-60.
[22] Supattra Boonmak, "Influence of Human Factors on Information Security Measures Effectiveness under Ethic Issues" Submit to 8th Global Conference on Business & Economics, Year:2008, ISBN : 978-0-9742114-5-9.
[23] Abhishek Vaish and Shirshu Varma "Proposed Next Generation Information Security Management Effectiveness Measurement Model" available at http://amrita.edu/cyber-workshop/proceedings/icscf09_submission_101.pdf/ Year: 2009.

Abhishek Vaish is faculty at Indian Institute of Information Technology-Allahabad. He is pursuing his Phd from Indian Institute of Information Technology- Allahabad in the area of information security. He has 10 paper published in the area of information security, computer forensics and sensor network and member of International Association of Computer Science and information technology, Singapore. He has a 5 years of including corporate and teaching. His current area of research includes image processing, cyber crime investigation, information security in health sector and wireless sensors network.

Dr. Shirshu Varma after completing his PhD served many organizations like BIT Mesra Ranchi, IET Lucknow, C-DAC Noida in the capacity of lecturer, Sr. lecturer & IT Consultant. Presently he is working Assistant Professor in IIIT Allahabad. Dr.Varma has published about 32 papers in international and national journals and conferences of repute. He is a member of IEEE and life member of ISTE. He has been a recipient of many national awards in this area. His areas of interest are intelligent sensor network, wireless sensor network, Optical wireless communication, Wireless communication & network.