Journal of the Midwest Association for Information Systems

Volume 2021 | Issue 2 Article 2

Date: 07-31-2021

A Practitioner Methodology for Mitigating Electronic Data Risk Associated with Human Error

Dennis C. Acuña, Sc.D.
University of Findlay, acunad@findlay.edu

Rajab Suliman, Ph.D.
University of Toledo, rajab.suliman@utoledo.edu

Nasir Elmesmari, Ph.D.
University of Benghazi, nasir.elmesmari@uob.edu.ly

Abstract

Given the growing importance of data stewardship in today's digital economy, the ability to better manage vulnerabilities associated with electronic data is of interest to organizational leadership. Human error is a vulnerability that increases the likelihood of electronic data risk, such as the threat of a data breach. One countermeasure against human error is the ability to measure human intent toward compliance with an information assurance (IA) policy, as one input for better managing the human factor within an organization. While large organizations are likely to have access to resources for managing the human factor, small to mid-size organizations are less likely to have access to similar resources. Thus, this paper explores the use of commonly available research tools to provide a poor man's countermeasure for better managing the threat/vulnerability pair that is electronic data risk/human error. Our methodology uses logistic regression to evaluate the statistical significance of using ordinal data to measure human intent to comply with an IA policy as such a countermeasure. Our findings conclude that the application of this methodology provides a sound technique for measuring human error vulnerability, and thus better managing electronic data risk.

Keywords: *Logistic regression, ordinal data, information assurance, human error, practitioner*

DOI: 10.17705/3jmwa.000068

1. Background

Electronic data is an organizational feedstock that can be used to achieve objectives and build competitive advantage (Davenport, 2006; Porter, 1979). As such, electronic data is an organizational asset and should be managed as an asset (Collins & Lanz, 2019; Thomson & von Solms, 2005). Despite the existence of governance, risk management and compliance (GRC) best practices for the management of electronic data assets, the frequency of reported data breaches since 2005 continues to increase (Figure 1).

One vulnerability contributing to the frequency of reported data breaches is the human factor, in the form of human error. Warkentin, Straub and Malimage (2012) contend that human error contributes to internal and external threats, which can be non-volitional, non-malicious, and malicious in nature. Dennis and Minas (2018) posit that some human error can be attributed to irrational non-cognitive behavior, as well as rational cognitive behavior. Some industry studies conclude that employee behavior is the largest single cause of security breaches (Johnston, Warkentin, Dennis, & Siponen, 2019), with commercial estimates inferring varying percentages of human error ranging as high as 50% (IBM, 2019; PwC, 2015; Verizon, 2019). Academic researchers Liginlal, Sim and Khansac (2009) posit that up to 65% of data breach incidents resulting in economic loss are attributable to human error. The difference in percentage estimates is not unusual. As shown in Figure 1, the frequency of reported data breaches and associated breached record counts can vary from year to year, but the pattern of reported data breaches and breached records both indicate rising linear trends.

Some studies contend that effective countermeasures can be developed to address these problems (Bulgurcu, Cavusoglu, & Benbasat, 2010; Sasse, Brostoff, & Weirich, 2001), and posit that developing and maintaining a culture of information assurance (IA) is essential for managing the human or behavioral aspect associated with data risk (Da Veiga & Eloff, 2007; Dhillon, Syed, & Pedron, 2016; van Niekerk & von Solms, 2010). One aspect of organizational IA culture, sometimes referred to as IA posture, is human compliance with IA policy (Thomson & von Solms, 2005). Schein (2004) asserts this contention by stating that culture is an abstraction, and that organizations need to understand the forces that result from social and organizational situations, lest they fall victim to them. Other studies have published findings on the effects of a computer security policy on IA culture, and compliance with IA policy (Acuña, 2017; D'Arcy & Hovav, 2007; Da Veiga & Eloff, 2007).

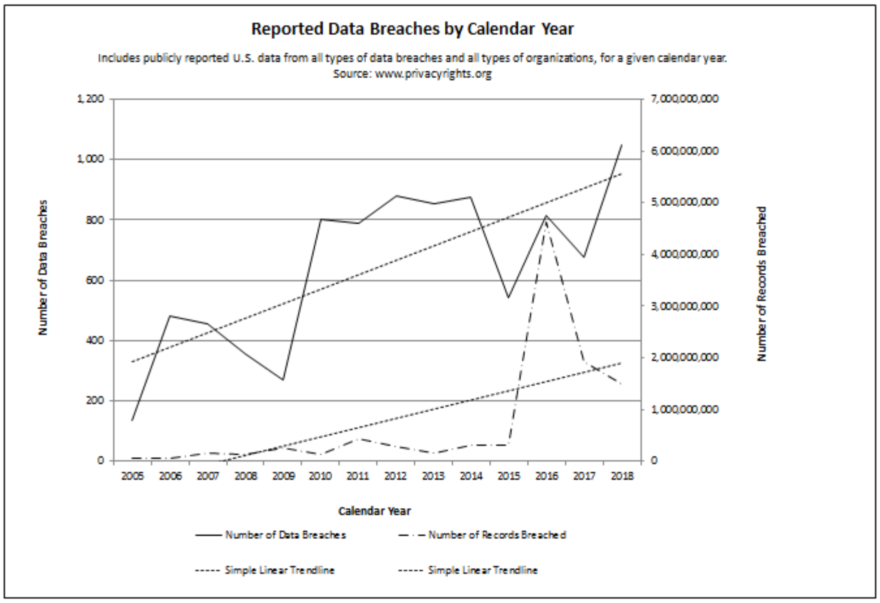


Figure 1. Reported Data Breaches by Calendar Year (Privacy Rights Clearinghouse, 2019)

Although human behavior is difficult to predict, human intent to perform a specific behavior such as complying with an IA policy can be measured (Ajzen, 1991). The theory of planned behavior (TPB) states that human behavior is determined by factors that influence the intention to perform a specific behavior. Rather than model specific human behavior, TPB models behavioral intention. The stronger the intention to perform the behavior, the more likely it is that the specific behavior will be performed. An artifact capable of measuring human intent to comply with an IA policy, such as a survey instrument, would therefore provide a practical technique for the measurement, and subsequent management, of human error vulnerabilities associated with electronic data risk (Liginlal et al., 2009). One instrument commonly used to measure human intent is a Likert scale, a survey tool that records a human response along an ordered scale of qualitative options such as “strongly disagree” to “strongly agree” (Appendix A, Figure A1). Of concern however, is that Likert scales produce data that is ordinal, or non-metric, as opposed to continuous or metric data.

Some researchers posit that the use of ordinal data in statistical analyses should be treated differently than metric data, in that the mode and the median are the accepted measures of central tendency for non-metric data as opposed to use of the mean for metric data (Jamieson, 2004). This belief is not universal, as other researchers support the treatment of ordinal data as interval, or metric, data in statistical analyses (Carifio J. & Perla R., 2007, 2008). While the practice of treating non-metric data as metric data may seem harmless to the practitioner, the application of parametric statistics derived from ordinal data without a strong supporting argument often serves to discredit the reputation of the practitioner, and discount the use of Likert scale instruments and ordinal data as practical research tools (Bishop & Herron, 2015).

2. The Practitioner Problem and Solution

While large organizations are likely to have access to resources for managing the human factor, small to mid-size organizations are less likely to have access to similar resources. As a result, small to mid-sized organizations often face limitation in the number of countermeasures they can deploy, thus weakening IA defenses. Based on the working hypothesis that deployment of a functional, understood countermeasure is better than the absence of such a countermeasure, it is posited that the use of ordinal data and other commonly available research tools be deployed as a poor man’s countermeasure for better managing the threat/vulnerability pair that is electronic data risk/human error (Hubbard & Seiersen, 2016). Providing organizational leadership with the ability to capture meaningful, longitudinal measurements on human intent to comply with IA policy can be an effective tool for monitoring and managing the IA culture, or IA posture, of an organization. The use of a Likert scale provides an effective, low cost means for developing such a countermeasure. However there are issues, both positive and negative, associated with this approach (Bishop & Herron, 2015; Carifio J. & Perla R., 2008; Hubbard & Seiersen, 2016; Jamieson, 2004; Joreskog, 2005).

First, Likert scales produce non-metric data which may be unacceptable to some organizations as a meaningful basis for longitudinal measurement. While the mode and median can be used as measures of human intent to comply with IA policy, a more powerful statistical measurement exists in the form of logistic regression, using the receiver operating characteristics (ROC) curve and the area under the ROC curve (AUC).

Second, Likert scales are administered at the individual level and not the organizational level, which may be viewed by some as an ineffective measurement for developing security education training and awareness (SETA) guidance at the organizational level. However, the input of individually sourced ordinal responses to build a logistic regression model and the interpretation of the composite output ROC/AUC statistics provides guidance for managing IA posture at the organizational level.

Thus, the remainder of this paper discusses the use of commonly available research tools in the form of Likert scales, ordinal data, the R computer program, and logistic regression, to develop a poor man’s countermeasure that is both efficient and effective for managing the threat/vulnerability pair that is electronic data risk/human error.

3. Research Objective and Hypotheses

To better manage the threat/vulnerability pair that is electronic data risk/human error, a practical, statistically viable artifact capable of measuring human intent to comply with an IA policy is desired. Thus, the research objective of this study is to determine the statistical viability of using an ordinal scale survey instrument to measure and classify human respondents into two categories; those who intend to comply with an IA policy, and those who do not intend to comply with IA policy.

Table 1. Research Hypotheses

Null Hypothesis	Alternative Hypothesis
H_0: A survey instrument utilizing an ordinal scale is not a statistically significant instrument for measuring human intent to comply with an IA policy.	H_a: A survey instrument utilizing an ordinal scale is a statistically significant instrument for measuring human intent to comply with an IA policy.

Therefore, it is the hypothesis of this study that an ordinal scale survey instrument, often referred to as a Likert scale, can be used to measure human intent to comply with an IA policy (Table 1).

4. Research Methodology

4.1 Research Background

This study is an extension of original, institutional review board (IRB) approved research into the effects of a comprehensive IA policy on human compliance with IA policy (Acuña, 2017). As such, this paper leverages an existing dataset.

4.2 Survey Design and Operalization

The IRB approved survey instrument for the original study (Acuña, 2017) utilized a 7-point Likert scale for measurement. Measurement of TPB indicators in information systems (IS) research is mixed, with evidence of unipolar and bipolar, 5-point and 7-point Likert scales. The IRB approved survey instrument adopted the unipolar 7-point Likert scale recommended by Ajzen (1991) for measurement (Appendix A, Figure A1).

Questions for the IRB approved survey instrument (Appendix A, Table A2) were drawn, when possible, from previous studies conducted within this domain (Flores & Ekstedt, 2016; Guo, Yuan, Archer, & Connelly, 2011; Pavlou & Fygenson, 2006). Six demographic control variables were utilized: IT/OT identity, gender, age, education, years of work experience, and industry sector (Appendix A, Table A1). A modified three-sector theory construct (primary, secondary, tertiary, quaternary) served as the basis for the industry sector model (Fisher, 1939). The inclusion of industry sector as a control variable aligns with the contention by Bulgurcu et al. (2010) that some industries are more vulnerable to computer security issues than other industries.

Questionnaire distribution and data collection for the IRB approved survey was contracted to Qualtrics (2020), a commercial Internet service that specializes in survey based research. The target population was experienced, industry based, authorized users located in the United States, randomly selected from various industry sectors. Identifiers capable of linking a response to a participant, including Internet Protocol (IP) address, were managed by Qualtrics and were hidden and unknown to the principal investigator. Operationalization of the survey instrument resulted in the collection of 210 responses. A summarization of the collected responses was presented at an academic conference and subsequently published in the conference proceedings (Acuña, 2018). For readability of this paper, a summarization of the Likert scale, demographic frequency distributions, and questionnaire responses is included in Appendix A of this report.

4.3 Data Analysis Technique

Given the ordinal dataset used for this paper, and the research objective of measuring and classifying human intent into the binary categories of complying with an IA policy or not complying with an IA policy, logistic regression was selected as the primary technique for data analysis. Logistic regression is a technique for modeling the relationship between multiple independent variables and a binary categorical dependent variable (Park, 2013). Use of logistic regression is an appropriate statistical analysis technique when the dependent variable is non-metric with two possible outcomes, and independent variables are metric or non-metric. Logistic regression is often used to address research objectives associated with establishing a classification system for determining group membership (Hair, Black, Babin, & Anderson, 2010). The Microsoft Windows R platform (R Core Team, 2019) was selected as the computer software for executing the analysis.

4.4 Sample Size

The minimal sample size for multiple logistic regression is the minimum number of observations needed to execute the logistic regression model. The factors involved in determining sample size include statistical power, predictor variables, smallest proportion of binary cases, effect size, and standard error, making sample size estimation for multiple logistic regression a complex effort (Park, 2013). Peduzzi, Concato, Kemper, Holford and Feinstein (1996) contend that minimal sample size is defined as $n = 10k/p$, where k represents the number of predictor variables and p denotes the smallest proportion of binary cases in the population, with (1) indicating that the event occurred and (0) indicating that the event did not occur (Park, 2013). Additionally, if the calculated number of observations is less than 100, it is recommended that the sample size be increased to 100 (Long, 1997). Based on a Likert scale cutoff point of 6, the proportion of binary cases for our dataset resulted in 156 (1's) and 54 (0's), resulting in the value of 54 as the smaller binary proportion. As shown in Table 2, the minimal sample size for a six predictor model is 234, rounded up from the calculated value of 233.333. The minimal sample size for a two predictor model is calculated at 77.778 and rounded up to 100, given that the calculated sample size is less than 100.

Table 2. Logistic Regression Sample Size *n = 10k/p*

	k	***p***		***n***
Constant	**Predictor Variables**	**Binary Case Proportion**	**Calculated Sample Size**	**Adjusted Sample Size**
10	6	54/210	233.333	234
10	2	54/210	77.778	100

In addition to the formula suggested by Peduzzi et al. (1996) and the guideline recommended by Long (1997), other researchers posit different formulas for minimal sample size. Hosmer and Lemeshow (2000) recommend sample sizes greater than 400, while Hair et al. (2010) suggest a sample size based on dependent variable groups, with each group consisting of 10 observations per estimated parameter. Lastly, we note that simply rounding the six predictor *p* value in Table 2 to one decimal place yields a calculated sample size of 200 observations instead of 233.33 observations. Given the range of formulas for sample size, the different sample sizes produced by each formula, and the sensitivity of sample size to binary case proportion, we conclude that our dataset of 210 observations, while less than the Peduzzi et al. (1996) recommended 234 observations for a six predictor model, provides working representation for our study.

4.5 Empirical Strategy

To ensure statistical significance, a link function was used to transform the linearity between the predictor variables and the response variable, with the most common choice being use of the logit function (Zuur, Ieno, Walker, Saveliev, & Smith, 2009). The logit function ensures that any transformed value from the linear predictor variables will be restricted to the range of 0 . . . 1 (Douma & Weedon, 2019). Based on the input dataset, logistic regression produces an S-shaped curve of predicted probability values ranging between 0 . . . 1. The probability values are calculated from the values of the independent variables and their estimated coefficients. Predicted probabilities > 0.50 result in a value of (1) indicating that the event occurred, while values ≤ 0.50 result in a value of (0) indicating that the event did not occur (Hair et al., 2010). The following sections describe our analysis and findings resulting from the use of logistic regression to measure and classify human respondents into two categories; those who intend to comply with an IA policy, and those who do not intend to comply with an IA policy.

4.6 Overall Model Evaluation

The model created for this study produced the goodness-of-fit statistics listed in Table 3. Given that a likelihood ratio (MLE) with a low p-value (0.015) indicates good model fit, and a Hosmer-Lemeshow test with a high p-value (0.606) is also indicative of good model fit, the findings in Table 3 suggest similar conclusions; that the fitted model including all predictor variables is more effective than the null model, leading to the conclusion that the fitted model is meaningful (Park, 2013).

Table 3. Overall Model Evaluation and Goodness-of-Fit Statistics (n = 170)

Test Name	Test Purpose	Significant p-value	p-value
Likelihood ratio test (MLE)	Model parameter evaluation	Low	0.015 (*)
Hosmer-Lemeshow test	Lack of model fitness	High	0.606

This study utilized six demographic control variables as classifiers: IT/OT identity, gender, age, education, years of work experience, and industry sector. Demographic sub-categories containing fewer than five observations were combined with contiguous sub-categories to minimize error (McDonald, 2009). Given a survey dataset representing 210 respondents, the R model was programmed to segment the dataset as 80% training data and 20% test data. This resulted in a training dataset of approximately 170 random respondents and a test dataset of approximately 40 random respondents. Each of the following tables and figures represent the training dataset of 170 random respondents.

Table 4 displays the significance of the individual relationships between the control variables based on the Wald Chi-Square test. The only independent variables that are statistically significant classifiers for the event are age with $\alpha = 0.05$ and education with $\alpha = 0.10$. Based on this finding we repeated the analysis by dropping the factors associated with the highest p-values. This action lead to the same conclusion, that only age and education offer significant contribution to the event.

Table 4. Statistical Significance of Regression Coefficients Using Wald Chi-Square Test

Variable	Estimate	Std. Error	z-value	p-value
(Intercept)	-2.530	1.057	-2.394	0.017 (*)
IT/OT	0.198	0.472	0.42	0.674
Male/Female	0.385	0.438	0.879	0.379
Age3	2.095	0.673	3.112	0.002 (**)
Age4	1.574	0.736	2.139	0.032 (*)
Age5	1.753	0.809	2.166	0.030 (*)
Age6	0.901	1.015	0.888	0.375
Education3	1.219	0.741	1.647	0.100 (.)
Education5	-0.375	0.804	-0.467	0.641
Education6	0.496	0.663	0.748	0.454
Education8	0.079	0.755	0.104	0.917
WorkExperience3	0.817	0.514	1.589	0.112
WorkExperience4	0.024	0.608	0.039	0.969
WorkExperience5	1.123	0.709	1.585	0.113
IndustrySector2	0.775	0.808	0.959	0.338
IndustrySector4	0.994	0.811	1.226	0.220

4.7 Predictive Accuracy

The classification confusion matrix for the training data using all control variables (Table 5) displays the predictive accuracy of the logistic regression model (Peng & So, 2002).

Table 5. Classification Confusion Matrix of Training Data with All Control Variables

	Predicted		
Actual	Yes	No	% Correctly predicted
Yes	$n_{11} = 114$	$n_{10} = 35$	76.51% sensitivity
No	$n_{01} = 8$	$n_{00} = 13$	61.90% specificity
Overall % correct			74.71% overall correct

$$Sensitivity = \ 114/(114 + 35) = 76.51\%\,; Specificity = \ 13/(8 + 13) = 61.90\%$$

The 2x2 matrix for predicted values displays the cross classification of the observed values for the response variable and the predicted values at the defined cut-off value. A default cut-off value of 0.5 was used, with predicted values > 0.5 classified as human intent to comply (1) with an IA policy, and predicted values ≤ 0.5 classified as human intent to not comply (0) with an IA policy. The 2x2 matrix for predicted values using all control variables (Table 5) is summarized as a dichotomous observed response and a dichotomous predicted response. Given that the fitted model exhibits goodness-of-fit (Table 3), we expect to see a high count of correctly predicted values of the actual classes likely to comply (1) versus not likely to comply (0). The ability to correctly predict a class (1) observation is commonly known as sensitivity and is calculated as $n_{11}/(n_{11} + n_{10})$. Specificity is the ability to correctly predict class (0) and is calculated as $n_{00}/(n_{01} + n_{00})$. As shown in Table 5, the overall correct prediction of 74.71% indicates an improvement over a 50% level of chance. Higher percentages of sensitivity and specificity indicate a fitted model with better classification performance. This finding aligns with an overall correct accuracy of 80% produced by executing the fitted model with the test dataset.

Table 6 displays the confusion matrix after dropping non-significant factors. Dropping non-significant factors improves the overall accuracy to 75.88% (Table 6) from 74.71% (Table 5), compared to when all six control variables are modeled. This finding is a good indication that the model is preforming well.

Table 6. Classification Confusion Matrix of Training Data with Age and Education Only

	Predicted		
Actual	**Yes**	**No**	**% Correctly predicted**
Yes	$n_{11} = 117$	$n_{10} = 36$	76.47% sensitivity
No	$n_{01} = 5$	$n_{00} = 12$	70.59% specificity
Overall % correct			75.88% overall correct

$Sensitivity = \ 117/(117 + 36) = 76.47\%; Specificity = \ 12/(5 + 12) = 70.59\%$

4.8 Discrimination with ROC Curves and AUC

Extending the 2x2 matrix referenced in Table 5, all data values are examined without the benefit of a single cutoff point. The resulting analysis produces a scatter plot of values ranging between 0 . . . 1, such that data pairs (x, y) or (1-specificity, sensitivity) define the area representing the receiver operating characteristics curve (ROC) (Berrar & Flach, 2012). The area under the ROC curve (AUC) provides the overall performance of the fitted logistic regression model (Bewick, Cheek, & Ball, 2004).

As depicted in Figure 2 and Figure 3, data points below the diagonal line dividing the ROC space represent poor model performance (worse than random), while data points above the diagonal line indicate good model performance (better than random). Higher AUC values suggest better predictability of the fitted model (Park, 2013).

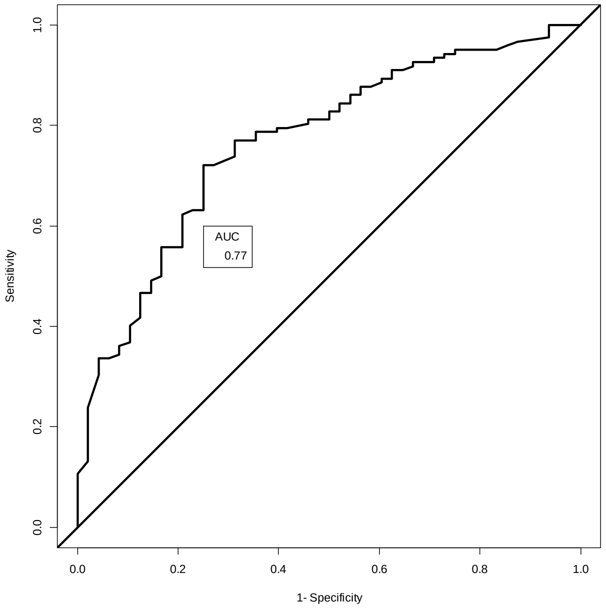


Figure 2. AUC (76.8%) for Six Control Variables

Figure 2 depicts the AUC for the six demographic control variables defined within this study. As indicated, modeling six variables results in an AUC of 0.768, compared with an AUC of 0.739 (Figure 3) when only age and education are modeled.

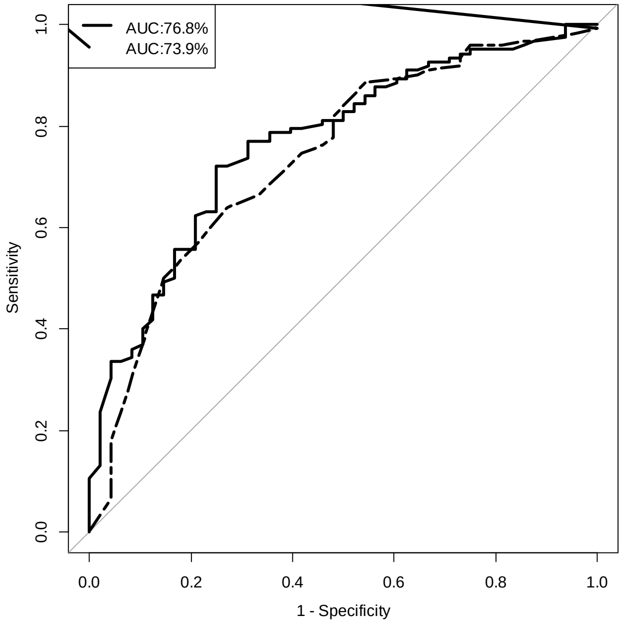


Figure 3. AUC (73.9%) for Two Control Variables (Age and Education)

Using R function *test.roc* we found no statistically significant difference in AUCs when modeling all six control variables or modeling only two control variables: age, and education (z = 0.877, p-value = 0.381). In conclusion, we find that age and education are good classifiers for measuring human intent to comply with an IA policy.

Figure 4 depicts the Pearson residual plot versus the estimated probability for the model. In this instance, the LOWESS smoothing approximates a line having zero slope and a near zero intercept. We conclude there is no significant model inadequacy.

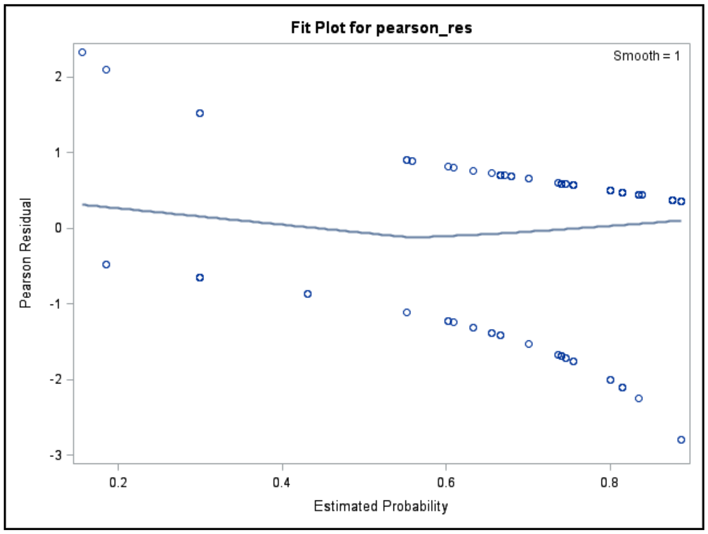


Figure 4. Residual Plot with LOWESS Smoothing

AUC values (Table 7) range in performance from no discrimination (AUC = 0.5) to outstanding discrimination (AUC > 0.9). The terminology describing AUC performance varies among researchers, with different qualitative attributes describing the same quantitative performance (Table 7). Our findings are consistent with acceptable/excellent discrimination.

Table 7. AUC Discrimination Levels and Performance Attribute

AUC Discrimination Range	**Performance Attribute** (Mandrekar, 2010)	**Performance Attribute** (Yang & Berdine, 2017)
$\mathrm{AUC} = 0.5$	No discrimination	No discrimination
$0.5 < \mathrm{AUC} \leq 0.6$		Poor discrimination
$0.6 < \mathrm{AUC} \leq 0.7$		Acceptable discrimination
$0.7 < \mathrm{AUC} \leq 0.8$	Acceptable discrimination	Excellent discrimination
$0.8 < \mathrm{AUC} \leq 0.9$	Excellent discrimination	
$0.9 < \mathrm{AUC}$	Outstanding discrimination	Outstanding discrimination

5. Research Limitations

5.1 Likert Scale Cutoff Point

The Likert scale cutoff point for categorization was set at 6, meaning that survey responses ≥ 6 were categorized as (1) indicating that the event occurred, and survey responses < 6 were categorized as (0) indicating that the event did not occur. The cutoff point of 6 was selected based on the fact that the dataset exhibited negative (left) skewness with the mode falling consistently in the 6-7 range of the Likert scale (Appendix A, Figure A1, Table A2). This logic also suggested that selecting 6 as the cutoff point on a 7 point Likert scale minimized outcome bias in regard to categorization of survey responses.

5.2 Sample Size

Setting the Likert scale cutoff point also has an effect on the sample size calculation used by this paper. For the dataset used by this paper, lowering the cutoff point results in more (1's) which reduces the proportion of (0's), which increases the minimal sample size. Raising the cutoff point results in more (0's) which increases the proportion of (0's), which decreases the minimal sample size. While our sample size of 210 is less than the Peduzzi et al. recommendation of 234, raising the Likert scale cutoff point from ≥ 6 to $= 7$ would result in a sample size approximating 210 observations. Thus, given the sensitivity of sample size to the Likert scale cutoff point and rounding preferences, we conclude that our dataset of 210 observations provides working representation for our study. We note that future work would benefit from a study of the different formulas for calculating logistic regression minimal sample size, and from sensitivity analysis of the variables used in the sample size formula.

6. Research Findings and Practitioner Contribution

6.1 Research Findings

Based on the results of our analysis, we reject the null hypothesis and accept the alternative hypothesis that an ordinal scale survey instrument is a statistically significant instrument for measuring human intent to comply with an IA policy. We also find that the application of logistic regression on the dataset produced from an ordinal scale survey instrument is a practical technique for classifying human respondents into two categories; those who intend to comply with an IA policy, and those who do not intend to comply with an IA policy. Among these findings we determine that age and education are good classifiers for measuring human intent to comply with an IA policy, and that the fitted model including all predictor variables is more effective than the null model, leading to the conclusion that the fitted model as described by this paper is meaningful.

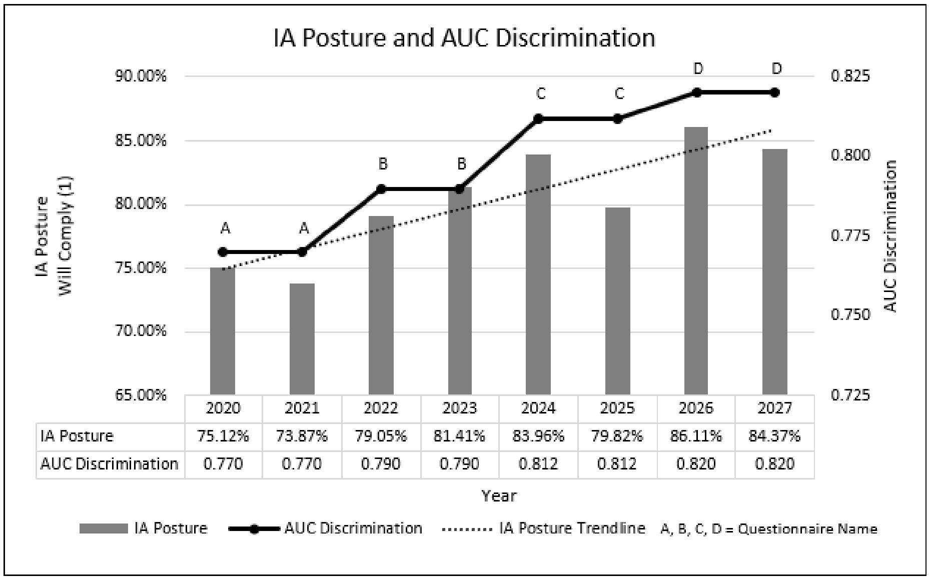
6.2 Practitioner Contribution

Use of a Likert scale survey instrument and the data analysis technique described in this paper provide a practical, statistically viable means to measure and classify human intent to comply with an IA policy. Longitudinal application of this methodology on the members of an organizational body will provide the practitioner with consistent, predictive measurement in the form of statistics that are representative of an organization's intent to comply or not comply with an IA policy. These statistics can be used to graph change over time, thus providing a visual metric of whether organizational IA posture is improving, plateauing, or worsening.

6.3 A Poor Man's Countermeasure

An example of a graph leveraging the commonly available research tools discussed in this paper is depicted in Figure 5. The graph titled "IA Posture and AUC Discrimination" is an example of imaginary performance regarding an organizational SETA program. The data shown in this graph is artificial and is not real, and is used for illustrative and explanatory purposes only. We break down each graph component and its intended meaning as follows.

As prescribed by our imaginary SETA program, a survey instrument is administered to our organizational workforce on an annual basis. The survey instrument collects data on the six demographic control variables used by this study which are now used as predictor variables. If permitted, the demographic data might be readily obtainable from the human resources department, in which case a survey instrument will not be needed. The control variables are input into our previously fitted logistic regression model which outputs (predicts) the number of people likely to comply with an IA policy (1), and the number of people not likely to comply with an IA policy (0). The percentage of (1's) is then inserted into the data table as the data series titled "IA Posture". This process is repeated on an annual basis.



	2020	2021	2022	2023	2024	2025	2026	2027
IA Posture	75.12%	73.87%	79.05%	81.41%	83.96%	79.82%	86.11%	84.37%
AUC Discrimination	0.770	0.770	0.790	0.790	0.812	0.812	0.820	0.820

Figure 5. Example of a Poor Man's Countermeasure

Our graph also depicts the use of different Likert scale survey instruments over time, annotated as questionnaires *A*, *B*, *C*, and *D*. Each questionnaire is used for two years to provide a basis for comparison of performance management, and then modified to adjust for current findings and relevant concerns. Modification of the questionnaire and its associated questions requires us to rebuild our fitted logistic regression model every two years, which results in a new AUC predictor value represented within the data series "AUC Discrimination". The AUC discrimination statistic represents the predictive strength of our fitted logistic regression model (Park, 2013). High AUC values (Table 7) suggest better predictability of the fitted model while low AUC values suggest weaker predictability.

Examining IA posture for the year 2020, we note our fitted model predicted 75.12% of the workforce would comply with our IA policy. We are confident that this finding is significant, in that the AUC discrimination for questionnaire *A* is 0.770 which is indicative of acceptable/excellent discrimination (Table 7). Other years on the graph are interpreted in the same manner. A trendline for the data series "IA Posture" is added for good measure, the upward trend suggesting that our SETA program is having the desired effect on our workforce.

Of note is that IA Posture dipped in the years 2021, 2025, and 2027. The dips are signals to organizational leadership that the IA posture for our workforce has worsened from the previous year in regard to willingness to comply with our IA policy, and that an adjustment is needed in our SETA program. Given the binary classification output of our model, personalized SETA messages can be crafted for each classification to elicit the desired IA behavior (Johnston et al., 2019). Based on the improved results in 2022 and 2026, we surmise that the adjustments to our SETA program had the desired effect and that organizational IA posture is back on track. A similar adjustment will need to be made prior to delivery of the 2028 survey instrument. We also conclude that our IA support team is improving, as the re-fitted models are producing stronger AUC discrimination statistics over time, thus ensuring confidence in organizational leadership that our SETA program is effective.

7. Conclusion

In conjunction with other IA GRC best practices, application of the methodology outlined in this paper constitutes a poor man's countermeasure for managing organizational IA posture, using commonly available research tools. While not perfect, deployment of a functional, understood countermeasure is better than the absence of such a countermeasure, thus providing organizations with a practical methodology for mitigating electronic data risk associated with human error. As stated by Hubbard and Seiersen (2016), "A mere reduction, not necessarily an elimination, of uncertainty will suffice for a measurement" (p. 21).

8. References

Acuña, D. C. (2017). *Effects of a Comprehensive Computer Security Policy on Human Computer Security Policy Compliance*. Doctoral Dissertation Final Defense. Dakota State University. Madison, SD.

Acuña, D. C. (2018). *Manifest Observations on a Comprehensive Computer Security Policy*. Paper presented at the Proceedings of the Thirteenth Midwest Association for Information Systems Conference, Paper 59, University of Missouri-St. Louis.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Berrar, D., & Flach, P. (2012). Caveats and Pitfalls of ROC Analysis in Clinical Microarray Research (and how to avoid them). *Briefings in Bioinformatics, 13*(1), 83-97.

Bewick, V., Cheek, L., & Ball, J. (2004). Statistics Review 13: Receiver Operating Charachteristic Curves. *Critical Care, 8*(6), 508.

Bishop, P. A., & Herron, R. L. (2015). Use and Misuse of the Likert Item Responses and Other Ordinal Measures. *International Journal of Exercise Science, 8*(3), 297-302.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-A527.

Carifio J., & Perla R. (2007). Ten Common Misunderstandings, Misconceptions, Persistent Myths and urban legends about Likert scales and Likert response Formats and their Antidotes. *Journal of Social Sciences, 3*(3), 106-116.

Carifio J., & Perla R. (2008). Resolving the 50-year Debate Around using and Misusing Likert Scales. *Medical Education, 42*(12), 1150-1152.

Collins, V., & Lanz, J. (2019). Managing Data as an Asset. *CPA Journal, 89*(6), 22-27. Retrieved from https://login.ezproxy.findlay.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bft&AN=136901846&site=ehost-live

D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems Misuse. *Communications of the ACM, 50*(10), 113-117.

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

Davenport, T. H. (2006). Competing on Analytics. *Harvard Business Review, 84*(1), 98-107. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=19117901&site=ehost-live&scope=site

Dennis, A. R., & Minas, R. K. (2018). Security on Autopilot: Why Current Security Theories Hijack our Thinking and Lead Us Astray. *SIGMIS Database, 49*(SI), 15–38.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56*, 63-69.

Douma, J. C., & Weedon, J. T. (2019). Analysing continuous proportions in ecology and evolution: A practical introduction to beta and Dirichlet regression. *Methods in Ecology and Evolution, 00*, 1-19.

Fisher, A. G. B. (1939). Production, Primary, Secondary and Tertiary. *Economic Record, 15*, 24–38.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=67194187&site=ehost-live&scope=site

Hair, J. F., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed.): Prentice Hall.

Hosmer, D. W., & Lemeshow, S. (2000). *Applied Logistic Regression* (2nd ed.). New York, NY: John Wiley & Sons, Inc.

Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk*. Hoboken, NJ: John Wiley & Sons, Inc.

IBM. (2019). IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years. Retrieved from https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

Jamieson, S. (2004). Likert scales: how to (ab)use them. *Medical Education, 38*(12), 1217-1218.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. *Decision Sciences, 50*(2), 245-284.

Joreskog, K. G. (2005). *Structural Equation Modeling with Ordinal Variables using LISREL*.

Liginlal, D., Sim, I., & Khansac, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security, 28*.

Long, J. S. (1997). *Regression Models for Categorical and Limited Dependent Variables*. Thousand Oaks, CA: Sage Publications.

Mandrekar, J. N. (2010). Receiver Operating Characteristic Curve in Diagnostic Test Assessment. *Journal of Thoracic Oncology, 5*(9), 1315-1316.

McDonald, J. H. (2009). *Handbook of Biological Statistics* (Second ed. Vol. 2). Baltimore, MD: Sparky House Publishing.

Park, Hyeoun-Ae. (2013). An Introduction to Logistic Regression: From Basic Concepts to Interpretation with Particular Atention to Nursing Domain. *Journal of Korean Academic Nursing, 43*(2), 154-164.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly, 30*(1), 115-143. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=19754863&site=ehost-live&scope=site

Peduzzi, P., Concato, J., Kemper, E., Holford, T. R., & Feinstein, A. R. (1996). A Simulation Study of the Number of Events per Variable in Logistic Regression Analysis. *Journal of Clinical Epidemiology, 49*(12), 1373-1379.

Peng, C. Y. J., & So, T. S. H. (2002). Logistic Regression Analysis and Reporting: A Primer. *Understanding Statistics: Statistical Issues in Psychology, Education, and the Social Sciences, 1*(1), 31-70.

Porter, M. E. (1979). How competitive forces shape strategy. *Harvard Business Review, 57*(2), 137-145.

Privacy Rights Clearinghouse. (2019). Data Breach Chronology. Retrieved from http://www.privacyrights.org/data-breach

PwC. (2015). *2015 Information Security Breaches Survey*. Retrieved from http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Qualtrics. (2020). Online Survey Platform. Retrieved from https://www.qualtrics.com/

R Core Team. (2019). R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria. Retrieved from https://www.R-project.org/

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, *19*(3), 122.

Schein, E. H. (2004). *Organizational Culture and Leadership* (3rd ed.). San Francisco, CA: Jossey-Bass.

Thomson, K. L., & von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, *24*(1), 69-75. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404804002627

van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

Verizon. (2019). 2019 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Warkentin, M., Straub, D., & Malimage, K. (2012). *Featured Talk: Measuring Secure Behavior: A Research Commentary*. Paper presented at the Annual Symposium on Information Assurance & Secure Knowledge Management, Albany, NY.

Yang, S., & Berdine, G. (2017). The receiver operating characteristic (ROC) curve. *The Southwest Respiratory and Critical Care Chronicles, 5*(19), 34-36.

Zuur, A. F., Ieno, E. N., Walker, N. J., Saveliev, A. A., & Smith, G. M. (2009). *Mixed Effects Models and Extensions in Ecology with R*. New York: Springer.

9. Appendix A

Survey Instrument and Data Summarization (Acuña, 2018)

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree

Figure A1. Unipolar 7-Point Likert Scale for Belief Strength Measurement (Variable ID H11-HA3)

Table A1. Participant Demographics (percentages subject to rounding error)

Demographic	**Category**	**Frequency** **Σ** (n=210)	**Percent** **Σ** (n=210)	**Frequency** **IT** (n=106)	**Frequency** **OT** (n=104)
Identity	Information Technology (IT)	106	50.48%	106	0
	Operational Technology (OT)	104	49.52%	0	104
Gender	Male	148	70.48%	71	77
	Female	62	29.52%	35	27
Age	Less than 18 years old	0	0.00%	0	0
	18 to 24 years old	20	9.52%	12	8
	25 to 34 years old	82	39.05%	42	40
	35 to 44 years old	45	21.43%	24	21
	45 to 54 years old	43	20.48%	25	18
	55 to 64 years old	19	9.05%	3	16
	65 years or older	1	0.48%	0	1
Education	Some high school, but no diploma	2	0.95%	0	2
	High school diploma or equivalent (GED)	18	8.57%	7	11
	Some college credit, but no degree	32	15.24%	14	18
	Trade/technical/vocational certificate	8	3.81%	4	4
	Associate's degree	20	9.52%	9	11
	Bachelor's degree	92	43.81%	49	43
	Some graduate school work, but no graduate degree	5	2.38%	3	2
	Master's degree	25	11.90%	16	9
	Doctorate degree	8	3.81%	4	4
Work Experience	Less than 1 year	5	2.38%	3	2
	1 to 5 years	50	23.81%	21	29
	6 to 10 years	73	34.76%	37	36
	11 to 15 years	34	16.19%	22	12
	16 to 20 years	24	11.43%	13	11
	21 to 25 years	12	5.71%	6	6
	26 to 30 years	8	3.81%	4	4
	31 to 35 years	3	1.43%	0	3
	36 years or more	1	0.48%	0	1
Industry Sector	Extraction of natural resources	12	5.71%	9	3
	Transformation of natural resources	86	40.95%	19	67
	Physical service provider	20	9.52%	8	12
	Knowledge based service provider	92	43.81%	70	22

Table A2. Manifest Observations (Mode) on a Comprehensive Computer Security Policy

Variable ID	**Manifest Observation on a Comprehensive Computer Security Policy**	**Mode** **Σ** (n=210)	**Mode** **IT** (n=106)	**Mode** **OT** (n=104)
H11	My coworkers agree that I should comply with the new policy.	6	6	6
H12	My coworkers will think that I should comply with the new computer security policy.	6	6	6
H13	My supervisor will want me to comply with this new policy.	7	7	6
H21	It is important that I convince my coworkers to comply with the new computer security policy.	7	7	6
H22	My coworkers rely on my opinion.	6	7	6
H23	The new policy is important and others need to know how I feel about it.	6	7	6
H31	I will be reprimanded if my organization is aware of my non-secure actions.	7	7	6
H32	My management notices when I follow security procedures, and encourages me to keep doing a good job!	6	6	6
H33	I am encouraged when the company notices I am following security procedures.	6	7	6
H41	As a professional, I have to do certain things on my job. Strictly following computer security policies is one of them.	6	7	6
H42	Following computer security rules and policies is an important part of what I do as a professional.	7	7	6
H43	Breaking security policies hurts my image as a professional.	7	7	7
H51	This security policy helps to secure all computer systems.	7	7	6
H52	This security policy is absolutely necessary.	7	7	6
H53	This security policy is important.	7	7	6
H61	I understand the risks posed by poor security and that I may be reprimanded if I don’t comply with policy.	7	7	7
H62	I am aware of the potential threats and negative consequences that are possible if I don’t follow the proper security procedures.	7	7	6
H63	It is important that I follow the rules for keeping my organization secure so that I don’t get into trouble.	7	7	7
H71	My co-workers and I agree that complying with the new policy is the right thing to do.	6	7	6
H72	It is important to me that my co-workers comply with the new policy.	7	7	6
H73	It is important that my co-workers know that I intend to comply with the new computer security policy.	7	7	7
H81	I believe that complying with the new security policy is a good idea.	7	7	7
H82	I think that complying with the new security policy is the right thing to do.	7	7	7
H83	By complying with the new security policy I am helping the company stay secure from computer threats.	7	7	6
H91	Complying with the new policy helps to improve my job performance.	6	7	6
H92	Complying with the new policy lets me perform my tasks more effectively.	6	6	6
H93	Complying with the new policy makes it easier for me to do my job.	6	7	6
HA1	I am confident that I will comply with the new computer security policy.	7	7	7
HA2	I understand the benefits of the new computer security policy and I intend to comply with it.	7	7	6
HA3	Regardless of how others think or act, I intend to comply with the new computer security policy.	7	7	6

Author Biographies

Dennis C. Acuña is an information systems and information technology practitioner, with 36 years of hands-on experience in the oil and gas industry. He holds a doctorate in information systems from Dakota State University (2017) and currently teaches courses in information security, risk management for information systems, and information technology management at the University of Findlay, and the University of Toledo. He conducts original, empirical research in the field of information assurance and presents his findings at industry and academic conferences, along with publication in peer-reviewed academic journals. In addition to teaching and research activities, Acuña works as an independent, information systems governance, risk management, and compliance (GRC) consultant.

Rajab Suliman is an assistant lecturer in the Department of Information Operations and Technology Management (IOTM) in the College of Business and Innovation (COBI) at the University of Toledo. His research interests include business analytics, modeling and optimization using response surface methodology (RSM), linear mixed model (longitudinal data analysis), experiment design, and regression analysis (linear and non-linear). Suliman also works with extended zero-one beta regression models to investigate the effect of covenant proximity on brain activity. Suliman holds a Ph.D. in computational science and statistics from South Dakota State University (2017).

Nasir Elmesmari is chair of the Department of Statistics at the University of Benghazi / Al Marj-Libya. His research interests include genome wide association (GWAS) in genetics, linear mixed model (threshold model) and logistic model, MCMC Gibbs algorithm for simulation, time series and modeling of linear models. Elmesmari earned a Ph.D. in computational science and statistics from South Dakota State University (2017) with a dissertation titled “Threshold Models for Genome-wide Association Mapping of Familial Breast Cancer Incidence in Humans”