International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyberpsychology Based Insider Threat Prediction Model Approach for Cybersecurity

Jitendranath Palem[1], Sivaprakash Palaniswamy[2]

[1]General Manager, Cybersecurity ofDigital Foundation Services, HCLTech
[2]Vice President, Cybersecurity of Digital Foundation Services, HCLTech

Abstract

Cybersecurity plays an important role not only in the field of information technology, but also in our everyday lives in society. Protecting information has become one of today's biggest challenges. Every time we think about Cybersecurity, the first thing that comes to mind is cybercrime, which is becoming extremely complex and unpredictable every day. Various Governments and companies are taking numerous measures to prevent cybercrime. Beyond a variety of measures, Cybersecurity is still a huge concern for many, as most measures are solely technology-based.

It is unlikely that we will succeed in solving our problems if we do not truly understand their ultimate source- the human mind.We live in an environment of violent promotion. We make the situation worse by watching, sharing, posting and glorifying violence on entertainment platforms through gadgets.

Due to the virtue of technology, all sorts of entertainment are readily available. As the world turns into a global digital village, attackers are getting smarter and more unpredictable. Attackers are disguised in many ways and risk is ever present. In an organization setting, insider threats or malicious insiders cover a range of scenarios ranging from disgruntled employees to those who specifically penetrate the organization's systems to steal or damage. Although the software industry develops security products based on artificial intelligence, cyber-attacks continue to occur worldwide. Basic cognitive capacities of humans are disrupted at a higher rate because of the wide variety of information explosion across computer systems or devices. This provides an opportunity for sociologists and psychologists to directly detect and diagnose any abnormal behavior on an individual level. The software industry can see the value of integrating psychology and Cyberpsychology to develop holistic cybersecurity products based on systems thinking. Some organizations already use certain psychological methods, like psychometric interviews based on tests, counseling sessions on psychological well-being and so on.This paper focuses on demonstrating a fundamental prediction model based on ordinal logistic regression technique for creating an awareness and the importance a holistic cybersecurity product and services based on Cyberpsychology. Integrating cyberpsychology into an AI-based cybersecurity product will provide a powerful combination and effectively prevent malicious internal attacks.

Keywords: Cybersecurity, Cyberpsychology, Insider threats, psychological factors, Machine learning, Ordinal Logistic Regression model and Prediction

1. Introduction

The insider threat has been identified as a key threat to organizations and governments. Understanding the nature of internal or malicious threats and associated threats can assist in developing mitigation strategies, including non-technical means. It is natural that humans will always interact with any device at some level and human behavior thus becomes a part of the whole network eco system. A human actor is always the initiator of any attack upon a system. It is therefore imperative to understand how people interact and communicate with the technologies at hand and what individual behaviors may introduce vulnerabilities. When we apply the same logic in the context of an employee and employer scenario, it helps us to better understand the insider threat mechanism and the factors that make susceptible to malicious influence. In this paper, Insider threat prediction model is proposed based on Cyberpsychology philosophy. An insider attack is the execution of a latent threat by an insider to achieve their goals, which usually has a detrimental effect on the organization. They are often straightforward to perpetrate without detection using their legitimate access, or acquiring unauthorized access using their knowledge of system weaknesses to defeat the controls. The proposed methodology in this paper describes the ideal independent variables the management has to capture and measure in a real time basis in order to devise suitable prediction models in a cost-effective manner using the statistical quantitative analytical computing methods of machine learning.

Insider threats to institutions, enterprises, and government agencies continue to be a major problem. The veracity and frequency of this threat in firms today are well demonstrated by current studies. [1,2]. According to a 2020 global report [3], the average global cost of insider threats rose by 31% in the last two years to $11.45 million, and the occurrence of incidents spiked by 47% in that period. Through the assessment and analysis of incidents, the challenge of insider threat (IT) can be better understood and addressed. Insider threat incidents have increased to significant levels [4]. The most important conclusion is that credential theft poses the most expensive insider danger per event. Both the incidence and expense of these catastrophes have greatly grown. In fact, since 2016, the average number of occurrences per organization has climbed from 1 to 3.2, and the average cost has gone up from USD $493,093 to USD $871,686 in 2019. Organizations are spending more annually to cope with insider negligence, but the cost per occurrence is significantly lower [5]. This is because insiders often have good knowledge of the environmental set-up, and ready access to the assets owned by their employers. Such individuals often have the trust of their organization, which enables them to gain authorized access and bypass electronic and physical security controls [6]. Nonetheless, more than 75% of these incidents are typically handled internally without being reported to law enforcement agencies, and often no legal action is taken [7].

2. Scope

Despite tremendous effort in recent years, insider threat mitigation has generally made only modest progress [8]. People who are not employed by the organization's security team may be able to identify malicious insider threat actions. This is demonstrated in [9,10], which demonstrates that just one in five instances of such activities are discovered using a mix of automated methods for logging, monitoring, and reporting suspicious activity in addition to manual diagnosis and analysis. Many of the Cyberpsychology books and articles reveals an astounding fact that many of the Cybersecurity service providers in the world predominantly see the security issues with the lens of technology and they are

very keen on strengthening their defense mechanism through hefty investment on advanced technologies. This kind of approach does not yield a complete sustainable benefit and especially it cannot transform their services into proactive from a reactive based mechanism. Furthermore, this kind of merely technology centric products and corresponding business process hinders meeting the corporate ESG(Environmental, social and governance) ratings.

3. Literature Review

In recent years, the literature on insider threat detection has garnered much attention. Past studies have focused on insider threat profile [11, 12], and abnormal detection approaches [13, 14]. However, to the best of our knowledge, there is no study on insider threat prediction model creation based on cyber-psychology. Furthermore, most of the Cybersecurity service providers are gradually realizing the power of employing a Cyberpsychology practitioner or expert roles that can effectively and holistically manage the insider threats. In the banking and financial industry, actual insider attack cases that were discovered through public reporting were reviewed by Randazzo et al. [12]. They used a behavioral and technical viewpoint to analyze the situations. The report also describes the communication patterns and behaviors' leading up to the damaging activities. They presented insights that can help with future study and policy development.

According to research conducted by Lieberman Software Corporation at Microsoft Ignite 2015, 35% of IT professionals believe insider threats pose a greater risk than external cyber-attacks, which supports the growing worry about the risks of insider assaults [15]. Whether an insider acts maliciously or unintentionally, the insider threat is real, serious, and challenging to counter. For this reason, dangers exist. An author Cole noted that "unknown" and "no value placed" losses were highest in a SANS 2017 Insider Threat Survey [16], indicating that most organizations lack adequate monitoring and reporting methods to assess the true cost of insider assaults. The readers may feel that few of these citations are quite old however; the fact is that, whether these citations are old or new, the impact is significant and the risk is still relevant today. In spite of the damage to their reputation and the potential for fines, more than 40% of respondents indicated that they were worried about bad press, indicating that organizations at least recognize the issue and the need to report breaches [17].

A review of the literature and posts on Cybersecurity attacks shows that increasingly they involve social engineering techniques; where psychological principles are used to manipulate people into disclosing sensitive information or allowing others to access a secure system [18]. For example, to get people to click on a link, phishing emails and phone calls use a variety of psychological techniques related to social influence, such as appeals to fear or creating a sense of urgency or scarcity [19]. However, despite the psychological nature of such Cybersecurity attacks, research into the role of psychology in Cybersecurity is still limited. Also, often research into the closely linked area of social engineering is conducted from the discipline of computing rather than psychology. However, within the last year the importance of psychology has begun to be recognized in the academic literature [20]. In contrast, large scale Cybersecurity incidents are often instigated by groups, as opposed to individuals acting alone. As such these incidents can be regarded as the result of group actions and group processes; theories from Psychology are used to help understand the formation, operation and influence of groups on their members and these can be usefully applied to online groups.

Psychology can offer much in helping to understand the motivations of individual hackers or scammers, for example drawing on the research into individual differences, looking at factors such as self-esteem, introversion, openness to experience and social anxiety [21]. Other work has shown that individual's motivations are not always related to financial gain but can be purely for entertainment or social status reasons. Numerous hacking cases, particularly those committed by adolescents and young adults, have been closely linked to peer pressure and other social psychological factors. Numerous online behaviorshave been explained by psychological theories of disinhibiting and individuation, which can also be utilized to comprehend Cybersecurity problems.

4. Proposed method for Predictive Model creation

Proposed method of predictive model creation involves identifying the ideal independent variables. Many organizations are still having silo-based data and tools. These highly disintegrated tools are prone for the insider attacks. A theoretical synthetic data that contains 120 records are used for predictive model creation and leveraged the Ordinal logistic regression technique for building a predictive model. The findings revealed that there is an impact of employees' information on insider threat risk. In this study, increasing the Habit of Alcohol habits and less performance appraisal rating, interested in movies like Science fiction and Crime/Thriller/Horror movies and Political News Interest was associated with an increased in the likelihood of exhibiting Insider Threat Risk. The study lays a foundation for understanding behavioral traits when employing staff members, as well as for being able to continuously observe staff behavior to prevent potential dissatisfaction or other worrying behavior.

A great deal of research has been devoted to the exploration and categorization of threats posed from malicious attacks from current employees who are disgruntled with the organization, or are motivated by financial gain. These so-called "insider threats" pose a growing menace to information security, but given the right mechanisms, they have the potential to be detected and caught. In contrast, human factors related to aspects of poor planning, lack of attention to detail, and ignorance is linked to the rise of the accidental or unintentional insider. In this instance there is no malicious intent and no prior planning for their "attack," but their actions can be equally as damaging and disruptive to the organization. This paper presents an approach for creating a predict. Formal definitions of 'Cybersecurity' typically revolve around systems, standards, technologies and processes for protecting computer systems, networks and the data they contain from unauthorized access or malicious attacks. Such a definition may imply that Cybersecurity is somewhat of a dry, technically focused enterprise, mainly of concern to computer network professionals or system engineers and industry professionals. That is a far away from the truth: Cybersecurity and security breaches have profound implications for all of us Humans will always interact with any device at some level, and human behavior thus becomes a part of the system. For example, what factors might make some individuals or organizations more susceptible to malicious influence. How do psychological phenomena and information technologies intervene, strengthen or facilitate such processes of influence? What can be done to protect individuals, groups and systems from such attacks? These questions are clearly in the domain of psychology and the behavioral sciences. Without considering them, no approach to Cybersecurity can ever be successful.

In the literature, a number of insider models have been put out. One of them employs numerous, but challenging to quantify, signs, such as language and psychological characteristics, to be able to anticipate insider assaults. Markov's Hidden Inferring divergence between a user's activity patterns and a

set of existing activity models has also been done using models. Psychological traits of an insider, including depression and introversion, have also been recognized and addressed. Best practices have also been suggested for the detection and prevention of the insider threat. In this study, the Ordinal logistic regression model was used to predict the internal threat risk in the organization. There are fifteen independent variables and one dependent variable as insider threat risk likert scale variable has five values 1 to 5, for the low risk to high risk of an attribute.

Table 1: Table Type Styles

<table>
<tr><th colspan="2">Explanatory Variables(X)</th><th>Response Variable(Y)</th></tr>
<tr><td>1. Gender</td><td>9. Manager feedback</td><td rowspan="9">Insider threat risk</td></tr>
<tr><td>2. Age</td><td>10. Customer Feedback</td></tr>
<tr><td>3. Education Qualification</td><td>11. Habit of smoking</td></tr>
<tr><td>4. Marital Status</td><td>12. Habit of Alcohol</td></tr>
<tr><td>5. Employee band</td><td>13. Honor/Award</td></tr>
<tr><td>6. Employee Experience</td><td>14. Movies Interested</td></tr>
<tr><td>7. Tenure in the company</td><td>15. Political news interested</td></tr>
<tr><td>8. Performance appraisal rating</td><td></td></tr>
<tr><td colspan="2">Having more independent variable can lead to over-adjustment, Hence, it is important to consider only the minimum necessary variables based on “Employee wellbeing individual counseling sessions” using various methods of Cyberpsychology, Neuro linguistic program techniques or ethnographic a placebo technique</td></tr>
</table>

5. Output Summary

In this section, the results of the quantitative dataare presented. The data was first entered into an excel file and exported into an analytical tool. The sample size for the study is n=120. The analysis carried out was percentage analysis to find out the demographical information of respondents. Descriptive statistics are used to summarize the data.Variables are expressed as the mean. Chi-Square test is performed to find the association between two categorical variables. Technique used in the data analysis method known as Ordinal logistic regression to determine the associations between two data factors. The value of one of those parameters is then predicted depending on the other using this relationship. Typically, the forecast has a limited number of possible outcomes, such as low risk to high risk.

Table 2: Frequency of Personal information of the employees

	Frequency (n)	Percentage (%)
Gender		
Male	84	70.0
Female	36	30.0
Age		
Less than 25	9	7.5
26 to 30	33	27.5
31 to 35	19	15.8

36 to 40	21	17.5
More than 40	38	31.7
Education Qualification		
Under Graduate	19	15.8
Post Graduate	29	23.3
Ph.D.	25	20.8
Diploma	21	17.5
Others	27	22.5
Marital Status		
Single	76	63.3
Married	33	27.5
Widow	6	5.0
Separated	5	4.2
Total	**120**	**100.0**

The individual information of the personnel is shown in Table 2. Out of 120 respondents, 70% were men, The majority of responders (23.3%) among the participants were post-graduates, and 63.3% of them were single and unmarried.

Table 3: Frequency of official information of the employees

	Frequency (n)	**Percentage (%)**
Employee Band		
EB1	31	25.8
EB2	32	26.7
EB3	33	27.5
EB4	10	8.3
EB5	14	11.7
Experience		
Less than 1 year	20	16.7
1 to 5 years	39	32.5
6 to 10 years	38	31.7
More than 10 years	23	19.2
Tenure in the company		
Less than 1 year	24	20.0
1 to 5 years	69	57.5
6 to 10 years	16	13.3
More than 10 years	11	9.2
Manager feedback		
Excellent	59	49.2
Good	26	21.7
Poor	35	29.2
Customer Feedback		

Excellent	73	60.8
Good	12	10.0
Poor	35	29.2
Honor/Award		
Yes	51	42.5
No	69	57.5
Total	**120**	**100.0**

The official information about the staff is shown in Table 3. The majority of respondents (27.5%) were into Band EB3, and the majority of respondents (32.9%) had experience ranging from 6 to 10 years but less than 1 year. The majority of participants (49.2%) received excellent feedback from their manager, and 60.8% of participants received excellent feedback from their clients. It was also discovered that 42.5% of them received an award or honor.

Table 4: Frequency of habits of the employees

	Frequency (n)	**Percentage (%)**
Habit of smoking		
Yes	53	44.2
No	47	39.2
Sometimes	20	16.7
Habit of Alcohol		
Yes	64	53.3
No	34	28.3
Sometimes	22	18.3
Total	**120**	**100.0**

The staff behavior is shown in Table 4. It shows 44.2% of respondents did smoking regularly, followed by 39.2% of respondents who reported that they did not smoke, and 16.7% of respondents who reported occasional smoking. The majority of respondents among the participants53.3% said they did regularly consume alcohol, followed by 28.3% who said they did not and 18.3% who said they did so occasionally**.**

Table 5: Frequency of insider threat risk

	Frequency (n)	**Percentage (%)**
Very High Risk	37	30.8
High Risk	19	15.8
Medium	19	15.8
Low Risk	22	18.3
Very Low Risk	23	19.2
Total	**120**	**100.0**

Table 5 shows the frequency of insider threat risk. Majority 30.8% chances of very high risk of insider threat risk and 19.2% were did not insider threat risk.

Table 6: Association between insider threat risk and getting feedback From the managers and customers

		Insider Threat Risk					Total	Chi Square (p value)
		Very high risk	High risk	Medium	Low risk	Very low risk		
Manager Feedback	Excellent	6	12	9	11	21	**59**	**41.162 (0.000)****
	Good	11	1	4	8	2	**26**	
	Poor	20	6	6	3	0	**35**	
Customer Feedback	Excellent	15	13	10	14	21	**73**	**29.815 (0.000)****
	Good	2	0	3	5	2	**12**	
	Poor	20	6	6	3	0	**35**	
Honor/ Award	No	28	8	5	14	14	**69**	**14.851 (0.005)****
	Yes	9	11	14	8	9	**51**	
Total		**37**	**19**	**19**	**22**	**23**	**120**	

**p<0.01, N.S: Not Significant

The relationship between insider threat risk and respondents' Job role professional information is seen in Table 6. Due to the fact that the p values for the manager feedback (p<0.01), and customer feedback (p<0.01) and honor/award (p<0.01) are all less than the 0.01 significant threshold. Therefore, there is a connection between the respondents' official information and the danger of insider threat. According to the above table, there is a risk of insider threat as a result of poor manager and customer feedback. The risk here could be even attrition risk as well.

Table 7: Association between insider threat risk and Habits getting of the respondents

		Insider Threat Risk					Total	Chi Square (p value)
		Very high risk	High risk	Medium	Low risk	Very low risk		
Habit of smoking	Yes	17	11	8	10	7	**53**	7.559 (0.478) N.S
	No	16	4	7	7	13	**47**	
	Sometimes	4	4	4	5	3	**20**	
Habit of Alcohol	Yes	22	9	14	3	16	**64**	**46.532 (0.000)****
	No	1	10	5	13	5	**34**	
	Sometimes	14	0	0	6	2	**22**	
Total		**37**	**19**	**19**	**22**	**23**	**120**	

**p<0.01, N.S: Not Significant

The relationship between the respondents' habits and their chance of insider threat is shown in Table 7.Because the p-values for drinking habits are both below than the 0.05 level of significance. As a result,

there is a connection between respondents' changing habits and the risk of an insider threat. According to the above data, individuals who often drink alcohol are at risk for experiencing an insider threat**.**

Figure 1: Insider threat risk and official information of the respondents

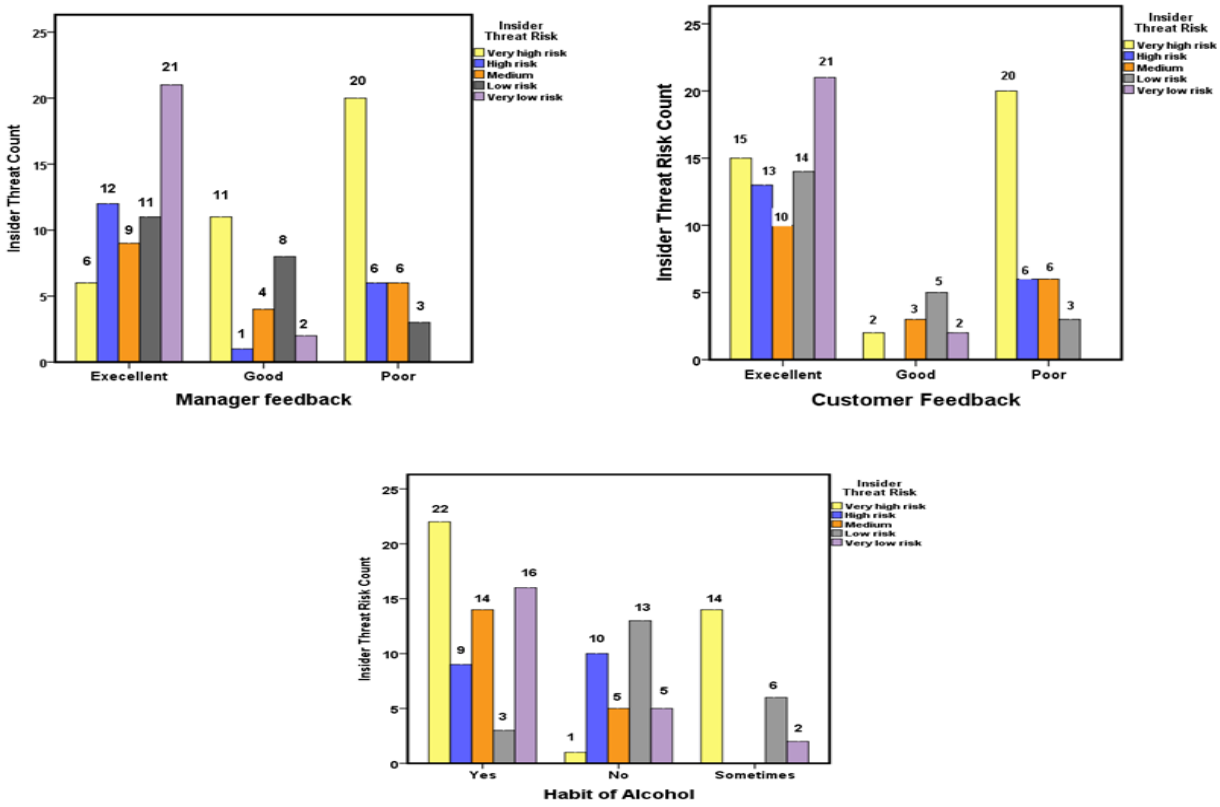


Table 8: Association between insider threat risk and movies interested

		Insider Threat Risk					Total	Chi Square (p value)
		Very high risk	High risk	Medium	Low risk	Very low risk		
Crime/Thriller/ Horror Movies	Rarely	0	2	3	2	11	**18**	**89.297 (0.000)****
	Occasionally	0	0	0	6	0	**6**	
	Once in a month	4	2	8	6	7	**27**	
	Once in a week	6	9	6	2	1	**24**	
	Daily	27	6	2	6	4	**45**	
Science Fiction Movies	Rarely	0	0	3	4	12	**19**	**146.675 (0.000)****
	Occasionally	0	0	0	6	0	**6**	
	Once in a month	4	0	9	6	7	**26**	
	Once in a week	0	13	5	0	0	**18**	
	Daily	33	6	2	6	4	**51**	
Comedy Movies	Rarely	4	5	4	3	5	**21**	22.720 (0.121)
	Occasionally	4	6	3	3	4	**20**	
	Once in a month	13	0	2	3	4	**22**	
	Once in a week	6	7	4	7	4	**28**	

	Daily	10	1	6	6	6	**29**	
Cartoon Movies	Rarely	0	4	4	4	3	**15**	**28.953 (0.024)***
	Occasionally	4	6	1	2	2	**15**	
	Once in a month	11	4	3	5	7	**30**	
	Once in a week	16	2	7	5	2	**32**	
	Daily	6	3	4	6	9	**28**	
Family Type Movies	Rarely	0	5	7	3	3	**18**	**41.307 (0.001)****
	Occasionally	7	6	3	1	7	**24**	
	Once in a month	12	1	2	3	3	**21**	
	Once in a week	6	0	6	5	7	**24**	
	Daily	12	7	1	10	3	**33**	
Total		**37**	**19**	**19**	**22**	**23**	**120**	

**p<0.01, N.S: Not Significant

The relationship between insider threat risk and movie interest is shown in Table 8. There are five interesting movie types. Family Type, Cartoon, Comedy movies, Science fiction and Crime/Thriller/Horror movies. Because the p-values for science fiction films (p<0.01) and crime/thriller/horror films (p<0.01) are less than the 0.05 level of significance. As a result, there is a correlation between the risk of an insider threat and habitual viewers of science fiction and Crime/Thriller/Horror. According to the above indicator, individuals who are interested in science fiction and crime/thriller/horror films are at risk for insider threats**.**The risk could be in terms of having sleeplessness, adrenaline rush, lack of control, negative health and social effects, feelings of guilt, neglect of duties. When it comes to insider threats, many people think of someone who will actively damage the systems. However, this is not always the case. The unpredictable behavior of employees at work may cause an unwelcome disturbance in business due to underlying psychological factors.

Table 9: Association between insider threat risk and Political News Interest

		Insider Threat Risk					**Chi Square (p value)**
		Very high risk	**High risk**	**Medium**	**Low risk**	**Very low risk**	
Political News Interest	Very low Interested	0	3	3	2	11	**138.733 (0.000)****
	Low Interested	0	2	2	8	1	
	Average Interested	5	0	7	6	7	
	High Interested	0	14	5	0	1	
	Very high Interested	27	6	2	6	4	

**p<0.01

The relationship between insider threat risk and political news interest is shown in Table 9. The majority of the 27 respondents were found to be interested in political news. Since the Political News Interest (p<0.01) p value is less than the 0.01 level of significance. Hence, there is a link between the risk of insider threats and political news interest. The accompanying table demonstrates that respondents'

interest in political news increases the risk of insider threats. For instance, A simple conversation at work may turn into a debate and a conflict.

Ordinal Logistic Regression Model

Table 10: Model Fitting Information

Model Fitting Information				
Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	353.208			
Final	211.510	141.698	24	**.000**
Link function: Logit.				

Model Fitting Information is used to test the mode fit. A likelihood ration and chi-square tests are to test whether there is a significant improvement in the fit of the final model relative to the intercept only model. In this case, we see the significant improvement in the fit of the final model over the null model [X^2 (24) = 141.698, p<0.001].

Table 11: Goodness-of-Fit

Goodness-of-Fit			
	Chi-Square	df	Sig.
Pearson	441.385	204	.121
Deviance	199.527	204	.575
Link function: Logit.			

The Goodness-of-Fit table contains the Pearson Chi-Square test and Deviance test, which are useful for determining whether a model exhibits good fit to the data. Non-significant test results are indicators that the model fits the data well [22]. In this case, we see that both the Pearson Chi-Square test [X^2 (204) = 441.385, p=.121] and Deviance test [X^2 (204) = 199.527, p=.575] were both non-significant. These results, suggest that good model fit.

Table 12: Pseudo R-Square

Pseudo R-Square	
Cox and Snell	.693
Nagelkerke	.724
McFadden	.375
Link function: Logit.	

Table 12 reveals the Pseudo R-Square. The Pseudo R-Square values are treated as rough analogues to the R square values in Ordinal Logistic Regression. . The model explained 69% (Cox and Snell R^2) of the variance in Insider Threat Risk and correctly classified 62.6% of cases

Table 13: Prediction for movies and political interested and Insider Threat Risk

Observed		Predicted					
		Very high risk	High risk	Medium	Low risk	Very low risk	Percentage Correct
Insider Threat Risk	Very high risk	33	1	3	0	0	**89.2**
	High risk	6	11	1	1	0	**57.9**
	Medium	3	2	7	7	0	**36.8**
	Low risk	0	0	7	9	6	**40.9**
	Very low risk	1	0	3	4	15	**65.2**
Overall Percentage							**62.5**

Table 13 depicts the classification table for movies and political interested and Insider Threat Risk. Overall, the accuracy rate was very good at **62.5%.** The model exhibits good sensitivity since among those employees who will interest in science fiction and Crime/Thriller/Horror and Political News, 89.2% were correctly predicted to interest in science fiction and Crime/Thriller/Horror and Political News.

Table 14: Impact of movies and political interested on Insider Threat Risk

			Estimate	SE	Wald	df	Sig.	95% Confidence Interval	
								Lower Bound	Upper Bound
Threshold	Insider Threat Risk	Very High Risk	-4.163	.789	27.865	1	**.000****	-5.708	-2.617
		High Risk	-2.494	.732	11.615	1	**.001****	-3.928	-1.060
		Medium	-.783	.665	1.385	1	**.039***	-2.087	.521
		Low Risk	1.179	.660	3.196	1	**.004****	-.114	2.472
Location	Family type Movies	Daily	-2.870	1.016	7.978	1	**.005****	-4.861	-.878
		Once in a week	-.887	.804	1.219	1	.270	-2.463	.688
		Once in a month	-1.924	.810	5.647	1	**.017***	-3.511	-.337
		Occasionally	-.340	.839	.164	1	.686	-1.984	1.305
		Rarely	0[a]	.	.	0	.	.	.
	Cartoons Movies	Daily	-1.959	.968	4.092	1	**.043***	-3.857	-.061
		Once in a week	-3.445	.972	12.571	1	**.000****	-5.349	-1.540
		Once in a month	-1.207	.776	2.420	1	**.020***	-2.729	.314
		Occasionally	-2.984	.824	13.110	1	**.000****	-4.599	-1.369
		Rarely	0[a]	.	.	0	.	.	.
	Comedy Movies	Daily	-2.752	.964	8.150	1	**.004****	-4.642	-.863
		Once in a week	-3.335	.814	16.788	1	**.000****	-4.931	-1.740
		Once in a month	-2.342	.855	7.508	1	**.006****	-4.017	-.667
		Occasionally	-1.141	.690	2.732	1	.098	-2.493	.212
		Rarely	0[a]	.	.	0	.	.	.

	Science Fiction Movies	Daily	26.614	1.322	405.376	1	**.000****	24.023	29.204
		Once in a week	19.662	3.017	42.457	1	**.000****	13.747	25.576
		Once in a month	22.555	2.308	95.477	1	**.000****	18.030	27.079
		Occasionally	22.345	1.302	294.628	1	**.000****	19.793	24.896
		Rarely	0[a]	.	.	0	.	.	.
	Crime/Thriller/ Horror	Daily	-24.819	1.364	330.865	1	**.000****	-27.493	-22.144
		Once in a week	-18.115	2.168	69.787	1	**.000****	-22.364	-13.865
		Once in a month	-21.151	1.607	173.150	1	**.000****	-24.302	-18.001
		Occasionally	-22.792	.000	.	1	**.000****	-22.792	-22.792
		Rarely	0[a]	.	.	0	.	.	.
	Political News Interest	Very high Interested	6.347	1.751	13.136	1	**.000****	2.915	9.779
		High Interested	4.175	1.581	6.972	1	**.008****	1.076	7.274
		Average Interested	2.034	1.388	2.147	1	**.043***	-.687	4.755
		Low Interested	1.532	1.164	1.733	1	.188	-.749	3.813
		Very low Interested	0[a]	.	.	0	.	.	.
Link function: Logit.									
a. This parameter is set to zero because it is redundant.									

p<0.01, *p<0.05

Table 14 reveals the impact of movies and political interested on Insider Threat Risk. The Wald test ("Wald" column) is used to determine statistical significance for each of the independent variables. The statistical significance of the test is found in the "Sig." column. From these results we can see that Science fiction movies interested ($p<0.01$), Crime/Thriller/Horror ($p<0.01$) and Political News Interest ($p<0.05$) added significantly to the model/prediction, but Family type, Cartoons and Comedy movies interested did not add significantly to the model. The model explained 72% (Nagelkerke R^2) of the variance in Insider Threat Risk and correctly classified 62.7% of cases. However, increasing the interested in movies like Science fiction and Crime/Thriller/Horror movies and Political News Interest was associated with an increased in the likelihood of exhibiting Insider Threat Risk.

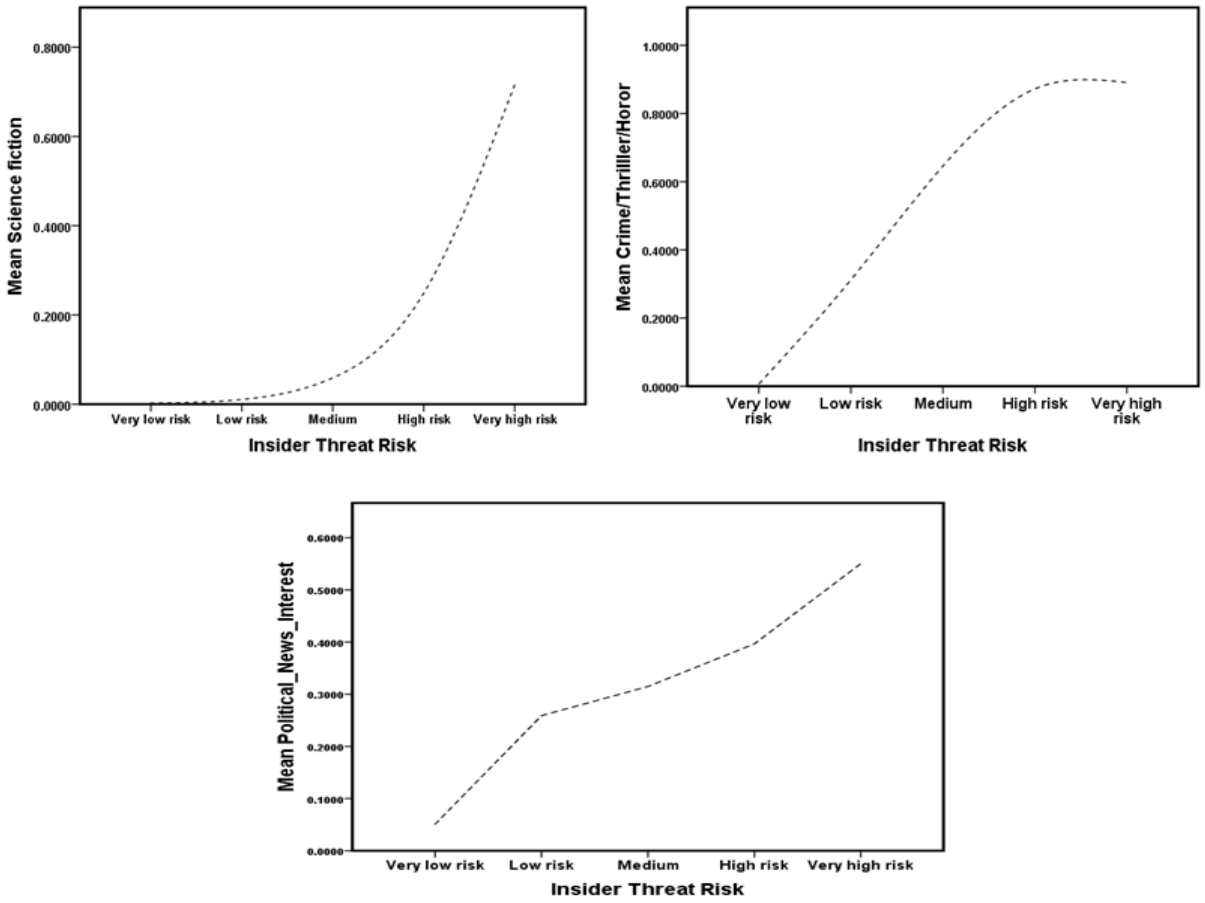
Table 15: Test of Parallel Lines[a]

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothesis	211.510			
General	213.211	211.510	72	.090
The null hypothesis states that the location parameters (slope coefficients) are the same across response categories.				
a. Link function: Logit.				

Table 15 depicts the test when the result of the test of parallel lines, indicates non-significance, then we interpret it to mean that the assumption is correct. Statisticalsignificant is taken as an indicator that the

assumption is not correct. In the results from our analysis, we interpret that the results to mean the assumption is correct (as p=.090).

Figure 2: Impact of movies and political interested on Insider Threat Risk, Probability Prediction



Impact of employees' information on Insider Threat Risk

Table 16: Model Fitting Information

Model Fitting Information				
Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	377.774			
Final	252.430	125.344	31	.000
Link function: Logit.				

Model Fitting Information is used to test the mode fit. A likelihood ration and chi square tests are test whether there is a significant improvement in the fit of the final model relative to the intercept only model. In this case, we see the significant improvement in the fit of the final model over the null model [X^2 (31) = 125.344, p<0.001]

Table 17: Goodness-of-Fit

Goodness-of-Fit			
	Chi-Square	df	Sig.
Pearson	1239.370	253	.323
Deviance	252.430	253	.498
Link function: Logit.			

The Goodness-of-Fit table contains the Pearson Chi-Square test and Deviance test, which are useful for determining whether a model exhibits good fit to the data. Non-significant test results are indicators that the model fits the data well [22]. In this case, we see that both the Pearson Chi-Square test [X^2 (253) = 1239.370, p=.323] and Deviance test [X^2 (253) = 252.430, p=.498] were both non-significant. These results, suggest that good model fit.

Table 18: Pseudo R-Square

Pseudo R-Square	
Cox and Snell	.648
Nagelkerke	.677
McFadden	.332
Link function: Logit.	

Table 18 reveals the Pseudo R-Square. The Pseudo R-Square values are treated as rough analogues to the R square values in Ordinal Logistic Regression. The model explained 65% (Cox and Snell R^2) of the variance in Insider Threat Risk and correctly classified 66.7% of cases

Table 19: Prediction for movies and political interested and Insider Threat Risk

Observed		Predicted					
		Very high risk	**High risk**	**Medium**	**Low risk**	**Very low risk**	**Percentage Correct**
Insider Threat Risk	Very high risk	34	3	0	0	0	**91.9**
	High risk	4	12	3	0	0	**63.2**
	Medium	0	0	9	4	6	**47.4**
	Low risk	1	4	3	5	9	**40.9**
	Very low risk	1	5	1	0	16	**69.6**
Overall Percentage							**66.7**

Table 19 depicts the classification table for movies and political interested and Insider Threat Risk. Overall, the accuracy rate was very good at 66.7%. The model exhibits good sensitivity since among those employees who will have a habit of alcohol and less Performance appraisal rating, 91.9% were correctly predicted to habits of alcohol and less performance appraisal rating.

Table 20: Impact of employees' information on Insider Threat Risk

Parameter Estimates									
			Estimate	SE	Wald	df	Sig.	95% Confidence Interval	
								Lower Bound	Upper Bound
Threshold	Insider Threat Risk	Very High Risk	-0.090	2.102	0.002	1	**0.046***	-4.210	4.030
		High Risk	1.760	2.116	0.692	1	**0.006****	-2.388	5.908
		Medium	3.260	2.122	2.360	1	**0.024***	-0.899	7.420
		Low Risk	4.823	2.137	5.094	1	**0.024***	0.635	9.012
Location	Gender	Male	0.869	0.605	2.064	1	**0.041***	-0.316	2.054
		Female	0[a]			0			
	Age	Less than 25	1.725	0.969	3.167	1	0.075	-0.175	3.624
		26 to 30	2.437	0.773	9.948	1	**0.002****	0.923	3.951
		31 to 35	0.716	0.834	0.738	1	0.390	-0.918	2.350
		36 to 40	-0.133	0.779	0.029	1	0.865	-1.659	1.394
		More than 40	0[a]			0			
	Education	Under Graduate	-0.114	0.716	0.025	1	0.874	-1.516	1.289
		Post Graduate	-0.850	0.743	1.309	1	0.252	-2.306	0.606
		Ph.D.	0.637	0.785	0.659	1	0.417	-0.901	2.174
		Diploma	-0.898	0.863	1.083	1	0.298	-2.588	0.793
		Others	0[a]			0			
	Marital Status	Single	0.076	1.229	0.004	1	0.950	-2.332	2.485
		Married	-1.687	1.348	1.567	1	0.211	-4.329	0.955
		Widow	-1.569	1.654	0.900	1	0.343	-4.810	1.672
		Separated	0[a]			0			
	Employee Band	EB1	-2.412	0.938	6.612	1	**0.010***	-4.251	-0.574
		EB2	-2.074	0.937	4.898	1	**0.027***	-3.910	-0.237
		EB3	-0.417	0.885	0.222	1	0.638	-2.152	1.318
		EB4	-3.039	1.352	5.054	1	0.025	-5.689	-0.390
		EB5	0[a]			0			
	Experience	Less than 1 year	-3.567	2.162	2.721	1	0.099	-7.805	0.671
		1 to 5 years	-2.311	1.375	2.826	1	0.093	-5.005	0.383
		6 to 10 years	-3.308	1.281	6.665	1	**0.010***	-5.820	-0.797
		More than 10 years	0[a]			0			
	Tenure	Less than 1	1.015	2.050	0.245	1	0.621	-3.003	5.032

		year							
		1 to 5 years	-0.402	1.457	0.076	1	0.783	-3.257	2.454
		6 to 10 years	-0.740	1.061	0.486	1	0.486	-2.820	1.341
		More than 10 years	0[a]			0			
Link function: Logit.									
a. This parameter is set to zero because it is redundant.									

p<0.01, *p<0.05

Table 20 reveals the impact of employees' information on Insider Threat Risk. From these results we can see that gender ($p<0.05$), employee band ($p<0.05$) and experience ($p<0.05$) added significantly to the model/prediction, but rest of the variables did not add significantly to the model. The model explained 67% (Nagelkerke R^2) of the variance in Insider Threat Risk and correctly classified 66.7% of cases. However, increasing the gender that are male, employee band (EB1 and EB2) and experience which is 6 to 10 years was associated with an increased in the likelihood of exhibiting Insider Threat Risk.

Table 21: Test of Parallel Lines[a]

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothesis	252.430			
General	251.243	252.430	93	.854
The null hypothesis states that the location parameters (slope coefficients) are the same across response categories.				
a. Link function: Logit.				

Table 21 commonly referred to as the test of parallel lines because the null hypothesis states that the slope coefficients in the model are the same across response categories (and lines of the same slope are parallel). If we were to reject the null hypothesis based on the significance of the Chi-Square statistic, we would conclude that ordered logit coefficients are not equal across the levels of the outcome, and we would fit a less restrictive model (i.e., multinomial logit model). If we fail to reject the null hypothesis, we conclude that the assumption holds. For our model, the proportional odds assumption appears to have held because the significance of our Chi-Square statistic is .854 > .05.

6. Proposed Solution approach based on the statistical inference:

Countering internal threats or malicious insiders can be accomplished by embracing Cyberpsychology best practices through subject matter experts and Cybersecurity practitioners. Cyberpsychology is the study of how new computing technologies—in particular, the Internet—affect how people feel, act, and think both online and offline. When applied to organizational psychology, it can assist businesses in effectively resolving the issue at hand. The most popular and simple to use strategy is the prediction model mentioned above. This document focuses on a technique for gathering the necessary data in a methodical manner from many sources, particularly employee personal information. In light of this, the following strategy has been developed.

1)Each company contains data on its personnel, including information on their age, experience, tenure, location, marital status, performance evaluations, peer and client comments, management feedback, and more.Cyberpsychology practitioners can collaborate with the HR Wellness Counseling Team or employees (through some cutting-edge initiatives) through employee engagement activities and frequently plan individual counseling activities throughout the year. Through these initiatives, they can have the employee's permission to use their personal information for recommending the best potential solutions for them, and the information will remain secure within the company's virtual private networks.

2) With the best interest of the employee's wellbeing in mind, Cyberpsychology practitioners can achieve voluntary submission of personal information such as habits, hobbies, SWOT (strength, weakness, opportunity, threat) self-assessments, medical reports, background verification report, personality traits reports, etc.

3)An insider risk prediction model can be created using the gathered data and the many professional parameters indicated in point number one above.

4)The employee may receive the individual reports in the form of psychometric test results. Of course, some businesses may already be utilizing these tactics, but they may still see a chance to expand them in order to detect hostile insiders as part of the development of a cybersecurity culture.

5)Self-control and healthy habits are the greatest ways to promote harmony and maintain the culture of safety and security so that the expense of cybersecurity services may be invested for greater business purposes.

7. Conclusion

In conclusion, when it comes to insider threats, many people think of someone who will actively damage the systems. However, this is not always the case. The unpredictable behavior of employees at work may cause an unwelcome disturbance in business due to underlying psychological factors.

Insider threat continues to be a significant problem for all types of organizations. This study looked into insider threats and how important it is for businesses to deal with them in order to reduce risk. Insiders have emerged as a significant security concern for all businesses, as insiders can range from low-level workers to high-ranking individuals who have access to and knowledge of sensitive organizational data. In this study, majority of insider threat happened for less or low performance feedback from management, habits of alcohol, Science fiction and Crime/Thriller/Horror movies and Political News Interest was associated with an increased in the likelihood of exhibiting Insider Threat Risk. This does not necessarily be the same case for all organizations. For example, a top performer employee may also feel grumpy when the promotions do not happen timely and can become a potential malicious insider. Authors strongly believe that emotional intelligence, psychometric test-based training recommendations, Cyberpsychology oriented tools and products embedded into the tools that the employee use it on day-to-day basis as part of their business as usual can create a risk-free environment from the malicious insider threat prevention perspective. It is imperative for employee to enroll for a mindfulness session, as was already noted, various insider threats that target various organizational subsystems, such as device level, data level, corporate and business level, must be handled. Future research will concentrate on how human, organizational, and technological elements change through time in order to minimize adversarial responses and produce predictions that are more accurate. On the basis of the forecast result, a decision support system may also be created to offer recommendations for mitigating future dangers. Finally, this

strategy can be made simpler by focusing only on one sort of insider threat prediction in order to make those predictions more accurate, even if the organizations would still be exposed to other insider threat categories. Cybersecurity product development organizations and service providers can transform their products and services into holistic by integrating the Cyberpsychology techniques and methods. This can happen when the organizations realize that Cybersecurity is not just a technical problem but a social problem and the solution lies in consistently understanding the mindset of people involved across the board.The solution approach proposed in this paper can be accomplished by some predictive analytics software tools however, the emphasis should be on the method of capturing the independent variables in a positive way for creating a positive culture of cybersecurity and resiliency through innovative methods of employee engagement.

8. Conflict of Interest

This document does not represent the opinions, products, or information of the author's company or business associates. If there are any parallels, it is simply coincidental, and the authors are not responsible for it.

9. Author's Biography

Jitendranath Palemholds a Master's Degree in Computer Applications from **NIT** (National Institute of Technology) Warangal, India. He has vast experience in Information Technology in the Quality, Statistical Process controland DataAnalytics domains. He is a certifiedLean Six sigma Blackbelt, IBM certified Artificial Intelligence (A.I)skills academy faculty SME, Advisory Data Scientist, Cognitive and Design Thinking practitioner, Microsoft certified Azure AI Fundamental professional. He has been named as an IBM inventor on a regular patent application filed with the U.S. Patent & Trademark Office in the IT services domain.He is a Certified Cyberpsychology practitioner and he has studied a diploma course in Psychology, Advanced diploma in Cyber Laws, Cognitive Behavior therapy. In addition, he is an accredited Professional Life Coach, Certified Mental Health Counselor, and Practitioner.

Sivaprakash Palaniswamy holds a Master's Degree in Computer Applications from **BharathiarUniversity,** Coimbatore**,** India. He brings his 30+ years of professional experience from various industrial sectors including banking, textiles and information technology. He has expertise in information technology services across multiple disciplines, especially in Life Sciences/Healthcare, Banking & Finance and Retail. His IT experience includes leading large-scale migration and transformation programs and also leading large service delivery teams, spread across technical domains such as cybersecurity/GRC, application management/development and infrastructure management. He holds technical certifications such as CISSP, CCSP, ITIL V3 Expert and CobiT 4.1.

10. References

1. Omar, M.Insider Threats: Detecting and Controlling. *In New Threats and Counter measures in Digital Crime and Cyber Terrorism*; IGI Global: Hershey, PA, USA, 2015; p. 162.
2. Barrios, R.M. *A multi-leveled approach to intrusion detection and the insider threat*. J. Inf. Secur. 2013, 4, 54–65.

3. Cost of Insider Threats Global Report, Observer IT. 2020. Available online: *https://www.observeit.com/costof-insider-threats* (accessed on 25 June 2020).
4. Walker-Roberts, S., Hammoudeh, M., Dehghantanha, A., 2018. *A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure*, IEEE Access 6, 25167-25177.
5. Ponemon Institute LLC, 2020, Cost of Insider Threats: Global Sponsored by ObserveIT. Technical Report. Available online: https://www.ibm.com/downloads/cas/LQZ4RONE.
6. Mills, J.U., Stuban, S.M., Dever, J., 2017. Predict Insider Threats Using Human Behaviors. IEEE Engineering Management Review 45, 39–48.
7. Cappelli, D., Moore, A.P., Trzeciak, R., 2012. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. Addison-Wesley Professional. 1st edition.
8. Walker-Roberts, S., Hammoudeh, M., Dehghantanha, A., 2018. *A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure*, IEEE Access 6, 25167-25177.
9. Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., Rogers, S., 2005. Insider Threat Study: Computer System Sabotage in Critical Infrastructure. Technical Report May.
10. 10. Zeadally, S., Yu, B., Jeong, D.H., Liang, L., 2012. Detecting insider threats solutions and trends. Information Security Journal 21, 183–192.
11. 11. J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in Proc. of the 2014 IEEE Security and Privacy Workshops (SPW'14), San Jose, California, USA. IEEE, May 2014, pp. 214–228.
12. M. R. Randazzo, M. Keeney, E. Kowalski, D. M. Cappelli, and A. P. Moore, "Insider threat study: Illicit cyber activity in the banking and finance sector," Tech. Rep., June 2005.
13. M. B. Salem, S. Hershkop, and S. J. Stolfo, A survey of insider attack detection research. Springer US, August 2008
14. J. Wang, Y. Zhang, C. Posse, and A. Bhasin, "Is it time for a career switch?" in Proc. of the 22nd international conference on World Wide Web (WWW'13), Rio de Janeiro, Brazil. ACM, May 2013, pp. 1377–1388.
15. Stoneff, C. (2017, April 25). Insider threats or external cyber-attacks: which is worse? Retrieved from https://www.identityweek.com/insider-threats-or-external-cyber-attacks/
16. SANS 2017 Insider Threat Survey, Available online: https://www.sans.org/webcasts/2017-insider-threat-survey-mounting-effective-defense-insider-threat-103917/
17. Cole, E. (2017, August). Defending against the wrong enemy: 2017 SANS Insider Threat Survey. Retrieved from https://www.sans.org/readingroom/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890
18. Pekka Tetri & Jukka Vuorinen (2013) Dissecting social engineering, Behaviour & Information Technology, 32:10, 1014-1023.
19. Cialdini, R. B. (2008). Turning persuasion from an art into a science. In P. Meusburger, M. Welker, & E. Wunder (Eds.), *Clashes of knowledge: Orthodoxies and heterodoxies in science and religion* (pp. 199–209).
20. McAlaney, J., Thackray, H. and Taylor, J. (2016). The social psychology of cybersecurity. *The Psychologist*, 29(9), 686-689.

21. Fullwood C. (2015) The role of personality in online selfpresentation. In Attrill A, ed. Cyberpsychology . Oxford: Oxford University Press, pp. 9–28.
22. Filed 2018 and petrucci 2009, Goodness of fit. Retrieved from https://www.researchgate.net/publication/232855786_A_Primer_for_Social_Worker_Researchers_on_How_to_Conduct_a_Multinomial_Logistic_Regression