Modeling User Behaviour in Response to Cyberthreats.

Caldwell, Anthony[1], McGarvey, John[2]

Department of Computing

Letterkenny Institute of Technology, (LYIT), Letterkenny, Co. Donegal

E-Mail: [1]mr.anthony.caldwell@gmail.com [2] John.McGarvey@lyit.ie.

Abstract - Considerable challenges exist for the average computer user, organizations and indeed governmental agencies with the advent and evolution of threats directed against the computer user today. Combating cyberthreats has not only become a highly politicized issue but also a lucrative one as is evidenced from the growth in information security workforce. In conjunction with the nebulous existence of threats there is also an implied sense of calculability, even predictability, as often proclaimed by many security industry experts and academics. The end user must still make an independent decision on whether to react to these threats or not. To attempt to understand end user motivations when faced with threats, attitude-behaviour models are sometimes used. The theory of planned behaviour has been adapted to understand the impact of factors which may trigger behaviours in end users to deal with a cyberthreat. The model suggests that end users' intentions are not significantly mediated by their attitudes, perceived abilities to prevent threats or perceptions of their peer group.

I. INTRODUCTION.

Early research noted the importance of trust which was associated with lower perceived risk in some models but also strongly affected by the consumers' perceptions of the size and reputation of the online retailer **[1,2]**. While trust is important, of equal importance is the security of data during transmission and reception via the implementation of strong cryptographic algorithms **[3,4,5]**. Increasingly, end users are faced with the problem of securing their data on a myriad of hardware, software and cloud platforms with the result that the data itself needs to be secure while static, prior to transmission, to prevent malware being distributed. This paper focuses on how users perceive threats to this data and if they consider the safety of their data in response to cyberthreats. This is important because attacks on the end user as a result of viruses/malware show no signs of decreasing **[6,7,8,9,10,11]**. Consumer trust may be conceptualized by honesty, benevolence, and competence and in general, has a strong impact on the perception of fear. Importantly, reductions in trust can increase anxiety and fear **[12,13]**. Early research suggested that 49% of the types of security incidents experienced by end users were perpetrated by viruses **[14]** with attacks from worms and viruses listed among the top five issues in security surveys in this period **[15]**. Often in the case of information security, any suggestions about a new cyberthreat are supported by constructive steps (typically from the reporter) to avert the new threat and emphasize value of accepting this advice. For example, as an end user's perception of the severity of a new virus, malware, denial of service threat increases, beliefs regarding the capabilities of anti-spyware software to adequately address the threat may decline **[16,17]**. In attempting to map users' intentions when exposed to signs that a threat is imminent, attitude-behavior models may be of some value. In general, these models are chosen because of their relative ability to predict behaviour, their simplicity of design and the ease of with which their parameters can be translated into testable quantities **[18]**. Among the most often used are the theory of reasoned action **[19,20,21]** and theory of planned behavior **[22]** which are frequently adapted to purpose. Given that this paper uses attitude-behaviour models as a basis it is worthwhile to consider their background.

II. THEORY OF REASONED ACTION.

Between 1975 and 1980 the theory of reasoned action (TRA) (see Fig 1) originated and developed from social psychology literature **[19]**. The theory proposed that a significant predictor of behavior is the intention to behave. This intention is determined by attitudes toward the target behavior and some perceived subjective norms. Significantly, the theory also states that both attitudes and subjective norms are a function of beliefs **[17]**. Attitude is described as the evaluation of a behavior as good or bad and subjective norm refers to the actor's perceptions about how they ought to behave **[18,19]**.

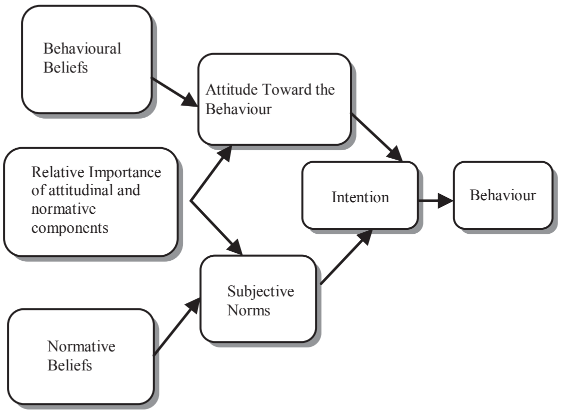
Behavioural Beliefs
Attitude Toward the Behaviour
Relative Importance of attitudinal and normative components
Intention
Behaviour
Subjective Norms
Normative Beliefs

Fig 1: The Theory of Reasoned Action.

III. THEORY OF PLANNED BEHAVIOUR.

Evolving from the theory of reasoned action, the theory of planned behavior (TPB) (see Fig 2) includes factors that relate to attitudes and the ability to predict behaviours in the presence of certain attitudes. In general, the greater the intention to engage in a behaviour, the more likely it is to be performed **[20]**. The TRA states that two major factors influence intention: attitudes towards the behaviour and subjective norms or perceived social pressure. TPB adds to the TRA by including perceived behavioral control as an additional factor referring to the perceived ease or difficulty of carrying out the target behaviour. In simple terms, TPB suggests that an individual will probably engage in a behaviour based on their intentions. This intention to engage is influenced by variable beliefs (positive and negative) about the behavior described as attitudes, the perception of social pressure to perform the behaviour (subjective norms) and perceived ability to perform the behavior (perceived behavioural control).

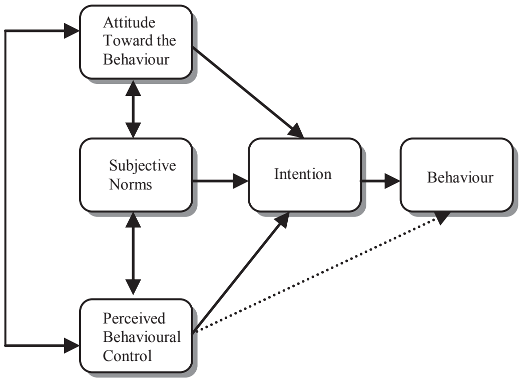

Fig 2: The Theory of Planned Behaviour.

The existing body of research typically modifies antecedents of the TPB and uses this as a theoretical framework. These models can be adapted to describe behavior, particularly in education **[23,24,25]**. Both the TRA and TPB models have been the basis of numerous studies and there is much evidence to suggest that there is significant support for the proposed relationships and factors in both models. Understanding threat perception is an important factor when it comes to predicting motivation to adopt a new software product, patch or engage with a new information system entirely. End user security is a challenging area and deserves some attention.

IV. LITERATURE REVIEW.

Security is a challenging area when we consider the end users' wide variance in threat awareness, intention towards dealing with threats and the skills needed to control these threats **[16]**. Accordingly, there are many theories and models which seek to understand how and why individuals change. In particular, research seems to suggest that theories which examine the causal linkages between attitude-behavior demonstrate significant predictive power **[2]**. As regards the perception of threats as applied to security management, Siponen (2000) recommends the use of persuasion which may provoke an emotional response and as a result may affect user attitudes and motivations **[26]**. However, much research and indeed life experience would indicate that while direct threats may be effective, fear appeals may be equally convincing. According to Williams (2012) fear appeals are characterized by factors such as fear, threat and perceived efficacy and as noted by Johnston and Warkentin (2010), 'a fear appeal is a persuasive message with the intent to motivate individuals to comply with a recommended course of action through the arousal of fear associated with a threat'**[16, 17]**. Industrial and academic reports are replete with warnings, threats and recommended actions to deal with their dire predictions **[27, 28]**. The TRA and TPB may be of some value in this respect when used in the analysis of end user behavior when dealing with knowledge of cyber threats i.e. from malware, spyware, viruses, social engineering etc. Research supports the use of adaptations of the TRA and TPB models to investigate attitudes towards information systems where both attitude and subjective norms are significant predictors of behavioural intention [**23, 25**]. The behavioural models discussed here simply offer an insight into how best to isolate some factors which may potentially improve the end user experience by understanding how the perception of threats may affect their decisions. As noted by Pintrich (2003), the integration of intentional and self-regulatory processes may augment models aimed at predicting and understanding motivation **[29]**. Since attitudes have an affect upon intentions in the TPB it is reasonable to posit that if the user's perception of threat is low risk, then it is at least conceivable that their attitude towards the download/webpage/antivirus update will be positive. Perceptions of peer group (subjective norms) upon the user are also those positive or negative opinions or attitudes that may be formed as a collective which may impact on a user's motivation towards using the system. In simple terms, subjective norms are important because users can be strongly influenced by encouragement from important peers **[30,31]**. The use of fear appeals is common in many types of marketing communications and is an effective motivator. If the perceptions of a peer group is that anti-virus product X is good at preventing most computer viruses, then there is a reasonable chance that an individual member or the peer groups will also form the same opinion. Similarly, if the antivirus product also recommends that the user upgrade their product to enhance its capabilities, using fear appeals may also be just as effective. The proposed theoretical framework models user behaviour in response to cyberthreats. A review of the literature seems to suggest several features such as, the user's attitude towards the cyberthreat, the perceptions of the users peer group about the cyberthreat and the user's perception of self-efficacy to deal with the cyberthreat.

V. RESEARCH METHOD.

The TPB model may be used as a framework to understand users' fears in relation to cyberthreats such as viruses. The hypothesized structural model for the study consists of three exogenous variables (attitudes towards cyberthreat, perceptions of peer group (subjective norms) and perceived ability to prevent threat (perceived behavior control) and two endogenous variables (intention and behavior). Intention is hypothesized to act as a mediator between all relationships of exogenous variables and behavior (see Fig 3).

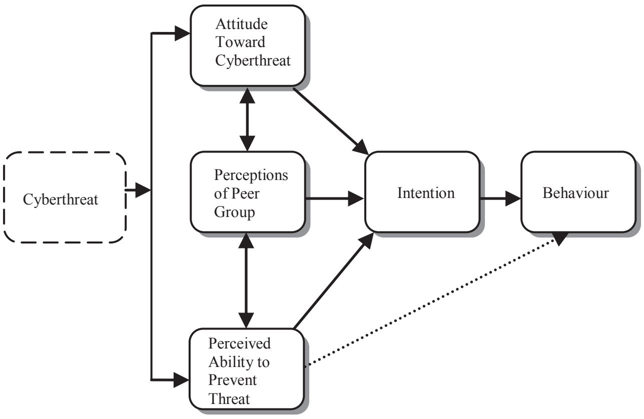
Attitude Toward Cyberthreat
Cyberthreat
Perceptions of Peer Group
Intention
Behaviour
Perceived Ability to Prevent Threat

Fig 3: Proposed model of understanding user behavior in response to cyberthreats.

We propose the following hypotheses to check within the analysis.

Table 1. Hypotheses for the proposed model.

Hypothesis	**Relationship**
H1	Attitude toward the behavior is positively related to intention.
H2	Perceptions of peer group is positively related to intention.
H3	Perceived ability to prevent threat is positively related to intention.
H4	Intention is positively related to behavior
H5	Intention mediates the relationship between attitude toward the behavior and behavior.
H6	Intention mediates the relationship between perceptions of peer group and behavior.
H7	Intention mediates the relationship between perceived ability to prevent threat and behavior.

VI. RESULTS AND ANALYSIS.

During the period 23/07/2012 until 23/11/2012, a non-probability convenience sample of 121 respondents was drawn from third-level college students in Co. Donegal and some members of the general public. Scientific generalizations about the total population cannot be made from this sample because of its unrepresentative nature however the sample allowed the collection of basic data regarding the relationships proposed in this study. The demographic profile of the sample is shown in table 2.

Table 2. Demographic profile of respondents in study.

Answer Options	Response Percent	Response Count
Male	74.2%	89
Female	25.8%	31
Did not attend school	3.3%	4
Graduated from secondary school	74.2%	89
Graduated from college	15%	18
Post Graduate	7.5%	9

The questionnaire demonstrated adequate reliability at 0.72 ($p < 0.000$). The confirmatory factor analysis results in table 3, demonstrated that the factor loadings of all observed variables or items was adequate, ranging from 0.50 to 0.82 except PPG4 which did not load onto any factor. The factor loadings (or regression estimates) of latent to observed variable should be above 0.50 which would indicate that the constructs conform to construct validity requirements. The remaining numbers of items for each construct are as follows: Attitude (7 items), perceptions of peer group (5 items), perceived ability to prevent threat (8 items), intention (2 items), and behaviour (1 item).

Table 3. Regression weights of each item onto its latent variable.

Factor	Code	Attributes	Factor Loadings
Factor 1: Attitude (7 items).	ATT 1	Alerts from my antivirus program make me feel uncomfortable.	0.670
	ATT 2	Media reports about new computers viruses make me feel uncomfortable about my computer safety.	0.757
	ATT 3	If my friends/colleagues get a virus on their computer I feel worried.	0.709
	ATT 4	Updating my antivirus software makes me feel more secure.	0.750
	ATT 5	If my antivirus software is out of date, I feel worried.	0.775
	ATT 6	Updating my antivirus software makes me feel protected.	0.706
	ATT 7	Computer viruses are dangerous to me.	0.545
Factor 2: Perceptions of peer group (5 items).	PPG 1	My friends do regular updates of their antivirus program when they are requested.	0.825
	PPG 2	My friends recommend that my antivirus software should be updated to prevent viruses.	0.804
	PPG 3	When I'm uncertain of what to do about a new virus, I look to my friends/colleagues.	0.506
	PPG 4	My friends/colleagues think that computer viruses are dangerous.	0.000
	PPG 5	When I'm uncertain of what to do about a new virus, I look to the antivirus company website.	0.736
Factor 3: Perceived ability to prevent threat (8 items).	PAPT 1	I am able to update the anti-virus program when required.	0.655
	PAPT 2	If my computer had a virus I'd know what action to take.	0.535
	PAPT 3	I am confident that if I update my antivirus software I won't get a virus.	0.716
	PAPT 4	It is easy to prevent against computer viruses.	0.775
	PAPT 5	Getting a computer virus is out of my control.	0.816
	PAPT 6	I have previously updated my antivirus software when I get an alert to do so.	0.644
	PAPT 7	I have dealt with viruses successfully in	0.671

	PAPT 8	the past. I have dealt with antivirus software update alerts successfully in the past.	0.727
Factor 4: Intention (2 items)	INT 1	I intend to regularly update the anti-virus program on my computer.	0.707
	INT 2	I intend to read my company/institutional security policy when it is updated.	0.754
Factor 5: Behaviour (1 item).	B1	I will update the anti-virus program on my computer whenever an alert pops up.	0.607
TOTAL		**23 items**	

Measurement and structural models with latent and observed variables were built with AMOS 5.0 using questionnaire items with high factor loading. The final model is shown in Fig. 4. Ellipses represent unobserved latent variables, squares (or rectangles) represent observed variables. Single arrows represent the impact of one variable (linear dependency) on another while curved arrows represent a covariance between variables. Items marked e1 to e10 enclosed in a circle indicate measurement error. The numeric values attached to single-arrows are an estimate of standardized regression weight (standardized maximum likelihood parameter) indicating the strength of the path. The estimates of standardized regression weight from errors to variables (e1 to e10) have been removed from the path diagram so that the relationship among variables is clearer.

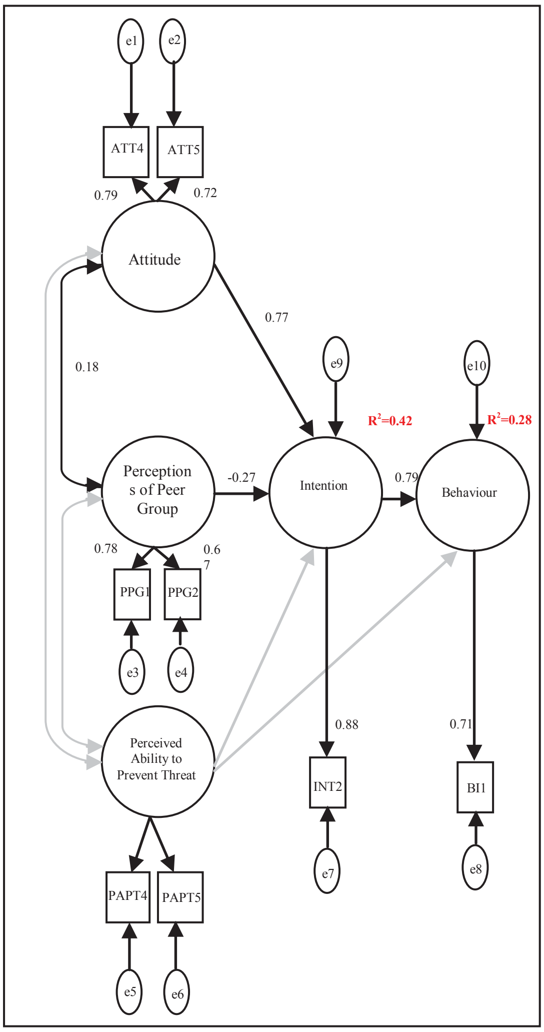

Fig 4: Structural model of users intentions to deal with cyberthreats.

The goodness of fit indices such as Goodness of Fit Index (GFI) of > 0.9 demonstrate a good model fit with the data based on assessment criteria such as GFI as shown in table 4 below. The R^2 which explains variance in a variable was 0.28 for behaviour and 0.42 for intention. Consequently, the three hypothesized direct effects of, H1: attitude to intention, H2: perceptions of peer group to intention; and H3: perceived ability to prevent threat to behavior are not significant.

Table 4. Goodness of Fit indices.

Model	**RMR**	**GFI**	**AGFI**	**PGFI**
Default model	.063	.931	.846	.414
Saturated model	.000	1.000		
Independence model	.169	.691	.603	.538

The indirect effect estimates for all three hypotheses were small and insignificant implying the absence of mediating effects of intention on these three relationships. In other words, the direct effects from the three variables (attitudes, perceptions of peer group and perceived ability to prevent threat) to behaviour were higher or more significant compared to indirect effects. Thus, H5, H6 and H7 were rejected.

Table 5. Intermediate effects of Intention upon Behaviour from Attitude, Perceptions of Peer Group and Perceived Ability to Prevent Threat.

Path	**Indirect effect**	**Effect**
Attitude→Intention →Behaviour	0.77*0.42=0.323	No mediating effect.
Perceptions of Peer Group→Intention →Behaviour	-0.27*0.42=-0.113	No mediating effect.
Percieved Ability to Prevent Threat→Intention →Behaviour	0.0*0.42=0.00	No mediating effect.

VII. CONCLUSION.

According to SophosLabs more than 30,000 websites are infected every day and 80% of those infected sites are legitimate **[11]**. 85% of all malware, including viruses, worms, spyware, adware and Trojans, comes from the web and 403 million unique variants of malware were identified by Symantec in 2011 versus 286 million in 2010 **[32,33]**. Perhaps the average end user is not aware of the scale and ease with which a virus can be transmitted or the potential damage that the virus can do. Worryingly, a recent report from Imperva revealed that antivirus initial detection rate of a newly created virus is less than 5% **[8]**. Reliance upon antivirus programs, while laudable, is a risk and change is required to educate users on the threat landscape. The findings presented here suggest that there is a lack of concern among end users regarding viruses. The data also suggest that perceived ability to prevent threat has no significant effect upon intentions to deal with a computer virus or the actual behavioral response. This may be supported by some evidence which suggests that as an end user's perception of the severity of a cyberthreat increases, beliefs regarding the capabilities of anti-spyware software to adequately address the threat decline **[16,17]**. This may lead to a lack of 'intention' on the part of the end user to accept updates from antivirus alerts or react to media reports on new virus alerts. Perhaps, computer viruses are not perceived as 'real' viruses and as such can do less harm that the biological variety but this depends upon the definition of 'harm'. The intention to deal with computer viruses is not simple to define nor does this proposed study suggest that these are the only factors by which it may be described. This paper suggests that the factors mediating intention such as attitude, subjective norms and perceived behavioural control may be a step towards further theoretical development. A study of the model in diverse settings will add empirical reliability and validity to the model. Sommer and Brown's (2012) cybersecurity study which showed an incremental improvement in the understanding about threat perception is valuable to many organizations and institutions if properly directed and may develop into significant gains for consumer and supplier over time. Antivirus software revenue streams benefit from new widely hyped viruses by the mass media **[9,10]**. The data in this study suggest that end user self-efficacy in dealing with such threats is high given the high level of confidence reported in dealing with updates to antivirus software.

ACKNOWLEDGEMENTS.

With grateful thanks to the Letterkenny Institute of Technology for their support in carrying out this research.

REFERENCES.

[1] Jarvenpaa, S., J., Tractinsky, N., Vitale, M., 'Consumer Trust in an Internet Store', Information Technology and Management, 1, 2000, pp. 45-71.

[2] Doney, P., M., Cannon, J., P., 'An Examination of the Nature of Trust in Buyer Seller Relationships', Journal of Marketing, 61, 1997, pp. 35-51.

[3] Baldwin., B., Byrne, A., Lu, L., Hamilton, M., Hanley, N., O'Neill, M., Marnane, W., P., 'A Hardware Wrapper for the SHA-3 Hash Algorithms', Proceedings of ISSC 2010, UCC.

[4] Blackledge, J., 'Information Hiding using Stochastic Diffusion for the Covert Transmission of Encrypted Images', Proceeding of ISSC 2010, UCC, pp 463-468.

[5] Baldwin., B., Byrne, A., Lu, L., Hamilton, M., Hanley, N., O'Neill, M., Marnane, W., P., 'A Hardware Wrapper for the SHA-3 Hash Algorithms', Proceedings of ISSC 2010, UCC.

[6] Minei, E., Matusitz, J., 'Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis', Journal of Human Behavior in the Social Environment, Volume 21, Issue 8, 2011.

[7] McAfee, '2012 Threat Predictions', available at http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf , retrieved 04/17/2012.

[8] Imperva, 'Assessing the Effectiveness of Antivirus Solutions', available at

http://www.imperva.com/download.asp?id=324 , retrieved 02/01/2013.

[9] Sommer, P., Brown, I., 'Reducing Systemic Cybersecurity Risk', 2011, available at http://www.oecd.org/dataoecd/57/44/46889922.pdf, retrieved 04/17/2012.

[10] Wahshat, Khalil and Al Smadi, 'Computer Virus, Study Survey', International Journal of Computer Science and Network Security, Vol.7 No.4, April 2007, pp.308-310.

[11] Sophos, 'Security Threat Report 2012', available at http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf , retrieved 23/02/2012.

[12] Flavián, C., Guinalíu, M., Gurrea, R., 'The role played by perceived usability, satisfaction and consumer trust on website loyalty', Information and Management 43, 2006, pp.1-14.

[13] Minei, E., Matusitz, J., 'Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis', Journal of Human Behavior in the Social Environment, Volume 21, Issue 8, 2011.

[14] McAfee, '2012 Threat Predictions', available at http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf , retrieved 04/17/2012.

[15] Dlamini, M., T., Eloff, J., H., P., Eloff, M., M., 'Information security: The moving target', Computers & Security, 2, 8, 2009, pp.189-198.

[16] Johnston, A., C., Warkentin, M., 'Fear Appeals And Information Security Behaviors: An Empirical Study', MIS Quarterly Vol. 34 No. 3, 2010, pp. 549-566.

[17] Williams, K., 'Fear Appeal Theory', Research in Business and Economics Journal, Vol. 5, 2012, available at http://www.aabri.com/manuscripts/11907.pdf, retrieved 05/10/2012.

[18] Zint, M., 'Comparing Three Attitude-Behavior Theories for Predicting Science Teachers' Intentions', Journal of Research in Science Teachin, Vol. 39, No. 9, 2002, pp. 819–844.

[19] Fishbein, M., Ajzen, I., 'Belief, attitude, intention and behavior: An introduction to theory and research.', Reading, MA: Addison-Wesley, 1975.

[20] Ajzen, I., 'The Theory of Planned Behavior',Organizational Behavior and Human Decision Processes 50, 1991, pp. 179-211.

[21] Fishbein, M., Ajzen, I., 'Attitudes and voting behavior: An application of the theory of reasoned action.' In G. M. Stephenson & J. M. Davis (Eds.), Progress in Applied Social Psychology (Vol. I, pp. 253—3 13). London: Wiley.

[22] Ajzen, I., Fishbein, M. 'Understanding attitudes and predicting social behaviour.', Englewood Cliffs, NJ: Prentice-Hall, 1980.

[23] Chen, T., Y., Chen., T., J., 'Examination of attitudes towards teaching online courses based on theory of reasoned action of university faculty in Taiwan',British Journal of Educational Technology, Vol 37, No 5, 2006, pp.683–693.

[24] Archer,R., Elder, W., Hustedde, C., Milam, A., Joyce, J., 'The theory of planned behaviour in medical education:a model for integrating professionalism training', Medical Education, 42, 2008, pp.771–777.

[25] Yu,T., K., Yu, T., Y., 'Modelling the factors that affect individuals' utilization of online learning systems: An empirical study combining the task technology fit model with the theory of planned behaviour', British Journal of Educational Technology, Vol 41, No 6, 2010, pp.1003–1017.

[26] Siponen, M., T., 'A Conceptual Foundation for Organizational Information Security Awareness,' Information Management and Computer Security, 8, 1, 2000, pp. 31-41.

[27] M86, 'M86 Security Labs: Threat Predictions 2012', available at http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_predictions_2012.pdf , retreived 03/29/2012.

[28] McAfee, '2012 Threat Predictions', available at http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf , retrieved 04/17/2012.

[29] Pintrich, P., R., 'A motivational science perspective on the role of student motivation in learning and teaching contexts.' Journal of Educational Psychology, 95, 2003, pp. 667-686.

[30] Stake, J.E., Mares, K.R. 'Science enrichment programs for gifted high school girls and boys: Predictors of program impact on science confidence and motivation', Journal of Research in Science Teaching, 38(10), 2001, pp.1065-1088.

[31] Ajzen, I., Madden, T., J., 'Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control', Journal of Experimental Social Psychology, Volume 22, Issue 5, September 1986, pp. 453–474.

[32] Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011, available at http://www.ponemon.org/library/2011-second-annual-cost-of-cyber-crime-study-benchmark-study-of-u-s-companies, retrieved 20/12/2012.

[33] Symantec, 'Internet Security Threat Report', Vol. 17, 2011 available at http://www.symanteccloud.com/globalthreats/overview/r_mli_reports, retrieved 10/12/2012.