# Impact of Moral Disengagement on Counterproductive Work Behaviours in IT Sector, Pakistan

**QaziMuhamamd Ali**
**Business and Management Sciences, Superior University, Lahore, Pakistan**
Phdba2@gmail.com

**Abstract:** This research examines the role of moral disengagement towards counterproductive work behaviour in the information technology sector of Pakistan. Furthermore, research is also focused on the mediating effect of information security awareness (Attitude & knowledge) and information security awareness behaviours. The target population consisted of public sector I.T. departments of Punjab, Pakistan. A convenience sampling technique is utilized. Data collection has been done through a survey questionnaire from technical and non-technical staff currently employed in the Public sector I.T. departments of province Punjab. Statistical software PLS-SEM is used for analysis. This study highlights the role of the information technology sector staffing level of engagement that affects the employee's counterproductive work behaviour and information security awareness behaviour. Moreover, the study proposes that management should take the initiative for the implementation of strategies that may be helpful to get awareness about information security amongst employees.

**Keywords:** moral disengagement (M.D.), information security awareness (ISA), information security awareness knowledge (ISAK), counterproductive work behaviour (CWB), and information security awareness behaviour (ISAB)

## 1. Introduction

Cyber security is gaining importance worldwide because of the excessive usage of computers in all spheres of life (Chang and Coppel 2020). The potential outcome of information security breaches can have a broader effect, which includes disrepute of firms, competitive advantage, efficiency, and bankruptcy in a minor case (Jeong et al. 2019), (Schatz and Bashroush 2016). In the United Kingdom, primarily breaches of information security are found because of human error like irresponsible behaviour of workers in the firm and fraudulent emails responded by the employees (Hadlington 2021).

Cyber security is becoming the most important element for developing countries due to having future threats and weak organizational procedures and processes (Chang and Coppel 2020). Pakistan is an example of cyber security laws that have been established/applied by the state to combat cyber-attacks. Yet the threat remains significant because of gaps in applying these practices for various reasons (Khan and Anwar 2020).

In the last few years, there have been exponential advances in a study examining the role of the human component as an indicator of global information security awareness (Egelman and Peer 2015), (Parsons et al. 2014), (McCormac et al. 2018), (Janicke et al. 2018). The main focus of the current study is on individual differences that relate to gender and personality characteristics like amicability and carefulness (Butavicius et al. 2017), (McCormac et al. 2017).

However, the little investigation found in the literature shows how ISA is influenced by individual differences like; little research has been done to examine the complex relationship between adherence to information security awareness and a willingness to be morally detached, a key factor considered in a dysfunctional context or unproductive firm engagement. Literature has shown that M.D. is seen as a likely coping process to cope with the pressure of workplace safety necessities (D'Arcy et al. 2014). CWB is associated with a general disregard for firm procedure and safety (Spector et al. 2006), (Spector and Fox 2010). Furthermore, the main focus of information security awareness studies is on banking sectors compared to other information technology sectors (Dharmawansa and Madhuwanthi 2020), (Nasser et al. 2020), (Akinbowale et al. 2020).

Thus, this research aims to identify the connection between counterproductive work behaviour, M.D, and ISA. The second goal is to investigate how cognitive-emotional characteristics of ISA, like knowledge and attitude of ISA, can act as mechanisms that are underlying the connection between M.D and ISA behaviour and CWB. Although a previous researcher has shown that moral withdrawal predicts higher counterproductive work behaviour (Moore et al. 2012), the procedures after this connection are unclear. Likewise, studies showing a link between M.D. and ISA are very limited, especially in Asian countries (Chen et al. 2019), for later results in a Chinese perspective. There is no organized study of possible methods that combine the two.

This study contributes towards the information security in the Information Technology sector a neglected sector. Further, it enriches the literature by investigating a double mediation mechanism between moral disengagement and counter productive work behaviour by examining the role of information security awareness attitude, knowledge and behaviour of IT departmental staff in improving the counterproductive behaviour. The study contributes to the limited literature available on information security in the Asian context in different public or private information technology sectors of Punjab.

## 2. Hypothesis development

### 2.1 Relationship between moral disengagement and information security awareness

The researcher defines moral disengagement (Bandura 1986) as controlling individual actions that self-regulate in nature but can be selectively motivated (Hystad et al. 2014). MD includes eight types of interrelated cognitive processes that enable an employee to abandon intrinsic moral values to behave morally questionable (Moore 2015). These cognitive practices enable a person to reduce the distress feeling (Moore et al. 2012).

The author highlights that few studies examine that M.D can play for an immoral act in firms (Moore et al. 2012). Researchers connected the tendency of M.D. to behaviour like theft and dishonesty (Detert et al. 2008). The further author highlights that moral disengagement is considered a strong predictor for planned violation of information security awareness. It is noted that the main focus of previous studies is on a small set of violations that are linked with information security awareness while neglecting the other aspects that are related to disengagement in information security awareness like knowledge related to ISA processes and procedures as well as attitude of employees towards the ISA (D'Arcy et al. 2014). Few established studies show the connection between Moral disengagement and ISA & ISA behaviour (Hadlington et al. 2021).

> ***H1:*** *Moral disengagement has a significant positive relationship with Information Security awareness attitude*
>
> ***H2:****Moral disengagement has a significant positive relationship with Information Security awareness Knowledge*
>
> ***H3:*** *Moral disengagement has a significant positive relationship with Information Security awareness behaviour*
>
> ***H4:*** *Moral disengagement has a significant positive relationship with counterproductive work behaviour*

### 2.2 Relationship between information security and information security awareness:

The researchers from different perspectives have defined the term information security awareness (ISA), and most of the studies change that term to cyber security. A researcher argued with another concept and meaning and we do not consider it the same entity (Von Solms and Van Niekerk 2013). The main focus of information security is the information protection and system to save, transmit and utilize that information (Whitman and Mattord 2012).

Information Security is usually directed by a set of regulations that are established for employees by the organization to explain in terms of protocols and procedures that they must follow and do not share the credentials, report unusual activity (Parsons et al. 2014). Researchers said that unethical motives and deviancy affect the workers to oppose the protocols and procedures or to utilize information communication technology improperly (Wilks 2011). Such non-compliance of employees with firm standards may be seen as a part of firm citizenship. However, it is also mainly a problem with a solid moral aspect (Wilks 2011). So, employees who have a high tendency involve more counterwork behaviour. The people who are most involved in the counterwork behaviour and who have a strong propensity for M.D can also be the ones who have a more deficient commitment level with ISA.

> ***H5:*** *Information Security awareness attitude has a significant positive impact on Information Security awareness knowledge*
>
> ***H6:*** *Information Security awareness attitude has a significant positive impact on Information Security awareness behaviour*

***H7:*** *Information Security awareness knowledge has a significant positive impact on Information Security awareness behaviour*

## 2.3 Relationship between information security awareness and counterproductive work behaviours

Researchers said that workplace deviance includes any conduct that breaches the firm standards wilfully threatens the well-being of employees and the firm itself (Robinson and Bennett 1995). The study proposed that CWB are volitional and excluded from those activities that may be considered directly instructed (Fox et al. 2012). Furthermore, researchers highlight that most of the studies in this perspective mainly focused on predicting why employees are more committed to counterwork behaviour and how to prevent them from doing it (Robinson 2008). Whereas, the researcher suggests that counterproductive work behaviour can be considered as a kind of complaining behaviour; for example, Employees or a cluster of individuals can attentively participate in the CWB to correct perceived inequality or firm indisposition (Kelloway et al. 2010)

As per a few studies, misuse of information communication technology at the organization is usually neglected due to counterwork behaviour (Weatherbee 2010). A previous study confirmed that cyberloafing (non-professional use of ICT in the workplace) is significantly associated with poor information security awareness, with more frequent participation in cyber-loafing associated with lower participation in information security awareness (Hadlington and Parsons 2017). Disengagement in ISA might be one of the potential features of counterproductive work behaviour (Carpenter and Berry 2017). Researchers point out the connection between the withdrawal of employees and counterproductive work behaviour.

***H8:*** *Information Security awareness attitude has a significant positive impact on counterproductive work behaviour.*

***H9:*** *Information Security awareness knowledge has a significant positive impact on counterproductive work behaviour*

***H10:*** *Information Security awareness behaviour has a significant and positive relationship with counterproductive work behaviour*

***H11:*** *Information Security awareness attitude mediates the relationship between moral disengagement and counterproductive work behaviour*

***H12:*** *Information Security awareness knowledge mediates the relationship between moral disengagement and counterproductive work behaviour*

***H13:*** *Information Security awareness behaviour mediates the relationship between moral disengagement and counterproductive work behaviour*

***H14:*** *Information Security awareness attitude, Information Security awareness knowledge, and Information Security awareness behaviour mediates the relationship between moral disengagement and counterproductive work behaviour*

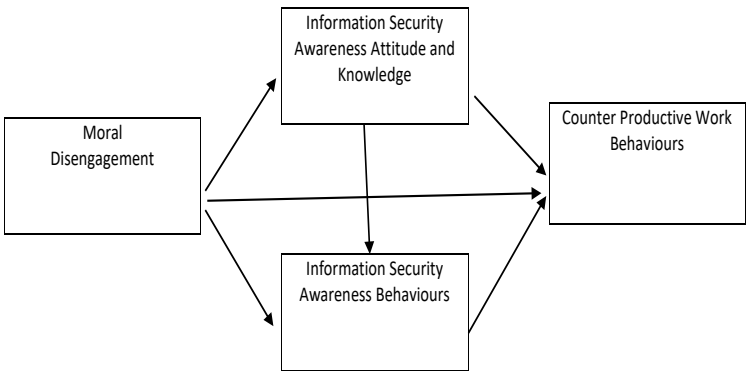



**Figure 1**: Theoretical framework

# 3. Methodology

## 3.1 Questionnaire

The measurement items of all variables were adopted from previous literature. A 5-point Likert scale was used from (1) Strongly Disagree to (5) strongly agree Current research aims to determine the connection between Moral Disengagement, ISA attitude and Knowledge, ISA Behaviours, and Counterproductive work behaviour based on technical staff's perception. The scale of 24 items was adopted from the literature of (Moore et al. 2016) to measure M.D. The researcher adopted ten items from the literature (Kaur and Mustafa 2013) to measure Information Security awareness. To measure the ISA behaviour, a scale of 06 items was adopted from the literature of (Kaur and Mustafa 2013). Moreover, the scale of 17 items was adapted from the literature of (Lee et al. 2005) to measure CWB in the information technology department.

## 3.2 Sample design and data collection

A quantitative survey method was used to collect the data from the public sector employees in the I.T. department of Pakistan, and a convenience sampling technique was utilized. Employees from several public sectors I.T. departments of Pakistan participated in the current study. The unit of analysis for this study is the employees of the I.T. department. The respondents were management staff, and technical staff responses were taken from two groups because the non-management staff is engaged in making the strategies and policies. In contrast, the technical staff is responsible for implementing those strategies. About 322 questionnaires were distributed among different workers employed in the I.T. department in Punjab after providing detailed information about the need for the current study, from which 223 were being returned out of which 16 were imperfect, so they were discarded and thus it was found that 207 were valid responses. The response rate of the current study was 64.28%.

# 4. Empirical findings

In this chapter, statistical data analysis has been done by using the smart PLS software as it is considered the most advanced technique for data analysis. Furthermore, PLS-SEM is utilized because of lesser needed data and data normality (Hair Jr et al. 2016). They keep going with this study by using Smart PLS-3 for analysis of data and evaluation of the hypothesis. The two-step procedures employed in this study highlighted the results recommended by (Henseler et al. 2009) and were considered most suitable in the field of social science research (Hair Jr et al. 2016).

## 4.1 Normality of data

In PLS-SEM, normal distribution of data is not required. It is critical to evaluate the normality distribution of data before applying inferential statistics (Hair et al. 2007). As per the researcher's recommendations (Munro 2005), Skewness and Kurtosis, and histogram charts are used to check the normality of data in PLS-SEM. The threshold for skewness and kurtosis is -2 to +2 for checking the normality of data. Results show that all variables are in between the threshold value, which shows that data are normally distributed.

## 4.2 Assessment of reflective measurement model

For assessing the measurement model in the current study, scholars confirmed both the validity and reliability of the data set. Composite reliability is used to assess data reliability whereas convergent, and discriminant validity measures the data validity. These results show the validity of measurements. Average Variance Extract (AVE) was used to assess convergent validity. The threshold for AVE is 0.500, and as shown in the table given below, 4.4.1. The AVE value of all items was more significant than the threshold value in the range of 0.504 to 0.936. Further, it also shows that all the measures of the 05 constructs were valid. Therefore, the model has sufficient convergent validity.

**Table 1:** Convergent validity

| Variables | Items | Loadings | Chronbach Alpha | Alpha | C.R. |
|---|---|---|---|---|---|
| Moral Disengagement | MD1 | 0.569 | 0.96 | 0.968 | 0.965 |
| | MD10 | 0.622 | | | |
| | MD11 | 0.715 | | | |

| Variables | Items | Loadings | Chronbach Alpha | Alpha | C.R. |
|---|---|---|---|---|---|
| | MD12 | 0.742 | | | |
| | MD13 | 0.902 | | | |
| | MD14 | 0.813 | | | |
| | MD15 | 0.875 | | | |
| | MD16 | 0.656 | | | |
| | MD17 | 0.759 | | | |
| | MD18 | 0.564 | | | |
| | MD19 | 0.892 | | | |
| | MD20 | 0.801 | | | |
| | MD21 | 0.652 | | | |
| | MD22 | 0.936 | | | |
| | MD23 | 0.817 | | | |
| | MD24 | 0.918 | | | |
| | MD7 | 0.617 | | | |
| | MD8 | 0.792 | | | |
| | MD9 | 0.85 | | | |
| Information Security Awareness Attitude | ISAA1 | 0.739 | 0.834 | 0.846 | 0.883 |
| | ISAA2 | 0.827 | | | |
| | ISAA3 | 0.773 | | | |
| | ISAA4 | 0.835 | | | |
| | ISAA5 | 0.697 | | | |
| Information Security Awareness Knowledge | ISAK1 | 0.775 | 0.828 | 0.877 | 0.882 |
| | ISAK2 | 0.898 | | | |
| | ISAK3 | 0.811 | | | |
| | ISAK4 | 0.74 | | | |
| Information Security Awareness Behaviour | ISAB1 | 0.834 | 0.886 | 0.933 | 0.919 |
| | ISAB2 | 0.878 | | | |
| | ISAB3 | 0.916 | | | |
| | ISAB4 | 0.808 | | | |
| Counterproductive Work Behaviour | CWB1 | 0.763 | 0.875 | 0.901 | 0.902 |
| | CWB14 | 0.641 | | | |
| | CWB16 | 0.779 | | | |
| | CWB2 | 0.912 | | | |
| | CWB3 | 0.909 | | | |
| | CWB5 | 0.504 | | | |
| | CWB6 | 0.692 | | | |
| | CWB7 | 0.605 | | | |
| | MD1 | 0.569 | 0.96 | 0.968 | 0.965 |
| | MD10 | 0.622 | | | |
| | MD11 | 0.715 | | | |

**Source:** Author's Design by using Smart PLS-3

## 4.3 Discriminant validity

HTMT ratio is a new criterion that is introduced to check the discriminant validity for variance-based SEM. (Henseler et al. 2015). The threshold value for HTMT ratios is less than 0.90, and if the value is greater than the threshold value, then the problem of discernment validity occurs. Table 4.3.1 shows the HTMT ratios of the 1st order construct, which shows each value is less than the threshold value, whereas table 4.3.2 shows the ratios. It also shows the values are less than 0.90 which means discriminant validity for constructs is established.

**Table 2:** HTMT ratio

| Items | CWB | ISAA | ISAB | ISAK | MD |
|---|---|---|---|---|---|
| CWB | | | | | |
| ISAA | 0.591 | | | | |
| ISAB | 0.247 | 0.348 | | | |
| ISAK | 0.564 | 0.874 | 0.306 | | |
| MD | 0.751 | 0.704 | 0.364 | 0.893 | |

**Source:** Author's Design by using Smart PLS-3

**Structure Equation Modelling (SEM) Path Analysis**

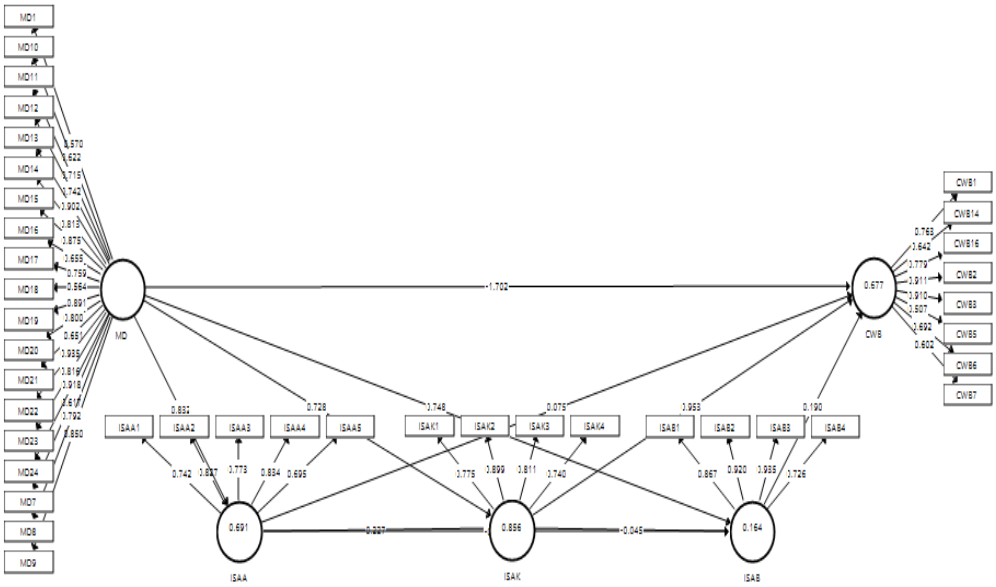



**Figure 2:** Measurement model assessment (Confirmatory Factor Analysis)

## 4.4 Assessment of Structural Model (SEM)

Hypothesis testing has been done using bootstrapping and PLS-SEM which shows the significant, positive, and negative relationships of variables. The indirect effect is used for mediation analysis. Table 4.4.1 shows the bootstrapping results. PLS-SEM and bootstrapping show the significant and positive relationship between moral disengagement and Information Security Awareness attitude (S.D. = 0.016, t = 5.801, p = 0.00). That means the 1st hypothesis is supported. Furthermore, a significant and positive connection between moral disengagement and Information Security Awareness knowledge shows β = 0.045 t = 16.216, p = 0.00). Therefore the 2nd hypothesis is also supported. A positive and significant relationship was found between moral disengagement and Information Security Awareness behaviour as the t value is greater than the threshold value. The p-value is less than 0.05 (β = 0.113, t = 6.597, P= 0.00) means hypothesis 3 is supported. However, results show the significant and positive relationship between moral disengagement and counterproductive work behaviour (β = 0.11, t = 15.526, P= 0.00), which means hypothesis 4 is supported. A significant and positive connection between Information Security Awareness and Information Security Awareness shows (β = 0.046 t = 4.904, p = 0.00). Therefore the 5$^{th}$ hypothesis is also supported. Further, a significant and positive connection has been found between Information Security Awareness attitude and Information Security awareness behaviour which shows β = 0.136 t = 3.736, p = 0.00). Therefore the 6$^{th}$ hypothesis is also supported. An insignificant connection between

Information Security awareness knowledge and Information Security awareness behaviour shows β = 0.142 t = 0.316, p = 0.752). Therefore the 7th hypothesis is also not supported. Besides this, the p-value of 0.437 was greater than the cut-off value of 0.05 which shows the insignificant relationships between Information Security awareness attitude and counterproductive work behaviour (β = 0.96, t = 0.778, p = 0.437) therefore hypothesis 8th is not supported and rejected. Moreover, a Significant and positive connection between Information Security awareness knowledge and counterproductive work behaviour shows β = 0.117, t = 8.129, p = 0.000). Based on the results hypothesis, 9th is supported. A positive and significant relationship was found between Information Security awareness behaviour and counterproductive work behaviour as the t value is greater than the threshold value. The p-value is less than 0.05 (β = 0.056, t = 3.407, P= 0.001); therefore it means hypothesis 10th is supported. As the t-value 0.776 and p-value = 0.438, which was lower than the threshold values, this study found an insignificant relationship between moral disengagement, Information Security awareness attitude, and counterproductive work behaviour (β = 0.08, t = 0.776, p =0.438). Based on the results hypothesis, 11th is rejected. A positive and significant relationship was found between moral disengagement, Information Security awareness knowledge, and counterproductive work behaviour as the t value is greater than the threshold value. The p-value is less than 0.05 (β = 0.117, t = 5.936, P= 0.000) therefore, it means hypothesis 12th is supported. However, results show the significant and positive relationship between moral disengagement, Information Security awareness behaviour, and counterproductive work behaviour (β = 0.029, t = 4.915, P= 0.000), which means hypothesis 13th is supported. Results of mediation analysis shows the insignificant relationship (β = 0.005, t = 0.338, P= 0.735) which means hypothesis 14th is not supported.

**Table 3:** Results of hypothesis (direct, indirect, mediation and moderation)

| | | SD | T | P | LLCI | ULCI | Decision |
|---|---|---|---|---|---|---|---|
| **H1** | MD -> ISAA | 0.016 | 5.801 | 0.000 | 0.799 | 0.86 | Supported |
| **H2** | MD -> ISAK | 0.045 | 16.216 | 0.000 | 0.64 | 0.814 | Supported |
| **H3** | MD -> ISAB | 0.113 | 6.597 | 0.000 | 0.5 | 0.938 | Supported |
| **H4** | MD -> CWB | 0.11 | 15.526 | 0.000 | 1.949 | 1.532 | Supported |
| **H5** | ISAA -> ISAK | 0.046 | 4.904 | 0.000 | 0.135 | 0.314 | Supported |
| **H6** | ISAA -> ISAB | 0.136 | 3.736 | 0.000 | 0.783 | 0.255 | Supported |
| **H7** | ISAK -> ISAB | 0.142 | 0.316 | 0.752 | 0.341 | 0.224 | Not Supported |
| **H8** | ISAA -> CWB | 0.096 | 0.778 | 0.437 | 0.123 | 0.244 | Not Supported |
| **H9** | ISAK -> CWB | 0.117 | 8.129 | 0.000 | 0.748 | 1.225 | Supported |
| **H10** | ISAB -> CWB | 0.056 | 3.407 | 0.001 | 0.085 | 0.303 | Supported |
| **H11** | MD -> ISAA -> CWB | 0.08 | 0.776 | 0.438 | 0.09 | 0.211 | Not Supported |
| **H12** | MD -> ISAK -> CWB | 0.117 | 5.936 | 0.000 | 0.502 | 0.949 | Supported |
| **H13** | MD -> ISAB -> CWB | 0.029 | 4.915 | 0.000 | 0.078 | 0.193 | Supported |
| **H14** | MD -> ISAA -> ISAK-> ISAB -> CWB | 0.005 | 0.338 | 0.735 | 0.011 | 0.008 | Not Supported |

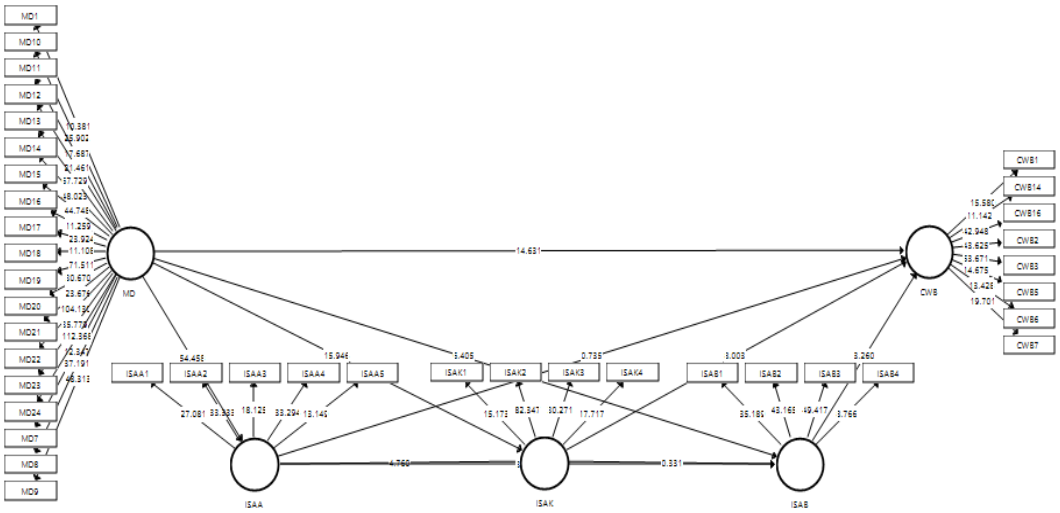



**Figure 3:** Structural model assessment

## 5. Discussion

The main objective of the present study was to inspect the way through which individual differences in M.D. and CWB are related to ISA. Whereas literature has pointed out the general connection between moral disengagement and counterproductive work behaviour related to the firm's information technology security protocol, more comprehensive and reliable models were lacking, allowing for the expansion of productive training and no other interventions. Based on various I.T. workloads, it has been theorized that ISA will at least partially explain the relationship between M.D. and CWB. A framework was projected in which Information Security attitude, knowledge, and behaviour mediates the relationship between moral disengagement and counterproductive work behaviour.

Overall, the findings revealed numerous fascinating trends among the tendency for M.D. and ISA. All the hypothesis of moral disengagement is significantly positively related to Information Security awareness and behaviour. Vigorous correlations among moral disengagement and Information Security awareness were those that imply a separation of concerns if all subscales are checked. From the Information Security perspective, this can indicate a significant obstacle to active protocol compliance. It can be effortless for people to bypass their Information Security awareness in several firms and depend on others to burden it. Literature has shown that many employees are often unaware of their role in the active firm cyber security of an organization and instead rely on that this is something that firm administration should be held accountable for (Hadlington 2017).

It should be noted that Information Security awareness attitude and knowledge were as closely related to counterproductive work behaviour as the behavioural aspect. In particular, this may reflect some conceptual overlap between counterproductive work behaviour and Information Security awareness behaviour. Research participants may understand to include a task related to information technology. As mentioned earlier, I.T. activities in many professions make up a significant portion of all work-related activities.

It is not surprising that counterproductive work behaviour and Information Security awareness negative behaviour go hand in hand. A second related point that needs to be emphasized is that Information Security awareness attitude and knowledge can, therefore, as our many mediation models postulate, influence counterproductive work behaviour and Information Security awareness behaviour. In addition, the counterproductive work behaviour was positively associated with the moral disengagement subscales and provided an accurate mirroring of the relationship between Information Security awareness and moral disengagement. The further endorses previous evidence of the moral disengagement association with immoral behaviour and general disrespect for basic security policies (Cohen et al. 2013), (Spector and Fox 2010).

The results of multivariate causal modeling are consistent with our theoretical model. As predicted, Information Security knowledge and behaviour reflect the relationship between M.D. and behavioural outcomes. Essentially, the behavioural results evaluated in the current study were mixed. Firstly, the process of mediation that leads to CWB instantly seems believable. It also leads to a lesser progressive attitude about ISA guidelines and protocols. Knowledge attitudes are essential ancestors of behaviour that impact the Information Security of a single user and the firm. However, the model's second mediation method expands the role of communicating information security awareness specific views and knowledge to the broader domain of counterproductive work behaviour. That may specify that the counterproductive work behaviour and the Information Security awareness behavioural element overlap at a theoretical or operational level, but the two constructs were defined in diverse theoretical contexts. The methods were used in current research change significantly in terms of a particular behaviour. Additional clarification could be such that Information Security awareness attitude and Information Security awareness knowledge follow a more general path from moral disengagement to counterproductive work behaviour. It characterizes more important motivators for compliance behaviour.

## 6. Limitation and future directions

Chances of further research always exist because of theoretical and methodological limitations. Several information technology departments in Pakistan are also making efforts to implement strategies that are helping to secure the information. Future research work should be sufficient enough to study the impact of moral disengagement and counterproductive work in Information Security awareness in-depth to understand I.T. sectors in a better way. Moreover, this study should be applied in different countries while considering the cross-cultural setting. It will be helpful to measure Information Security awareness in the I.T. sectors globally. The current study is based on quantitative; the data were collected based on adopted questionnaires from previous

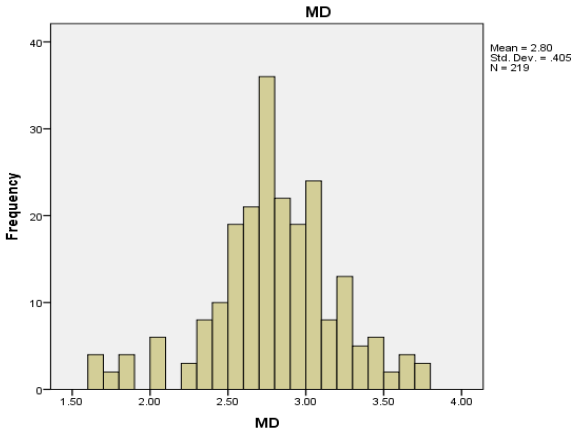
studies based on respondents' perception with limited information. Therefore, upcoming studies may focus on a mixed-method approach to examine the above-said relationships. It will be helpful for better understanding in analysis. Other Independent and dependent variables may be used to explore just like organizational abuse and discipline.

## Appendix 1

**Data Normality**

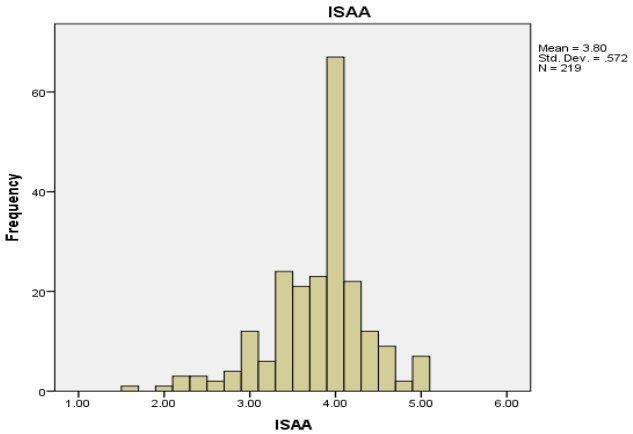
*Histogram Charts*

- 1. Moral Disengagement



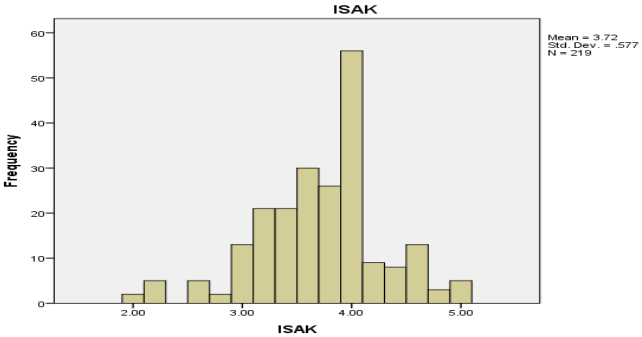

Source: Designed by using IBM SPSS-23

- 2. Information Security Awareness Attitude



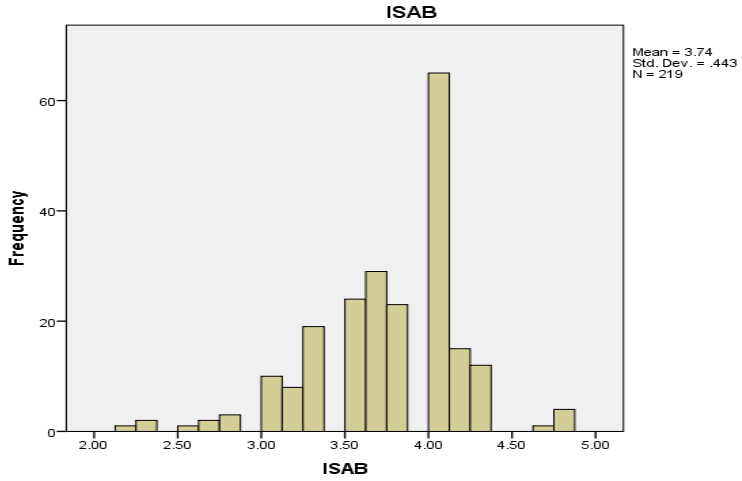

Source: Designed by using IBM SPSS-23

- 3. Information Security Awareness Knowledge



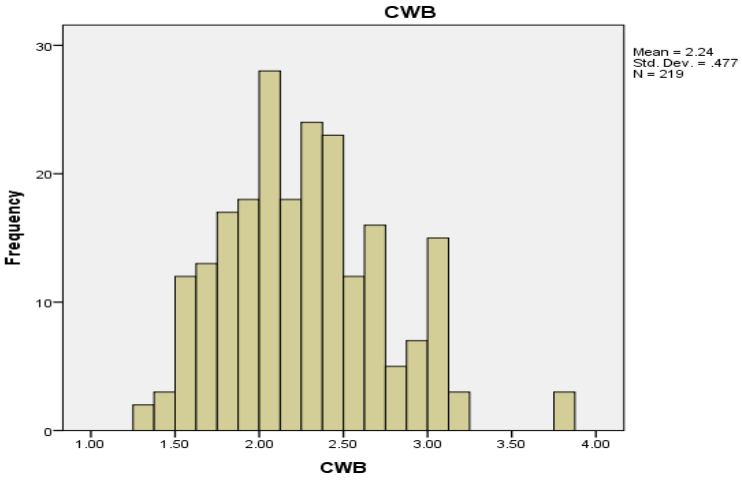

Source: Designed by using IBM SPSS-23

- 4. Information Security Awareness Behaviour




Source: Designed by using IBM SPSS-23

- 5. Counterproductive Work Behaviour




Source: Designed by using IBM SPSS-23

## References

Akinbowale, O. E., Klingelhöfer, H. E. andZerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using balance score card: a survey of literature. Journal of Financial Crime,Vol 27, No. 3, pp 945-958.

Bandura, A., & National Inst of Mental Health. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall, Inc.

Butavicius, M. A., Parsons, K., Pattinson, M. R., Mccormac, A., Calic, D. and Lillie, M. (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture,pp 12-23.

Carpenter, N. C. and Berry, C. M. (2017). Are counterproductive work behaviour and withdrawal empirically distinct? A meta-analytic investigation. Journal of Management, Vol 43 No. 3, pp834-863.

Chang, L. Y. andCoppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. Computers & Security, Vol 97, 101959.

Chen, H., Chau, P. Y. and Li, W. (2019). The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behaviour. Information Technology and People,Vol 32 No. 4, pp 973-994.

Cohen, T. R., Panter, A. andTuran, N. (2013). Predicting counterproductive work behaviour from guilt proneness. Journal of Business Ethics, Vol114 No. 1, pp45-53.

D'arcy, J., Herath, T. &Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems, Vol31 No. 2, pp. 285-318.

Detert, J. R., Treviño, L. K. andSweitzer, V. L. (2008). Moral disengagement in ethical decision making: a study of antecedents and outcomes. Journal of Applied Psychology, Vol 93 No. 2, pp 374-391.

Dharmawansa, A. D. andMadhuwanthi, R. (2020). Evaluating the Information Security Awareness (ISA) of Employees in the Banking Sector: A Case Study.

Egelman, S. & Peer, E. Scaling the security wall: Developing a security behaviour intentions scale (sebis). Proceedings of the 33rd annual ACM conference on human factors in computing systems, 2015. Pp. 2873-2882.

Fox, S., Spector, P. E., Goh, A., Bruursema, K. & Kessler, S. R. (2012). The deviant citizen: Measuring potential positive relations between counterproductive work behaviour and organizational citizenship behaviour. Journal of Occupational and Organizational Psychology, Vol 85 No. 1, pp 199-220.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, Vol 3 No. 7, e00346.

Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. Research Anthology on Artificial Intelligence Applications in Security. IGI Global.

Hadlington, L., Binder, J. andStanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. Computers in Human Behaviour, Vol. 114, 106557.

Hadlington, L. and Parsons, K. (2017). Can cyberloafing and Internet addiction affect organizational information security? Cyberpsychology, Behaviour, and Social Networking, Vol20 No. 9, pp567-571.

Hair, J. F., Money, A. H., Samouel, P. and Page, M. (2007). Research methods for business. Education+ Training.Vol 49 No. 4, pp 336-337.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. andSarstedt, M. (2016). A primer on partial least squares structural equation modeling (PLS-SEM), Sage publications.

Henseler, J., Ringle, C. M. andSarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the academy of marketing science, Vol 43 No. 1, pp 115-135.

Henseler, J., Ringle, C. M. andSinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. New challenges to international marketing. Emerald Group Publishing Limited,Vol 23, pp 277-319.

Hystad, S. W., Mearns, K. J. and Eid, J. (2014). Moral disengagement as a mechanism between perceptions of organisational injustice and deviant work behaviours. Safety Science, Vol68, pp138-145.

Janicke, H., Hadlington, L., Yevseyeva, I., Jones, K. andPopovac, M. (2018). Exploring the role of work identity and work locus of control in information security awareness,Vol 81, pp 41-48.

Jeong, C. Y., Lee, S.-Y. T. and Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information and Management, Vol56 No. 5, pp681-695.

Kaur, J. & Mustafa, N. Examiningthe effects of knowledge, attitude and behaviour on information security awareness: A case on SME. (2013). International Conference on Research and Innovation in Information Systems (ICRIIS), 2013. IEEE, pp. 286-290.

Kelloway, E. K., Francis, L., Prosser, M. and Cameron, J. E. (2010). Counterproductive work behaviour as protest. Human resource management review, Vol 20 No. 1, pp. 18-25.

Khan, U. P. and Anwar, M. W. (2020). Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward. Cyberpolitik Journal, Vol5 No. 10, pp 205-218.

Lee, K., Ashton, M. C. and Shin, K. H. (2005). Personality correlates of workplace anti-social behaviour. Applied Psychology, Vol54 No. 1, pp 81-98.

Mccormac, A., Calic, D., Parsons, K.,Butavicius, M., Pattinson, M. and Lillie, M. (2018). The effect of resilience and job stress on information security awareness. Information & Computer Security, Vol 26 No. 3, pp 277-289.

Mccormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behaviour, Vol 69,pp151-156.

Moore, C. (2015). Moral disengagement. Current Opinion in Psychology, Vol 6,pp199-204.

Moore, C., Detert, J. R., KlebeTreviño, L., Baker, V. L. and Mayer, D. M. (2012). Why employees do bad things: Moral disengagement and unethical organizational behaviour. Personnel Psychology, Vol65 No.1.pp 1-48.

Moore, C., Detert, J. R., Treviño, L. K., Baker, V. L., & Mayer, D. M. (2016). "Why employees do bad things: Moral disengagement and unethical organizational behaviour": Corrigendum. Personnel Psychology, Vol 69 (1), pp 307.

Munro, B. H. (2005). Statistical methods for health care research, lippincottwilliams&wilkins.

Nasser, A. A., Al Ansi, N. K. A. and Al Sharabi, N. A. (2020). On The Standardization Practices of the Information Security Operations in Banking Sector: Evidence from Yemen. Int. J. Sci. Res. in Computer Science and Engineering, Vol 8 No. 6. pp 8-18.

Parsons, K., Mccormac, A.,Butavicius, M., Pattinson, M. andJerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security, Vol 42.pp 165-176.

Robinson, S. L. (2008). Dysfunctional workplace behaviour. The Sage handbook of organizational behaviour, Vol1, pp 141-159.

Robinson, S. L. and Bennett, R. J. (1995). A typology of deviant workplace behaviours: A multidimensional scaling study. Academy of management journal, Vol38 No. 2, pp555-572.

Schatz, D. andBashroush, R. (2016). The impact of repeated data breach events on organisations' market value. Information & Computer Security,Vol 24 No. 1, pp 73-92.

Spector, P. E. and Fox, S. (2010). Counterproductive work behaviour and organisational citizenship behaviour: Are they opposite forms of active behaviour? Applied Psychology, Vol 59 No. 1, pp 21-39.

Spector, P. E., Fox, S., Penney, L. M., Bruursema, K., Goh, A. and Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviours created equal? Journal of vocational behaviour, Vol*68 No.* 3, pp 446–460.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. computersand security, Vol 38. pp 97-102.

Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information and communications technologies and cyberdeviancy. Human Resource Management Review, Vol20 No. 1, pp35-44.

Whitman, M. andMattord, H. (2012). Legal, ethical, and professional issues in information security. Principles of information security (4th ed.; pp. 133–147). Boston, MA: Course Technology, Cengage Learning. Retrieved from http://www. cengage. com/resource_uploads/downloads/1111138214_259148. pdf.

Wilks, D. C. (2011). Attitudes towards unethical behaviours in organizational settings: An empirical study. Ethics in Progress, Vol 2 No. 2 pp 9-22.