Factors Affecting Malware Attacks: An Empirical Analysis

Ajay Kumar
School of Business Studies, Sharda University, Gr, Noida & Delivery Project Executive (IBM India Limited), U.P., India
E-mail: akg_d78@yahoo.co.in
Nishikant Ojha
Associate Professor, School of Business Studies, Sharda University, Gr, Noida, U.P., India
Nishit Kumar Srivastava
Assistant Professor, Operations and IT department, ICFAI Business School, Hyderabad, India

Abstract

It has been well proved that malware attacks results in a loss of wealth and security to individuals and organizations. So, it is of utmost importance to understand that how a person or an organization becomes a victim of malware attacks. To understand the issues affecting malware attacks an empirical analysis was carried out. Firstly, factors affecting malware attacks were identified and a model was proposed, subsequently SEM (Structural Equation Modeling) was carried out to validate the proposed model and finally, regression analysis was used to establish the importance of the identified factors.

Keywords : *malware attacks, issues in malware attacks*

Introduction

Other than the social, economic and productive growth seen across the globe due to computer technology and internet penetration, there is another flip side of coin as well reported as criminal activities named as cybercrime. Malware attack is one of the most prevalent and devastating form of cybercrime. The growth of internet user-base and penetration is integrated to instant computer crime.

Malware attacks are now a day's common and may cause severe damage to any kind of institution or even economy. Such criminal offence was first recorded in year 1820 when the employee of one French textile company committed the act of vandalism in their company because the owner of company Mr. Jacquard manufactured the loom. This was a device to use for having repetitive steps of fabric weaving and all the employees felt threatened about their employment and livelihood (C´ardenas et al., 2016; Singh, 2007; Goth, 2005).

Recently Ransom ware can be cited as one of the examples which created huge panic situation around the globe resulting in huge financial loss to several individuals and organizations. According to the UN manual published in 1994, noted that any, illegal production or reproduction of computer programs will a consider as type of cybercrime. This step was in continuation of international dimension of computer crime and related criminal legislation which was considered and accepted in year 1979 (Singh, 2007; Goth 2005).

It has been well proved that malware attacks results in a loss of wealth and security to individuals and organizations. So, it is of utmost importance to understand that how a person or an organization becomes a victim of malware attacks. To understand the issues affecting malware attacks an open ended questionnaire is administered and is sent to various IT- industries in Indian sub-

continent. Capital Line 12 database was used to prepare the list of Indian IT companies to conduct the study. Capital Line provides information of 26873 companies out of which 4618 are IT companies. The list of the Indian IT companies was prepared in November 2012. It is expensive and time consuming to survey all the 4618 companies so surveying a suitable sample is the best technique to get the required data.

Determination of Sample Size

Yamane (1967) provided a simplified formula to calculate the sample sizes which was used to calculate the number of samples. A 95% confidence interval with 5% precision level gives the required number of sample to be 317 approximately. Previous studies show that 15-25 per cent is the rate of valid responses that a researcher gets back, so, the sample size was increased to 1268 considering 25 percent valid responses. Simple random sampling technique was used to derive the list of the company for the study. Finally, questionnaires were mailed to each company included in the sample.

Survey was carried out for the period of 6 months starting from December 2014 to May 2015. Despite of repeated follow-ups by phone and e-mails only 200 valid responses were received at the end of 6th month. To increase the response rate personal meetings and industry visits were conducted at Delhi, Noida, Ghaziabad, Faridabad and Bangalore. Total of 374 responses were received, out of which 323 responses were valid and 51 responses were incomplete.

Issues in Malware Attacks

From the responses received, the compiled list of issues affecting malware attacks is as given in the Table below and is almost similar to what we got for phishing.

Table 1: List of issues affecting malware attacks

S.No.	Issues	No. of respondents
1	Lack of knowledge	308
2	Lack of awareness	378
3	Carelessness	347
4	No software protection	279
5	Improper software protection	395
6	Using public computers	257

The above mentioned six causes have been identified as the major factors affecting malware attacks:

Lack of knowledge

Lack of knowledge of malware and its type resulted in corruption of confidential data and hence resulting in loss of wealth due to manipulation, downtimes and restructuring of the infected systems.

Lack of awareness

Lack of awareness hampers decision-making process in which the person is unable to identify malware attacks.

Carelessness

Even after having a proper knowledge about malware attacks the person due to work pressure/mental tension is unable to identify malware.

No software protection

No software protection is provided in the system increasing its vulnerability to malware attacks.

Improper software protection

In a quest to avoid investment on antivirus / firewalls, companies buy sub-standard software protection which does not provide enough protection against malware attacks.

Using public computers

Due to lack of resources some employees are forced to use public computers (computers at cybercafé/ someone else's computer) which are mostly malware infected causing loss of confidential data.

Losses due to Malware Attacks

From the responses received several types of losses are identified which are as given in the table below:

Table 2: Types of Losses

S.No.	Types of losses	No. of respondents
1	Loss of identity	277
2	Loss of confidential data	379
3	Loss of wealth	398

Loss of identity leads to embarrassing moments in the life of an individual/employee where an individual/employee may be defamed or loose confidential data leading to loss of public image and monitory losses. 277 companies among respondents have encountered such cases of identity losses.

Loss of confidential data is one of the leading problems of malware attacks where companies and individuals lose their secrecy leading to business losses (loosing clients, business plans, etc.) or monitory losses. 379 companies among respondents have encountered such cases of loss of confidential data.

.

Loss of wealth is the ultimate loss which is also the product of other losses. In other words it can be said that the other types of losses ultimately leads to loss of wealth for a company or an individual. 398 companies among respondents have encountered such cases of loss of wealth.

Matrix analysis of losses

In matrix analysis, losses are represented in columns against the factors affecting malware attacks and the intersecting boxes represent the number of responses in favour of the looses occurring due to the factor affecting malware attacks as given in each row. The matrix is as shown below.

Table 3: Matrix analysis

Issues / Losses	Loss of identity	Loss of confidential data	Loss of wealth
Lack of knowledge	43	22	374
Lack of awareness	42	31	383
Carelessness	22	09	364
No software protection	78	97	279
Improper software protection	44	29	204
Using public computers	19	34	178

Model Development

For better understanding of factors affecting malware attacks a base model was proposed consisting of three factors:

1) Knowledge,
2) Carelessness and
3) Improper software protection.

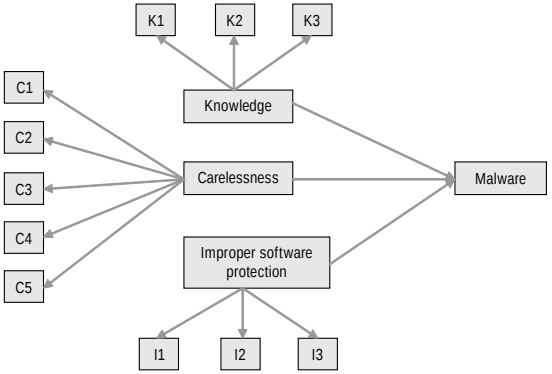
Details of variables used for measuring the above factors in this study are as given in the table below.

Table 4: Variables measuring the proposed factors

Factor 1: (Knowledge)
1.1 (K1) Level of education
1.2 (K2) Technical knowledge
1.3 (K3) Awareness
Factor 2: (Carelessness)
2.1 (C1) Irritation (due to unpleasant atmosphere at home/office)
2.2 (C2) Job dissatisfaction
2.3 (C3) Illness
2.4 (C4) Inquisitiveness
2.5 (C5) Use of unsafe public domains (like cyber cafe, free Wi-Fi, etc.)
Factor 3: (Improper software protection)
3.1 (I1) Cost of software
3.2 (I2) Improper assessment of software requirements
3.3 (I3) Improper choice of software vendor

Based on the questionnaire survey and the literature review the proposed model for malware attacks is as given below.

Figure 1: Proposed model



For further analysis and interpretation a new questionnaire is administered using five point likert scale. The issues shown in table 4 are used to develop the questionnaire which is then sent to the 374 respondents of the questionnaire 1 developed earlier. Survey was carried out for the period of 6 months starting from January 2016 to June 2016. At the end of the 6th month 371 responses received out of which 347 were valid responses while 24 responses were incomplete.

Data Analysis

Reliability

Chronbach's alpha test was conducted using SPSS 20.0 to check the scale reliability of the responses received. It was found to be 0.872 which is well above the conventional reliability criterion of 0.7 and hence the developed scale can be considered reliable for analysis (Srivastava and Mondal, 2016).

Table 5: Construct wise Chronbach's alpha test

Construct	Chronbach's alpha value
Knowledge	0.848
Carelessness	0.911
Improper software protection	0.863

Normality

Normality test is conducted on the data obtained using questionnaire to determine that whether the data set is well modeled with normal distribution or not. Skewness and Kurtosis measurements, K-S (Kolmogorov Smirnov) test and Sahpiro Wilk tests are conducted for testing the distribution of the data and are as shown in table 6, 7 and 8.

Table 6: Skewness and Kurtosis measurements

Items	Skewness (S)	Std. Error	Kurtosis (K)	Std. Error	Absolute (Abs S+ Abs K)
K1	.113	.251	.231	.133	0.344
K2	.331	.434	.772	.253	1.103
K3	.622	.132	-.345	.333	0.967
C1	.031	.219	.242	.471	0.273
C2	.942	.362	-.878	.277	1.820
C3	.633	.769	.789	.656	1.422
C4	.132	.225	.124	.345	0.256
C5	.223	.118	.334	.144	0.557
I1	.049	.092	.127	.093	0.176
I2	.329	.451	-.769	.548	1.098
I3	-.234	.345	.448	.356	0.682

Note: Value of skewness and kurtosis is within +1 and -1 and absolute value of skewness and kurtosis taken together is below the threshold limit of 2, hence the data can be considered to be normally distributed

Table 7: Normality test (K-S test)

Items	**Kolmogorov-Smirnov**		
	Statistic	**df**	**Sig.**
K1	0.234	10	0.001
K2	0.044	10	0.027
K3	0.327	10	0.012
C1	0.479	10	0.000
C2	0.068	10	0.003
C3	0.031	10	0.012
C4	0.228	10	0.000
C5	0.371	10	0.000
I1	0.539	10	0.002
I2	0.670	10	0.000
I3	0.242	10	0.003

Note: Significance level is within 0.05, hence data can be considered to be normally distributed

Table 8: Normality test (Shapiro Wilk test)

Items	Shapiro Wilk		
	Statistic	df	Sig.
K1	0.869	10	0.812
K2	0.997	10	0.832
K3	0.944	10	0.758
C1	0.976	10	0.671
C2	0.877	10	0.738
C3	0.845	10	0.488
C4	0.932	10	0.556
C5	0.968	10	0.477
I1	0.899	10	0.756
I2	0.844	10	0.811
I3	0.946	10	0.599

Note: Significance level is within 0.05, hence data can be considered to be normally distributed

Test results show that the data obtained is normally distributed. In Skewness and Kurtosis measurements the values are well within the range of +1 and -1 moreover the absolute value of Skewness and Kurtosis taken together is well within the limit of 2 which strengthens the notion of data is normally distributed. In K-S test the significance value of all the variables is below 0.05 which is the indication of data being normally distributed. Moreover, in Shapiro Wilk test the significance level of all the variables is above the threshold level of 0.05 which further corroborates with our finding that the data is normally distributed.

A Structural Equations Model

The model proposed and the hypothesized relationships among the different variables of the proposed model were tested and verified using the AMOS 20 structural equation modeling (SEM) package for SPSS. Before running the (SEM) structural equation modeling software, some data transformations were performed. Firstly, missing data patterns were analysed. Only a very few items contained some missing data. As of the extremely limited nature of the missing data, a very simple sample mean imputation in order to construct a full set of data was performed. Further transformation pertained to the survey items measurement levels. Since, assumptions of variables in SEM are made on the interval or ratio measurement level; nominal variables incorporation can only be done when receded as the collection of dummy variables. Rest other measurement items were either measured on the ordinal or the categorical scale, and data manipulation was not required. According to the suggestions of Mulaik and Millsap's (2000), a three-step approach for modelling was used in order to test the developed theoretical model:

1. Explanatory factor analysis establishing the number of latent variables;

2. Confirmatory factor analysis: confirming the measurement model;

3. A structural model: testing the relationships among the model variables;

Steps 2 to 3 are constituted in SEM software, the first step was performed in SPSS 20.0. The unidimensionality of each construct proposed in the model was assessed using PCA (Principal Component Analysis) assuring that the measurement items have a single underlying construct in common (Sethi and King, 1994). Polychoric and tetrachoric correlation matrix usage was preferred over the commonly Pearson's product moment correlation, as per the suggestions made by Joreskog and Sorbom (1996), who in their research observed that lack of variability in correlations of ordinal data can limit the upper and lower limit's of Pearson's Correlation to, -0.5 and 0.5 respectively, leading to the notion by Mlindrila (2010) that Pearon's correlation matrices when analyzed using factor analysis often lead's to artificial factors. Polychoric correlation matrix was obtained using the polycor package in R and the matrix was read into SPSS for subsequent analysis. In accordance with Ho and Li (2006), in order to perform exploratory factor analysis an ordinal measurement level is sufficient. Correlation among variables is another necessary assumption which should be sufficiently strong to validate the application of exploratory or confirmatory factor analysis (above 0.5).

	K1	K2	K3	C1	C2	C3	C4	C5	I1	I2	I3
K1	1.000										
K2	.532	1.000									
K3	-.499	-.114	1.000								
C1	-.711	-.244	.672	1.000							
C2	-.755	-.573	.299	.601	1.000						
C3	-.649	-.492	.266	.482	.598	1.000					
C4	-.562	-.244	.329	.588	.543	.576	1.000				
C5	-.648	-.242	.569	.733	.528	.394	.577	1.000			
I1	-.429	-.350	.488	.543	.432	.276	.539	.444	1.000		
I2	-.332	-.275	.213	.343	.478	.333	.318	.258	.956	1.000	
I3	-.556	-.417	.238	.419	.489	.463	.400	.471	.889	.797	1.000

In the correlation matrix above it can be seen that sufficient number of correlations are above the threshold level of 0.5.

Correlation matrix of the 11 variables showing the inter-correlation among the variables is shown in table above. From the correlation matrix it is observed that there exists high correlation among some of the variables which further motivates us to conduct confirmatory factor analysis to validate the group of variables explaining a single underlying construct or factor which is responsible for the observed correlations. Statistical software SPSS 20.0 was used for analysis. In analysis communalities indicate the amount of variance in each variable that is accounted for. Initial communalities are estimates of the variance in each variable accounted for by all components or factors. For principal components extraction, this is always equal to 1.0 for correlation analyses as shown in table below. Extraction communalities are estimates of the variance in each variable accounted for by the components. The communalities in this table are all high, which indicates that the extracted components represent the variables well. Interpretation of the derived factors was not easy, so, we opted for factor rotation using Varimax technique.

Table 10: Communalities

Communalities		
Items	**Initial**	**Extraction**
K1	1.000	.799
K2	1.000	.532
K3	1.000	.844
C1	1.000	.767
C2	1.000	.772
C3	1.000	.618
C4	1.000	.673
C5	1.000	.651
I1	1.000	.723
I2	1.000	.662
I3	1.000	.771

The KMO (Kaiser-Meyer Olin) statistic is used to further test whether the correlation pattern is diffused or compact, values above 0.5 are considered acceptable. Moreover, Bartlett's test of sphericity is used to tests the null hypothesis of correlation matrix singularity (Field, 2000).

Table 11: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.894
Bartlett's test of sphericity	Approx. Chi-Square	4371.214
	df	310
	Sig.	.000

Table 9 shows that the KMO sampling adequacy is above well accepted level of 0.7 which further encourage us to perform SEM (Structural equation modeling). Moreover, Bartlett's test of sphericity with significance level well below threshold level of 0.05 corroborates with the findings of KMO test. Further varimax rotation of components of knowledge factor was performed which explains 69.22 per cent of the variance in the data set which is well above the threshold level of 50 per cent.

Table 12: Varimax rotated component matrix of knowledge factor

Items	Component (1)
K1	0.727
K2	0.832
K3	0.681
Variance explained	69.22%
Chronbach's alpha value	0.922

Subsequently, varimax rotation was performed on carelessness factor which explains 67.23 per cent of the variances in the data set which is again well above the threshold level of 50 per cent.

Table 13: Varimax rotated component matrix of carelessness factor

Items	Component (1)
C1	0.921
C2	0.723
C3	0.862
C4	-0.671
C5	0.777
Variance explained	67.23%
Chronbach's alpha value	0.882

Finally, varimax rotation was performed on improper software protection factor which explains 73.94 per cent of the variances in the data set which is again well above the threshold level of 50 per cent.

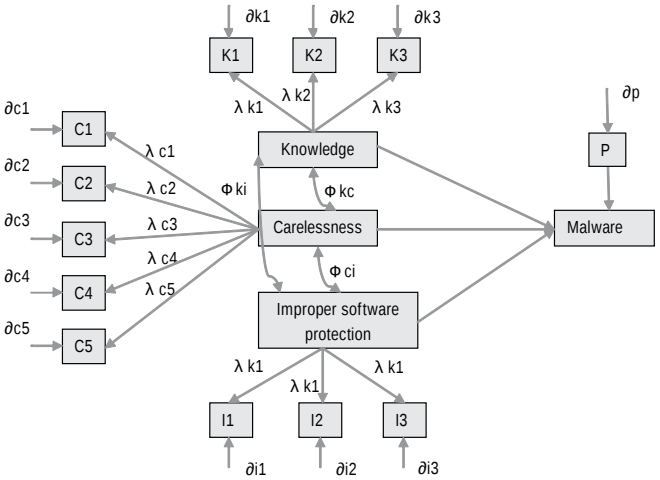
Table 14: Varimax rotated component matrix of improper software protection factor

Items	Component (1)
I1	0.869
I2	0.766
I3	0.842
Variance explained	73.94%
Chronbach's alpha value	0.898

While Exploratory Factor Analysis was conducted to identify the various latent dimensions in the data obtained and the establishing convergent validity of the indicators, CFA (Confirmatory Factor Analysis) tests the individual items adequacy, the divergent validity and reliability in an overall measurement model of the latent variable constructions. Before starting with the parameter estimation using AMOS, it is of utmost importance to verify the considered data in order to perform SEM, as it is understood that deviations with respect to the requirements may influence the method of estimation and parameter reliability. Remarks made earlier regarding the measurement level of the obtained data for factor analysis are equally applicable in SEM estimation. Most of the estimation and model fit methods and procedures are based on variance and covariance matrix calculation, measurement scales of ordinal-level can influence the estimation of under Maximum Likelihood estimation. Highly and precisely related to the measurement scale is normality issue which is a must for structural equation modeling. Non-normality, may occur because of limited sampling of subjects or scaling of variables which in turn may affect variance and covariance among variables (Schumacker and Lomax, 2004). Moreover, it is evident from the analysis done above that the data collected is normally distributed and is shown through Kolmogorov Smirnov test, Shapiro Wilk test and univariate skewness and Kurtosis measurements.

The measurement model is constructed based on the dimensions previously identified and shown in the proposed model. Knowledge, Carelessness and Improper software selection forms the exogenous constructs which are measured by the variables shown by codes in the model (K, C and I). ∂ represents error term, Φ represents correlation between exogenous constructs and λ represents factor loadings. The developed measurement model is as shown below.

Figure 2: Final Structural Equation Model



Structural model assessment

The structural model (n=347) yields the following model fit results: chi square (df=328) = 577.23 ($p<0.01$; which is below the required limit of 0.05 and is desirable for the model fit); RMSEA (Root Mean Square Error of Approximation) = 0.67 which is below the value of 0.08 and is desirable for model estimation. SRMR (Standardized Root Mean Square Residual) = 0.054 which is also below the value of 0.08 and is desirable for model estimate. GFI (Goodness of Fit Indices) = 0.96 which is above the required limit of 0.9 and is desirable for model fit estimation.

So, it is evident from the results obtained that the all the parameter of the structural model is within limits and fits the model well. Hence, it can be conferred that the proposed model is fit to explain the malware attacks.

Criticality of factors for each maintenance types

Once the factors affecting malware attacks are identified, it can be hypothesize that criticality of the factors varies. Thus it becomes essential to identify critical factors affecting malware attacks. Factor scores for each factor is calculated and the Friedman's test is applied to test whether there exists any significant difference among the means

of the three factors or not. Table below shows the test results and mean ranks for the three factors for malware attacks. Test results with significance (p) value below 0.05 clearly show that there exist significant differences among the means.

Table 15: Friedman test: mean rank for different factors

Factors	Mean Rank
Knowledge	2.18
Carelessness	3.72
Improper Software Protection	3.41
Friedman's Test Statistics	Chi Square = 24.321 p=0.000

To examine where the differences actually occur, post hoc analysis using Wilcoxon signed-rank test on the different combinations of related groups is conducted. The various groups of factors for post hoc analysis are: Knowledge - carelessness, knowledge - improper software protection and carelessness – improper software protection. In Wilcoxon signed-rank test there are high chances of Type I error. So, to counter that Benferroni adjustments are done in which we divide the required significance level (in this case 0.05) with the number of groups used for comparison (which is 3). So, the new significance level may be calculated to be (new sig. level = 0.05/3 = 0.0167) 0.0167. Now the new significance level is 0.0167 which will be used for analysis. Further it can be observed from the test as shown in the table below that all the group comparisons are having the significance level less than that of 0.0167 and it may be concluded that there is a significant difference among factors which further corroborates with our findings of Freidman's analysis. Even though it is established that there exists a significant difference among the identified factors, the strength of effect of each factor leading to malware attacks may be established using regression analysis.

Table 16: Wilcoxon Signed- Rank Test of Six-Maintenance Factors

Group of Factors for Comparison	Values	PC
Knowledge: Carelessness	Z	2.628
	Sig.	0.013
Knowledge: Improper Software Protection	Z	1.933
	Sig.	0.002
Knowledge: Improper Software Protection	Z	1.214
	Sig.	0.007

Note: p<0.0167

To understand the effects of each factor: multiple regression analysis is applied to the model developed to test the following hypotheses.

1. Knowledge factor:

H1o: Knowledge factor plays an insignificant role in explaining malware attacks.

H1a: Knowledge factor plays a significant role in explaining malware attacks.

2. Carelessness factor:

H2o: Carelessness factor plays an insignificant role in explaining malware attacks.

H2a: Carelessness factor plays a significant role in explaining malware attacks.

3. Improper software protection factor:

H3o: Improper Software Protection factor plays an insignificant role in explaining malware attacks.

H3a: Improper Software Protection factor plays a significant role in explaining malware attacks.

Regression Model

Table 17: Model Summary

R	R square	Adjusted R square	Standard error of the estimate
0.841	.693	0.689	22.244

Predictors: Constant, knowledge

Table above shows the correlation between the two variables that is knowledge factor and malware attacks.

Table 18: ANOVA

Model 1	Sum of squares	df	Mean square	F	Sig.
Regression	107094.3	1	106191.351	238.176	.000
Residual	47205.242	274	449.623		
Total	154299.542	275			

Predictors: Constant, knowledge
Dependant Variable: malware attacks

The above table above shows that the model is statistically significant as the significance value is below 0.05.

Table 19: Coefficients

Model	Un-standardized coefficients		Standardized coefficients	t	Sig.
	B	**Std. Error**	**Beta**		
Constant	-15.642	4.458		-3.699	.000
Knowledge	15.998	1.241	0.756	15.232	.000
Carelessness	14.422	1.101	0.698	12.221	.018
Improper Software Protection	12.143	1.871	0.927	11.063	.000

The beta coefficients table shows that all the factors are statistically significant and plays a significant role in explaining malware attacks. Hence, all the null hypotheses are rejected and alternative hypotheses are accepted (as shown in table below).

Table 20: Status of hypotheses test conducted

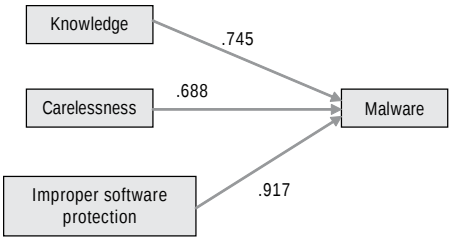
Factor	Null hypotheses	Alternative hypothese
Knowledge	Rejected (H1o)	Accepted (H1a)
Carelessness	Rejected (H2o)	Accepted (H2a)
Improper Software Protection	Rejected (H3o)	Accepted (H3a)

From the coefficient table it is observed that there is significant variation in beta coefficient value for each factor, where, improper software protection holds the maximum value of beta and carelessness has the minimum. It signifies that the most critical factor for malware attacks is improper software protection, then, knowledge factor and lastly carelessness factor. Table below shows the three factors in decreasing order of criticality.

Table 21: Criticality of factors (In descending order)

Rank	Factor	Beta Coefficient
1	Improper Software Protection	0.917
2	Knowledge	0.745
3	Carelessness	0.688

Figure 3: showing beta values and the most critical factor



From the above results it is clear that the improper software protection is the most critical factor for malware attacks. The variables explaining improper software protection are cost of software protection, improper assessment of software requirements and improper choice of software vendor. While, cost of software protection directly involves cost the other variables show a very high correlation with cost variable (as shown in correlation matrix shown earlier in this chapter). So, it may be concluded that cost is the major underlying variable which plays a major role against malware attacks.

Summary of the Empirical Study

In this study, an attempt has been made to validate the proposed model for malware attacks and identify the critical factors related to malware attacks in India. Through empirical study and

subsequent analysis, three such factors were identified, namely, knowledge, carelessness and improper software protection. The analysis reveals that the most critical factor related to malware attacks is improper software protection and it was observed that this factor is closely related to costing components. So, it may be concluded that the better control over financial aspects may help in countering the problem of malware attacks.

It can further be elaborated that the present protection against malware attacks is not enough due to a limited investment. Moreover, a continuous upgrade is required which involves investment and this is the point where most of the companies are not willing to invest. So, it may be concluded that the more the investment in protection methods against malware attacks the less will be the chances of being a victim of malware attacks.

References

C´ardenas, A. A., Radosavac, S., Grossklags, J., Chuang, J., and Hoofnagle, C. (2016). An Economic Map of Cybercrime, *Working Paper*, University of California, Berkeley 2 DOCOMO Communications Laboratories USA, Inc.

Singh, N.P. (2007). Online Frauds in Banks with Phishing. *Journal of Internet Banking and Commerce*, 12(2), 1-27.

Goth, G. (2005). Phishing Attacks Rising, but Dollar Losses Down. *IEEE Security & Privacy Magazine*, 3(1), 8.

Ho, C., and Li, D.(2006).Spatial analysis of city income distribution dynamics in China. *Paper presented at the Chinese Economists Society 2006 Annual Conference.*

Field, A. (2000). *Discovering Statistics Using SPSS for Windows*. London: SAGE Publications.

Joreskog, K.G., and Sorbom, D. (1996). *L/SREL 8: User's Reference Guide*. Chicago: Scientific Software International

Mlndrila, D. (2010). Maximum Likelihood (ML) and Diagonally Weighted Least Squares {OWLS) Estimation Procedures: A Comparison of Estimation Bias with Ordinal and Multivariate Non-Normal Data. *International Journal of Digital Society*, 1(1), 60-66.

Mulaik, S.A. and Millsap, R.E. (2000). Doing the Four-step Right. *Structural Equation Modeling*, 7, 36-73.

Schumacker, R.E. and Lomax, R.G. (2004). *A Beginners Guide to Structural Equation Modeling*. New Jersey: Lawrence Erlbaum Associates.

Sethi, V. and King, W. R. (1994). Development of Measures to Assess the Extent to Which an Information Technology Application Provides Competitive Advantage. *Management Science*, 40(12), 1601-1627.

Srivastava N.K. and Mondal S. (2016). Development of framework for predictive maintenance in Indian manufacturing sector. *Int. J. of Services and Operations Management*, 24(1), 73-98.

Yamane, T. (1967). *Statistics, An Introductory Analysis*. New York: Harper and Row.