# Affective responses to information security threats – The role of threat context and influence on perceived severity

### Research-in-progress

**Nik Thompson**
School of Management and Marketing
Curtin University
Kent St, Bentley, 6102, WA, Australia
Email: nik.thompson@curtin.edu.au

**Michael Oldfield**
Principal Mining Systems Operations
BHP
125 St Georges Terrace Perth, 6000, WA, Australia
Email: michael.oldfield@bhp.com

## Abstract

Evidence from organizational studies in employee behaviour and risk perception demonstrates the role of affective states in key areas of work performance. Yet this remains largely un-researched in the context of information security. We address this gap through an empirical study of affective responses to different information security threats, and the associated threat appraisals. Our results show that the pattern of affective responses is significantly different across different threat scenarios, and that concern is consistently the strongest reported affective response. Next, we demonstrate that these negative affective states have a significant influence on threat perceptions and can thus be expected to influence behaviour through this established pathway. Later stages of this research will collect a larger data set to test an integrated model of affect and information security behaviour.

**Keywords** information security, affective state, emotion-focused coping, policy compliance, cybersecurity.

# 1 Introduction

Despite vast strides in the IT security industry, cyber security attacks are on a steady upward trajectory. Organizational ICT infrastructure is a digital battleground, requiring foresight, agility, and strategy to ensure business continuity when faced with a wide array of attacks. In this complex and challenging environment, the well-established instrument of policy remains one of the critical tools relied on in enterprise ICT. It is easily understood, has strong parallels to other legal and societal rule structures, and is ubiquitous in modern enterprise. Yet compliance remains an enduring issue that has attracted much interest from researchers (e.g. AlGhamdi, Win, & Vlahu-Gjorgievska, 2020).

Prior work has revealed the inherent limitations in the traditional approach of implementing technology-based solutions accompanied by threats of discipline to encourage security policy compliance (Doherty & Fulford, 2005; Sommestad, Karlzén, & Hallberg, 2015). At the same time, behavioural studies reveal that human affective states are associated with risk-taking behaviour and ultimately possess the potential to directly impact compliance-related activities (D'Arcy & Lowry, 2019).

Safety behaviours more generally are influenced by emotional appeals (i.e. communicating positive or negative affect) (Yuen, Li, Ma, & Wang, 2020). Similarly, behavioural information security research has often considered negative affect-laden communications (generally as fear appeals) as a mechanism to motivate secure behaviours (e.g. Johnston & Warkentin, 2010). More recent work has demonstrated that this negative affective state significantly influences security behaviour, while also reducing the extent to which individuals undertake emotion-focussed coping such as threat devaluation (Thompson, McGill, & Narula, 2024). However, these studies have not considered patterns of the affective states evoked by the threat itself. This is a promising, yet under-researched area of behavioural information security.

The central goal of this research in progress is thus to explore and understand the range of affective states experienced by end users in response to security threats, and to link these with both the threat context and the broader implications in motivating secure behaviour.

# 2 Background and Theoretical Foundations

## 2.1 Affective States and Risk Perception

Affect is a psycho-physiological construct impacting mental and physical processes, and is more commonly described as the feelings, moods, or emotions which may be experienced by an individual. Affect is widely considered to vary along dimensions of valence (positive-negative), arousal (intensity), and motivation (Harmon-Jones, Gable, & Price, 2013). Studies in psychology and neuroscience have indicated that affective states can influence an individual's behaviour, decision-making, and interaction with others (Gonzalez-Ibanez, 2013). A large corpus of experimental research over several decades has led to a much greater understanding of how affective states influence behaviour (Forgas, Chan, & Laham, 2001).

Incorporating individual emotion processes within an organizational framework may provide a holistic view and enable decision-makers to better secure the operating environment (Baskerville, Hee Park, & Kim, 2014). As behavioural information security research is dominated by cognitive models, the integration of affective states represents a different perspective requiring new approaches and techniques. The importance of affective components in an organizational environment has been highlighted by management scholars due to their known impact on job performance and decision-making (Sigal & Donald, 2007).

Furthermore, affect can cause risk perception to temporarily fluctuate and be systematically influenced by elements that are not linked to anticipated payoffs and rewards (Sjöberg, 2007; Treffers, Koellinger, & Picot, 2016). This challenges the traditional theory that a specific individual's risk preference is stable over time across specific events. (Treffers et al., 2016). It is also relevant given that the vast majority of research models employed in behavioural information security research assume that some form of cost/benefit or risk/reward mechanism is employed in security risk judgements.

Affective states experienced by an individual may be considered as either dispositional (trait affect) or situational (state affect) (Watson, Clark, & Tellegen, 1988). Though these dimensions are correlated, it is not possible to explain an individual's immediate response to a situation in terms of trait alone (Eid & Diener, 1999). State affective responses, or emotions, are experienced in reaction to a specific cause and will diminish over time (Frijda, 1986). In keeping with this definition, it is anticipated that evocative stimuli, such as perceived information security threats, will lead to a state affect response. Thus, it is the state affect that is under investigation in this research.

## 2.2 Protection Motivation Theory

Protection Motivation Theory, developed by Rogers (1975), provides a framework that can explain the factors that influence a person's behaviours in response to a perceived threat. This theory has been widely adopted in the information security field, notably through the use of fear appeals to motivate secure behaviour. Protection Motivation Theory suggests that the response and actions of an individual are predominantly defined by the appraisals of the threat and the available coping mechanisms. Threat Appraisal is focused on the severity and vulnerability of the risk. Severity refers to the extent of damage which results from the behaviour. Vulnerability refers to the likelihood that the behaviour will result in a negative impact. Coping Appraisal is concerned with the efficacy and costs associated with responding to the threat.

Policy compliance and its associated challenges have been explained in an organizational context through the lens of Protection Motivation Theory (e.g. Ifinedo, 2012; Vance, Siponen, & Pahnila, 2012). Thus, this provides a well-established framework within which the novel dimension of affect can be introduced and studied. Whereas most studies on compliance assume that user behaviours are stable over time, this fails to explain incidents where users' behaviour differs from trends or expectations. A holistic approach considering both cognitive and affective factors can explain these differences (D'Arcy & Lowry, 2019). This perspective is grounded in research on rational choice, which holds that any behaviour is both cognitive and affective as cognitive processing cannot take place independently of affective factors (Slovic, Finucane, Peters, & MacGregor, 2013).

Ormond, Warkentin, and Crossler (2019) evaluated the role of affective absorption and flow in the context of information security policy compliance. Their empirical findings revealed that respondents who were frustrated by work-related tasks were less likely to comply with information security policy. In broader organizational studies Spector and Fox (2002) found that a wide range of emotions such as anxiety, boredom, and depression also increase counterproductive work behaviour. These findings widen the risk scope by demonstrating that a range of emotions, and not just those which are considered strongly negative (e.g. anger) are potential drivers of information security behaviour.

Building on this prior work on the affective drivers of individual behaviour, and its relevance to the information security context, we make two propositions to guide our exploratory research:

**Proposition 1:** *Security threats will elicit a range of affective responses, and these responses may differ based on the context of the threat.*

**Proposition 2:** *Affective responses contribute to threat appraisal processes through an influence on perceptions of threat severity.*

# 3 Methodology

An online survey was developed to measure the threat and coping appraisal constructs from Protection Motivation Theory, affective responses, and demographic details. Items from previously validated scales were used for all reflective constructs. Threat and coping appraisals were measured on 5-point Likert scales ranging from Strongly Disagree to Strongly Agree, using items developed by Ifinedo (2012). Affective responses were measured through an adaptation of the Positive and Negative Affect Schedule (PANAS) scale developed by Watson et al. (1988) which is commonly employed to rate participants positive and negative affective states. As the emotional responses to threats are negative, we focussed on these emotional responses in our survey, following the approach of Sjöberg (2007).

Two corporate information security-related scenarios were developed for this study. The first scenario describes an information security attack that targets a piece of industrial machinery resulting in a health and safety incident, whereas the second scenario describes an attack that results in a breach of corporate intellectual property (IP) with no health and safety implications. After obtaining human research ethics approval from our institution, as well as permission from our industry partner the survey was administered to staff working in the mining industry and based in Australia. The nature of our respondents' industry sector is such that they were familiar with the security threats discussed in the cases. Snowball sampling was employed, with the researcher sharing the survey link within his organizational connections and asking them to share it with their colleagues. We also included a question in the survey to verify that respondents were from our target industry.

Section 1 of the survey collected demographic details, following this, respondents were randomly allocated to either of the two scenario groups. They were asked to report their affective responses in relation to the scenario shown. Finally, the survey collected information security threat and coping appraisals, including those of Threat Severity.

# 4 Data and Analysis

In the current round of data collection 132 responses were received; 30 of these were incomplete and were screened from the final sample leaving a total of 102 usable responses. Respondents were skewed towards males with 85.3% male respondents. Though skewed, this represents the gender balance of the resources industry where this study was conducted. In terms of age, most respondents were in the 35-44 age bracket (38.2%), followed by 45-54 (29.4%) and 25-34 (20.6%). Respondents were randomly allocated to either of the two scenario groups by the Qualtrics platform. This yielded an even balance of 51 respondents in each of the scenario groups Health and Safety Risk, and IP Breach. These two groups will be denoted with the HSR and IP subscripts henceforth. Preliminary analysis of this data is presented in the following sections organized according to the two propositions:

## 4.1 Do security threats elicit a range of affective states, differing by context?

In descending order, the emotions of Concern *($M_{HSR}$=4.27, SD=.94;$M_{IP}$=3.75, SD=1.146)* Interest *($M_{HSR}$=3.76, SD=1.16  $M_{IP}$=3.51, SD=1.12)*, *Worry ($M_{HSR}$=3.61, SD=1.18 $M_{IP}$=3.37, SD=1.26)* and Fear *($M_{HSR}$=3.22, SD=1.14 $M_{IP}$=3.10, SD=1.20)* emerged as the strongest responses reported by participants.

The evidence of the magnitude of the Concern emotion is interesting and warrants further analysis. Especially as prior work that has attempted to motivate user response has focused on Fear. As the mean value of Concern was also apparently higher in the Health and Safety related scenario vs Data Integrity scenario *(4.27 vs 3.75)* further testing was conducted to evaluate if these differences were statistically significant. The data has a continuous dependent variable, the independent variable has two categorical groups (different threat scenarios) and the observations are independent, thus an independent samples t-test was suitable to evaluate these differences. There were no outliers in the data, as assessed by inspection of a boxplot, and a visual inspection of the Normal Q-Q plot confirmed that the data were normally distributed. Thus, this data met the assumptions required to proceed with the independent samples t-test. The assumption of homogeneity of variances was violated, as assessed by Levene's test for equality of variances *($p$ = .041)*, therefore equal variances were not assumed in interpreting t-test results.

The test revealed that levels of Concern were significantly higher in the Health and Safety threat scenario group as compared to the IP breach threat scenario group (*t(100) = 2.551, p=0.012)*.

### 4.1.1 Extracting a new marker for emotional influence

The previous section described firstly how the Concern emotion was identified as the strongest response in both scenarios, and secondly that this response is significantly stronger in the Health and Safety risk scenarios. This, however, provides only a unidimensional view of respondent affect, whereas our PANAS instrument measured affective response in terms of 12 components.

Though effective as a discriminator in our early data set, we sought to improve the variance explained by accommodating a wider range of these measured emotional responses. Bivariate correlations of the affect responses reveal several items are highly correlated. Specifically, Concern is strongly correlated with Fear (*r=.448*), Worry (*r=.702*) and Pessimism (*r=.446*). Due to these high observed correlations, this data is a good candidate for factor analysis to reveal if a single latent factor may explain a greater portion of the variance.

A Scree plot was generated to visualise the eigenvalue by component number. It was seen from the Scree plot that the variance explained levelled off rapidly by the third component. Therefore, further factor analysis was constrained to extracting two components. Exploratory factor analysis was conducted using the Maximum Likelihood estimation method and Varimax rotation and small coefficients suppressed (below 0.3). The resulting model did not pass goodness-of-fit tests (*χ2(2) = 75.588, p = .002*), leading us to reject this model. Further exploratory factor analysis was conducted, without constraining the model to a fixed number of factors and instead employing the eigenvalue>1.0 criterion. This resulted in a stable solution with acceptable goodness-of-fit *(($\chi^2(2) = 17.452, p = .829$))*. This factor will be utilised in later stages of our research, however, preliminary analysis reveals that it requires further transformation and development, and it is not yet ready to use as a reliable indicator of affect.

To address our second proposition, a more direct approach was taken to model affect. As we have shown that in our data set Concern correlates strongly with Fear, Worry, and Pessimism, a composite variable (Ley, 1972) was computed as the arithmetic mean of these 4 emotions. This variable captures the overall negative affect modelled to test the influences on threat severity in the next section.

## 4.2 Do affective states contribute to the threat appraisal?

Threat Severity, a core component of the threat appraisal process was measured using a five-item scale (Ifinedo, 2012). Scale analysis revealed a Cronbach's alpha of 0.81 and thus the scale was found to be reliable (Nunnally 1978). Threat Severity ranged from 2.20-5.00 out of a maximum of 5, with a sample mean of 4.60 (*SD=.52*).

Linear regression was carried out to analyse if affective response was a significant influence on Threat Severity. Four responses in the data set had standardized residuals greater than 3 SD and were removed as outliers, leaving a final sample of n=98 for this analysis. Residuals were independent, as assessed by a Durbin-Watson statistic of 2.194. There was homoscedasticity, as assessed by visual inspection of a plot of standardized residuals versus standardized predicted values. Residuals were normally distributed as assessed by visual inspection of a normal probability plot. Negative affect accounted for 12.3% of the variation in perceived Threat Severity, with adjusted $R^2$ = 11.4%, a medium size effect according to Cohen (1988). The relationship between negative affect and Threat Severity was found to be statistically significant *($F(1, 96) = 13.496, p < .001$).*

# 5 Discussion

This manuscript describes the results of our first phase of data collection and analysis into the role of affect in information security risk perceptions. Data was collected from 102 Australian resources industry employees, providing insights into their perceptions in response to two information security risk scenarios.

Our first proposition examined whether the context of the security threat elicited a different pattern of state affect in the respondents. This was motivated by our observation that in the limited work that has considered affect, there is no systematic evaluation of whether different threats may elicit different emotional responses. This is a significant gap and could to some extent explain why users may respond to security threats in some cases but not others. We found that both security threat scenarios elicited negative emotional responses, and this is consistent with expectations. However, the deeper insight into the pattern and magnitude of specific emotional responses is a novel contribution that extends prior work – notably our finding that concern is the strongest emotional response. This finding is relevant, given that fear appeals are the dominant component in behavioural studies (e.g. Johnston & Warkentin, 2010), and suggests that researchers should seek to broaden their focus.

Out of the information security scenarios, we also discovered that the one that had health and safety implications elicited a more strongly negative response, which we were able to empirically establish with statistical significance. A possible explanation for this difference lies in the way individual risk assessments take place. Slovic (1987) explains that individuals employ a "dread" factor as well as subjective assessments of risks that are not always tied to real-world probabilities. Certain types of hazards, notably those that threaten personal health and safety will carry a higher dread factor and thus elicit a stronger response, thus explaining our finding with the two security scenarios.

Our second proposition examined whether these measurable negative affective states would be likely to have a real-world impact in terms of changing user behaviour. We explored this by testing if the negative emotions impacted perceptions of threat severity – an important general determinant of risk behaviour. We found that negative emotions have a statistically significant influence on perceived threat severity. This is explained by the appraisal tendency of these emotions which predisposes the respondents to appraise the risks in certain ways (Lerner & Keltner, 2001). In this case, the negative affective state leads to more pessimistic perceptions of risks, as exhibited by the higher perceptions of threat severity. This finding also creates opportunities for further work as there is evidence that different emotional states could be likely to influence different judgments and choices (Lerner & Keltner, 2000).

Future work may thus examine specific emotions with risk assessments, motivations, and behavioural intentions. There are also potential limitations to our work which may be considered in later studies. As our data collection was conducted in the mining industry, the gender balance of respondents is skewed towards males. It is possible that there are gender differences in affective responses, and these may make an interesting area for further work. This is especially likely, given that our prior work has revealed gender differences in relevant areas such as information security behaviour (McGill & Thompson, 2021) or information disclosure (Thompson & Brindley, 2020). In addition, our approach of utilising written scenarios may have limitations as it is possible that hypothetical scenarios may not be as emotionally evocative as real-world events. Thus, another avenue for investigation is to replace the written scenarios with simulations to provide a more realistic gauge of emotional responses.

Our work thus far has made several discoveries regarding the experience, and role of affective states in the context of information security. These findings will inform the next iteration of our theoretical model which, after collecting additional data, we will empirically evaluate with structural equation modelling. We hope that these interesting findings to date will stimulate other researchers to explore this promising avenue of information security study.

# 6 References

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99*, 102030. doi:10.1016/j.cose.2020.102030

Baskerville, R., Hee Park, E., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People, 27*(2), 155-181. doi:10.1108/ITP-11-2011-0068

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. Florence: Florence: Routledge.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43-69.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39. doi:10.4018/irmj.2005100102

Eid, M., & Diener, E. (1999). Intraindividual variability in affect: Reliability, validity, and personality correlates. *Journal of Personality and Social Psychology, 76*(4), 662-676. doi:10.1037/0022-3514.76.4.662

Forgas, J. P., Chan, N. Y. M., & Laham, S. M. (2001). Affective influences on thinking and behavior: Implications for clinical, applied and preventive psychology. *Applied & Preventive Psychology, 10*(4), 225-242. doi:10.1016/S0962-1849(01)80001-9

Frijda, N. H. (1986). *The emotions*: Cambridge University Press.

Gonzalez-Ibanez, R. I. (2013). *A study of positive and negative affective states in collaborative information seeking*. (PhD). Rutgers University,

Harmon-Jones, E., Gable, P. A., & Price, T. F. (2013). Does negative affect always narrow and positive affect always broaden the mind? Considering the influence of motivational intensity on cognitive scope. *Current Directions in Psychological Science, 22*(4), 301-307. doi:10.1177/0963721413481353

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-566. doi:10.2307/25750691

Lerner, J. S., & Keltner, D. (2000). Beyond valence: Toward a model of emotion-specific influences on judgement and choice. *Cognition & Emotion, 14*(4), 473-493.

Lerner, J. S., & Keltner, D. (2001). Fear, anger, and risk. *Journal of Personality and Social Psychology, 81*(1), 146.

Ley, P. (1972). *Quantitative aspects of psychological assessment* (Vol. 1): London: Duckworth.

McGill, T., & Thompson, N. (2021). Exploring potential gender differences in information security and privacy. *Information and Computer Security, 29*(5), 850-865. doi:10.1108/Ics-07-2020-0125

Ormond, D., Warkentin, M., & Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems, 20*(12), 4.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93-114.

Sigal, G. B., & Donald, E. G. (2007). Why does affect matter in organizations? *Academy of Management perspectives, 21*(1), 36-59. doi:10.5465/AMP.2007.24286163

Sjöberg, L. (2007). Emotions and Risk Perception. *Risk management, 9*(4), 223-237. doi:10.1057/palgrave.rm.8250038

Slovic, P. (1987). Perception of risk. *Science, 236*(4799), 280-285.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2013). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk and rationality. In *The feeling of risk* (pp. 21-36): Routledge.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy, 9*(1), 26-46. doi:10.4018/IJISP.2015010102

Spector, P. E., & Fox, S. (2002). An emotion-centered model of voluntary work behavior: Some parallels between counterproductive work behavior and organizational citizenship behavior. *Human Resource Management Review, 12*(2), 269-292. doi:10.1016/S1053-4822(02)00049-9

Thompson, N., & Brindley, J. (2020). Who are you talking about? Contrasting determinants of online disclosure about self or others. *Information Technology & People, 34*(3), 999-1017.

Thompson, N., McGill, T., & Narula, N. (2024). "No point worrying"–The role of threat devaluation in information security behavior. *Computers & Security, 143*, 103897.

Treffers, T., Koellinger, P. D., & Picot, A. (2016). Do affective states influence risk preferences?: Evidence from incentive-compatible experiments. *Schmalenbach Business Review, 17*(3), 309-335. doi:10.1007/s41464-016-0018-3

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198. doi:10.1016/j.im.2012.04.002

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of Personality and Social Psychology, 54*(6), 1063.

Yuen, K. F., Li, K. X., Ma, F., & Wang, X. (2020). The effect of emotional appeal on seafarers' safety behaviour: An extended health belief model. *Journal of Transport & Health, 16*, 100810. doi:10.1016/j.jth.2019.100810

## Copyright