Manipulation of Risk and Goal Activation on Cyber Security Risk Preventive Behaviour Motivation

Investigating the Mediating Role of Security Fatigue

Pineda, Samantha N.M.

Award date:
2023

Eindhoven, July 2023

Manipulation of Risk and Goal Activation on Cyber Security Risk Preventive Behaviour Motivation: Investigating the Mediating Role of Security Fatigue

by Samantha Pineda

0955723

in partial fulfilment of the requirements for the degree of

Master of Science
in Human-Technology Interaction

Supervisors:
Dr. Jaap Ham
Dr. Uwe Matzat
Dr. Peter Ruijten-Dodoiu

Abstract

This research aimed to investigate the impact of manipulating risk and goal activation on risk-preventive motivation behaviour, including the mediating role of security fatigue. A 2x2 factorial design of experiments between subjects was conducted. Participants were randomly assigned to one of four conditions (high/low risk activation combined with high/low goal activation). The participants' motivation for risk preventive behaviour, risk perception, risk awareness, goal specificity, goal difficulty, and security fatigue were measured. Research has shown how risk awareness can increase security fatigue through overwhelming and tiring information. Unlike previous works, we use goal setting theory which is new in the context of cyber security. Expectations are that goal activation can bypass security fatigue and positively influence risk preventive motivation behaviour, and that risk activation be adversely impacted by security fatigue. Our findings revealed no significant effects of the risk or goal activation manipulations on risk preventive behaviour motivation. However, the study uncovered a significant correlation between all variables, among them, risk perception and awareness show a significant interaction with security fatigue on risk-preventive behaviour motivation. These results are in line with expectations arguing that security fatigue is triggered through risk activation, and not triggered by goal activation. These findings have valuable implications for the design of future cybersecurity campaigns since increasing a user's risk awareness also increases a user's security fatigue. Thus, when campaigns want to bypass security fatigue, goal orientated focus in cyber security could be a solution to increase risk preventive motivation behaviour among people.

Keywords: Cyber Security, Security Fatigue, Risk Awareness, Risk Perception, Risk Activation, Goal Activation, Goal Specificity, Goal Difficulty, Risk Preventive Behaviour Motivation

Acknowledgements

I am pleased to share my master thesis report and express my gratitude to my supervisors, Jaap and Zoë, for their invaluable support throughout my academic journey. Jaap's expertise and weekly meetings helped me organize my thoughts and ideas repeatedly. I am grateful for Zoë's guidance during my internship, which allowed me to learn new and innovative ways of thinking. With their exceptional support, I have grown and learned so much over the past few months. I am truly thankful for their guidance.

Table of Contents

Introduction

The use of technology has rapidly grown in the present world. People use social networks, store and manage (private) data via the Internet, perform online transactions and automate all kinds of processes (Bendovschi, 2015). Although using all these technologies certainly has many benefits, using them is not always safe. Li and Liu (2021) discuss the main cyber risks organisations can encounter such as, malware phishing and ransomware. These risks are aimed at disrupting and/or collecting sensitive data, shutting down computer systems and servers and holding files hostage. That is, along with the increased online activity, cybercrime increases too. Cybercrime includes spreading viruses or other malware, hacking and distributed denial of service (DDoS) attacks (McGuire & Dowling, 2013). As Demirkan and colleagues (2020) state: "*Cyber Security attacks today have become so common that it is no longer characterised as an "if it" is going to happen, but it is now a "when will it" happen.*". These attacks on companies result in negative effects such as, intruding on business continuity, information security, and customer trust (Bendovschi, 2015). For the prevention of cyber-attacks, companies should closely monitor new cyber trends and threats and proactively protect their data and assets. Companies can use several techniques to increase cyber security. Hard-coded measures such as firewalls, malware scanners, and anti-virus software help to prevent cyber-attacks and risks (Reddy & Reddy, 2014). In addition, companies are implementing mandatory security policies that ensure safe behaviour of employees. These measures dictate specific requirements that employees should follow to ensure security. For example, password control demands that passwords must contain different kinds of characters and numbers and

must be changed every few months. Another popular intervention tool is two-factor authentication, where the employee must follow two steps before any login can occur on the device (Kemmerer, 2003). Nevertheless, technology alone is not enough. It is not possible for companies to anticipate and address every behavioural safety risk through hard coding (Pfleeger & Caputo, 2012).

That is, as good as online security can be, human behaviour is one of the main factors causing risks in cyber security (Evans et al., 2016). Companies are not only dependent on security systems but also vulnerable to the unsafe behaviour of employees. Many times, people create cyber risks because they have too little/no knowledge, skills and/or awareness (Zimmermann & Renaud, 2019). There are several techniques to increase cyber security through human behaviour. One way to improve the behaviour of your employees in terms of cyber security is through security, training, and awareness (SETA) programs (Coventry et al., 2014; Telstra Corporation, 2018). This is to make employees aware of the existing cyber risks and the preventive measures that should be taken. Alshaikh and colleagues (2021) argue the importance of risk awareness and knowledge of risk for the employee to comply with secure behaviour. As for the Dutch government, guidelines are given on how to increase safe behaviour among your employees. They indicate the importance of awareness of risks and suggest stimulating constant alertness (*Cyberbewustwording*, n.d.). Thus, all this shows that currently campaigns often rely on risk awareness and risk perception as main factors for increasing risk preventive behaviour motivation.

The reasoning behind most of these campaigns seems to be based on many theories trying to explain and manipulate employees' intentions and actual behaviour in

cyber security. Theories often used are the Technology Acceptance Model (Dash & Ansari, 2022), the Drive Model (Bada et al., 2019), and Protection Motivation Theory (Lebek et al., 2014; Li et al., 2019). These theories have in common that they use costs and benefits in explaining human behaviour. For example, the Protection Motivation Theory is a psychological model that explains how individuals perceive and respond to threats and adopt protective behaviour. It suggests that people are motivated to protect themselves from potential harm or adverse outcomes by assessing the threat and their coping ability (Rogers, 1975). Kahneman (2003) explains how people assess the likelihood and severity of a risk through the availability heuristic, indicating it depends on how well someone is to recall or knows the risk in their mind. According to Pfleeger and Caputo (2012), risks that are easily remembered by people are perceived as more probable and serious. This suggests that people tend to perceive less noticeable risks as less common and less serious than they truly can be (Pfleeger & Caputo, 2012). Deploying this information in the context of cyber security, Tsai and colleagues (2016) showed that the severity of the online threats predicts the user's risk preventive behaviour motivation. That is why, to increase gains and so protective behaviour, companies choose to increase risk perception and risk awareness.

However, studies have shown that grounding interventions solely on these theories are not always effective; Ng and Xu (2007) show that risk perception did not affect actual behaviour, possibly because security is often seen as an inconvenience by people. Pattinson and colleagues (2016), showed a weak relationship between the amount of cyber security training and employees' ability to avoid a cyber threat. This

could indicate that awareness of cyber security training is not the ideal influence for increasing risk preventive behaviour motivation.

An important reason for the ineffectiveness of interventions focussing on risks and risks awareness might be that people who receive too much information about risks and security during training may experience security fatigue. Security fatigue can diminish the effectiveness of all cybersecurity interventions (Stanton et al., 2016). Security fatigue refers to the mental and emotional exhaustion that individuals experience when dealing with security measures, requirements, and decisions in their daily lives (Furnell & Thomson, 2009). Stanton and colleagues (2016) showed the negative impact of security fatigue on cyber behaviour. This is because the employee may either lack interest or feel overwhelmed by the information presented in cyber security campaigns. Security fatigue can lead to employees no longer engaging with cyber security advice (D'Arcy et al., 2014) and disregarding security-related protocols (Choi et al., 2018). Furnell and Thomson (2009) argue that elaborate explanations of cyber security and the activation of severe risk awareness and risk perception will increase the possibility of security fatigue. Which means, companies attempting to enhance an employee's risk preventive behaviour motivation through risk activation may lead to potentially negative outcomes.

As human behaviour is a key element in cyber security, it remains important to continue raising awareness of cyber risks. However, we should also find ways to diminish the impact of security fatigue. One effective method is to present information in a variety of ways, which can help people to stay vigilant (Anderson 2015). But still, by the 'overwhelming and tiresome' information flow that descends from previous

awareness campaigns there is a possibility that security fatigue is increased (Reeves et al., 2021).

In the current research, we argue that interventions to stimulate cybersecurity should try to avoid difficult and long explanations of cyber security information. We suggest exploring alternative methods to encourage risk prevention behaviour motivation. We argue that another strategy to diminish security fatigue can be goal priming. Goal priming involves bringing goals or motivations to the surface of one's consciousness by using external cues or stimuli. These cues can be explicit or implicit and can be presented through various means, such as words, images, or environmental cues. When these goals are activated, priming has the ability to affect how individuals make decisions. (Bargh, 2006). Moreover, psychological research shows that goal priming significantly affects behaviour motivation and persistence towards goal-relevant tasks (Custers & Aarts, 2010). Taking Goal Setting Theory, this theory outlines how setting specific and challenging but attainable goals can lead to higher performance and motivation levels (Locke & Latham, 2019). In order to follow the goal setting theory, it is important that the goals meet specific criteria. These criteria include being specific and challenging, yet achievable (Lunenburg, 2011). Nevertheless, goal-setting theory has yet to be applied in the context of cyber security and security fatigue.

We suggest that instead of solely raising risk awareness and risk perception, it is more effective to (also) focus on attainable goals and behaviour in cyber security. This approach can reduce or eliminate security fatigue and ultimately motivate individuals to engage in risk preventive behaviour. To compare the effectiveness of goal activation to

the effectiveness of risk activation on risk preventive behaviour motivation, the current research will study the question:

What is the influence of risk activation and goal activation on cyber security risk preventive behaviour motivation, and what is the mediating role of security fatigue in this relation?

We will study this question using a 2x2 design of experiment between subjects for employees of the same company manipulating high or low goal activation and high or low risk activation. The aim of goal activation will be increasing risk preventive behaviour motivation by increasing goal specificity and goal achievability. The aim of risk activation is to improve employees' risk awareness and risk perception. Participants will be asked to read a goal activating text which increases the goal of correct behaviour through explanations of goal specificity and goal achievability. Besides, participants will also be asked to read a risk activating text explaining risks and consequences when behaving risky. This manipulation will be checked by the perceived risk awareness and risk perception of the participant.

We expect that participants who have received high risk activation will show higher risk preventive behaviour motivation than participants who have had low risk activation. This is because research has shown that high-risk perception can increase motivation to avoid adverse outcomes, whereas low-risk perception can lead to reduced motivation to avoid adverse outcomes (Weinstein, 1989).

Also, taking security fatigue into account, we expect a mediation effect of security fatigue on the relationship between risk activation and the user's motivation to perform cybersecurity behaviour. That is, as previously described, research showed that

security fatigue increases when information is overwhelming and when the participant lacks interest (Stanton et al., 2016). Since cyber security risks are often outside the employees' field of knowledge and interest, we expect that risk activation will increase security fatigue. With the increase of security fatigue, we expect the consequence of a decreasing effect on risk preventive behaviour motivation. Thus, due to security fatigue, we expect a negatively mediated effect on the relation of risk activation and risk preventive behaviour motivation.

Next, we expect that participants who have received high goal activation will show higher risk preventive behaviour motivation than participants who have had low goal activation. This because previous research has shown an increase in motivation when goal specificity and goal achievability are high (Lunenburg, 2011). We expect the same result in a cybersecurity context.

Relatedly, taking security fatigue into account, we expect no mediation effect on goal activation. Since goal activation will focus on behavioural patterns of risk preventive behaviour and will not include any difficult terms or expected knowledge in cyber security, we do not expect that security fatigue will be triggered. Therefore, we do not expect a mediating effect of security fatigue on the relationship between goal activation and risk preventive behaviour motivation.

Figure 1 presenting the hypotheses; the influence of risk and goal activation on risk preventive behaviour motivation, taking security fatigue into account

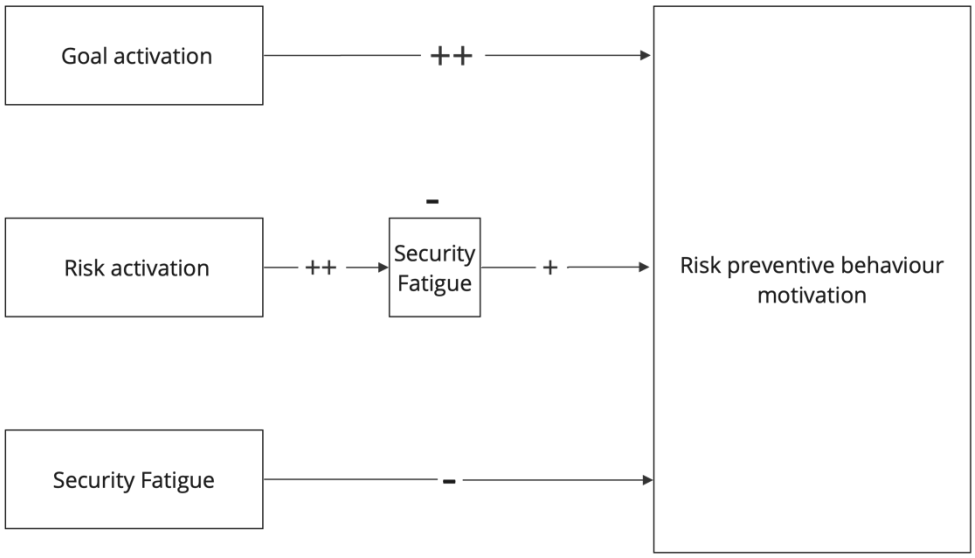


Figure 1 shows a visualisation of the expected effects of risk activation and goal activation on risk preventive behaviour motivation, taking the mediating effect of security fatigue into account. This shows that goal activation would increase risk preventive behaviour motivation more than risk activation, due to the negative effects of security fatigue. However, as previous research has shown, we expect that security fatigue itself has a negative effect on risk preventive behaviour motivation(Stanton et al., 2016).

Method

Participants and design

This study involved a total of 261 participants, comprising 191 men, 66 women and 4 preferred not to say. The participants had a mean age of 43.8 years (*SD* = 9.2) with a range of 26 to 64 years. All participants were employees of the same company and listed as frequent travellers. Participants are randomly assigned to one of four experimental conditions: high goal priming/high risk perception, high goal priming/low risk perception, low goal priming/high risk perception, and low goal priming/low risk perception.

A 2x2 factorial between subjects design was used, with as dependent variable risk preventive behaviour motivation and as independent variables risk activation (high or low) and goal activation (high or low). The analysis will consist of an analysis of variance (ANOVA), main effects and interactions. Assuming a medium effect size (f = 0.25), a power of 90% and a significance level of 5%, G*Power (Version 3.1.9.2, 2014) indicates a sample size of 232 needed. For this research, we deem that effect size enough to provide an interesting insight.

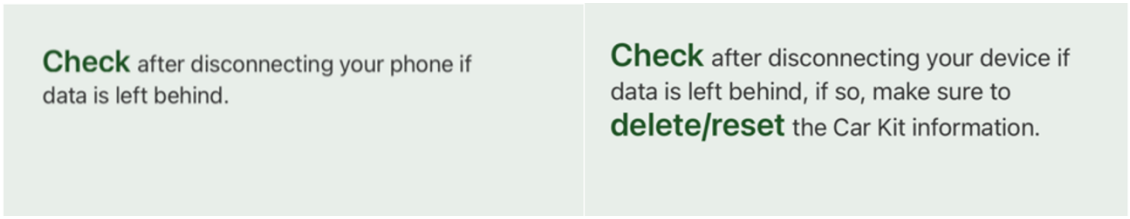
Materials

The survey was developed in Microsoft Forms since this was the assigned and trusted product for the company with which we worked. The survey was conducted in English. The survey showed two cyber security scenarios always in the same order. Scenario 1 shows the textual explanation of the risks and expected behaviour of *Connecting* your device to WiFi or Bluetooth. Scenario 2 shows the textual explanation

of the risks and expected behaviour of *Charging* your phone. These texts will also highlight some important wordings in bold.

Participants in the condition of High Goal activation were asked to read an elaborate explanation of expected safe behaviour. For example, they are shown the text "***Check*** *if there is data left behind; if so, please make sure to* ***delete or reset*** *the device*" Participants in the condition of Low Goal activation were asked to read a short explanation of expected behaviour without any steps of how to reach the goal. For example, "***Check*** *if there is data left behind*". Both conditions show some activating words in bold text. See Figure 2 for an example of scenario 1 goal activation. The overall activation will be measured by 'Goal Specificity' and 'Goal Difficulty'. This way, we can test the effect of the manipulation on the participant.

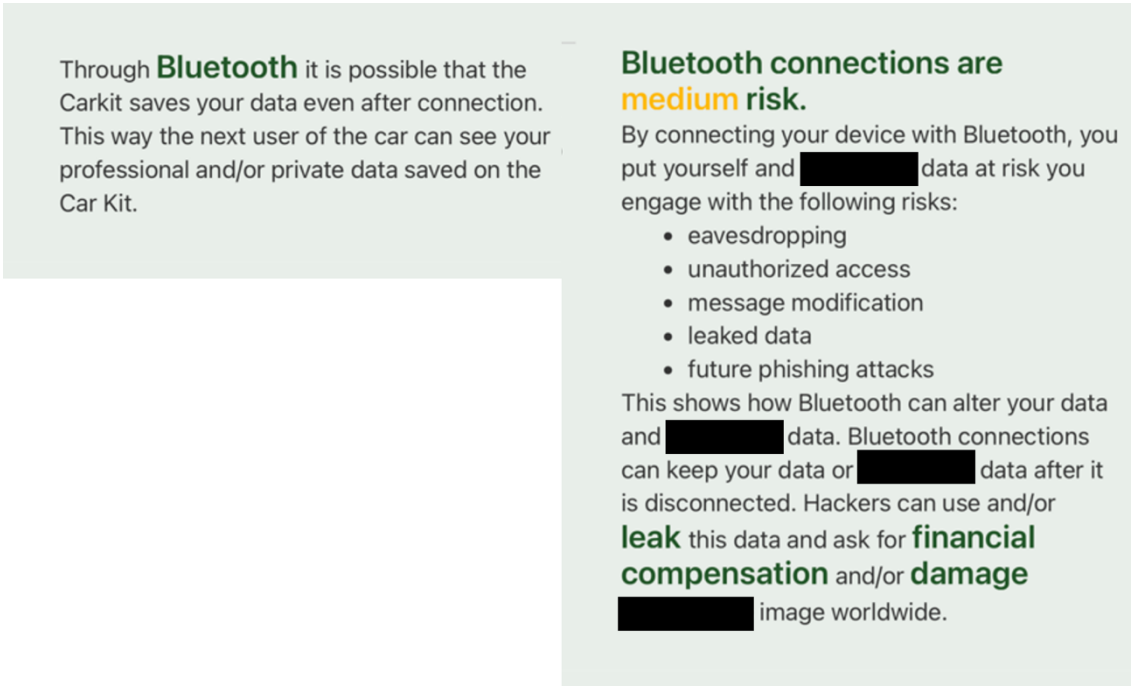
Figure 2 shows the manipulation of low goal activation (left) versus high goal activation (right)



Participants in the condition of high risk activation were asked to read a text explaining specific consequences and risks that the participants take if they show unsafe behaviour. Participants in the condition of low risk activation were asked to read a short explanation of consequences if risks are taken such as "*Data is leaked*". Participants in the condition of high risk activation are shown an elaborate explanation of risks and consequences of their behaviour for their personal and companies safety. See Figure 3 for an example of risk activation in scenario 1. The activation will be

measured by "Risk Awareness" and "Risk Perception" to ensure the manipulation influenced the participant.

Figure 3 shows the manipulation of low risk activation (left) versus high risk activation (right). The companies name is filtered out in black.



After a scenario was presented, 12 questions were posed. The order of the scenarios and questions was consistent for all participants. We employed a measurement approach consisting of two questions per scenario for each of the following variables: Motivation, Fatigue, Specificity, Difficulty, Awareness and Perception. Resulting that each variable was measured by in total four questions taking both scenarios together. A variable was calculated through the mean of two questions over two scenarios. Consequently, the survey had a total of 24 questions (12 questions per scenario), but they were condensed into six variables. An overview of all survey questions can be found in Appendix A.

To assess participant's risk preventive behaviour motivation, we averaged four questions (2 questions X 2 scenarios) and constructed a reliable measure (Cronbach's $\alpha = 0.85$). That is, for each scenario, participants were asked to answer the following two questions on a 7-point Likert scale ranging from 1 (totally disagree) to 7 (totally agree); *'I want to act correctly to prevent cyber risks'* and *'I am motivated to take preventive measures to reduce risk'*.

To check our goal activating manipulation, we measured specificity and difficulty. By averaging these eight questions (2 questions X 2 variables X 2 scenarios), we constructed a reliable measure (Cronbach's $\alpha = 0.79$) of the perceived goal activation of the participant. To measure specificity (Cronbach's $\alpha = 0.74$), participants were asked to answer the following two questions on a 7-point Likert scale ranging from 1 (totally disagree) to 7 (totally agree); *'This scenario shows a clear explanation of expected behaviour to prevent cyber risks.'* and *'I understand what is expected from me to prevent risks'*. To measure difficulty (Cronbach's $\alpha = 0.71$), participants were asked to answer the following two questions on a 7-point Likert scale ranging from 1 (totally disagree) to 7 (totally agree); *'It is too difficult for me to behave risk preventive in this scenario'* and *'I am able to act correctly to prevent cyber risks'*. Since the first statement of difficulty is in negative sentiment, the score scale is turned around when analysing the data. This is to make sure the sentiment of the two statements is in the same direction.

To check our manipulation of risk activation, we measured perception and awareness. By averaging these eight questions (2 questions X 2 variables X 2 scenarios), we constructed a reliable measure (Cronbach's $\alpha = 0.83$) of the perceived

risk activation of the participant. To measure perception (Cronbach's $\alpha = 0.68$), participants were asked to answer the following two questions on a 7-point Likert scale ranging from 1 (totally disagree) to 7 (totally agree); *'This scenario shows a big risk in cyber security.'* and *'I feel that these security measures are an unnecessary burden on my daily activities'.* To measure awareness (Cronbach's $\alpha = 0.69$), participants were asked to answer the following two questions on a 7-point Likert scale ranging from 1 (totally disagree) to 7 (totally agree); *'Because the potential consequences I am motivated to behave in a secure way'* and *'I don't think this scenario is that important in cyber security'.* Since the second statement both perception and awareness are in negative sentiment, the score scale is turned around when analysing the data. This is to ensure that the sentiment of the two statements is in the same direction.

To assess the mediating variable, we measured fatigue. By averaging these four questions (2 questions X 2 scenarios), we constructed a reliable measure (Cronbach's $\alpha = 0.73$). To measure fatigue, participants were asked to answer the following two questions on a 7-point Likert scale ranging from 1 (totally disagree) to 7 (totally agree); *'I feel tired by the security measures I need to follow'* and *'I feel overwhelmed when I read this information'*.

Procedure

This study adhered to the Code of Ethics of the NIP (Dutch Institute for Psychologists), and was approved by the Ethical Review Board of the Human-Technology Interaction Department at Eindhoven University of Technology.

Participants were approached by an online link in their company email. By clicking the link, participants could directly participate the survey. Participants were

first asked for their agreement to the informed consent of the study. Then participants are asked some demographic questions answering their age, gender, work department and if they had any previous experience with cyber-attacks. After completing demographics, scenario 1 is shown. This scenario was followed by the measurement of 'Risk Preventive Behaviour Motivation', ' Security Fatigue', ' Risk Awareness', 'Risk Perception', 'Goal Specificity' and 'Goal Difficulty', as described under Materials. After the assessment of the scenario 1 statements, participants were presented with the second scenario. Again, followed up by exactly the same 12 statements as scenario 1. After completion, participants were thanked and debriefed. The debrief included showing all the information given in the high goal activation and high risk activation to make sure that participants were not misled. When the participant was already in the high goal activation and high risk activation condition, they were informed that they received all information necessary about the scenarios. Participants were not compensated since they were all employees of the company.

Results

Prior to testing our hypothesis, we conducted a manipulation check to ensure the effectiveness of the manipulation (risk activation and goal activation) in each condition. We analysed this by running a t-test for the perceived goal activation in the manipulation of goal activation. We found no evidence that participants who had high goal activation scored higher on perceived goal activation than participants who had low goal activation ($p = 0.48$, $t = 0.71$). For the perceived risk activation, we found no evidence that participants in the high risk manipulation perceived higher risk activation than participants with low risk activation ($p = 0.41$, $t = 0.83$).

Hypothesis testing:

To test our hypothesis, we submitted the dependent variable, risk preventive behaviour motivation, to a 2x2 design of goal activation (high or low) and risk activation (high or low). Testing the influence of risk activation on risk preventive behaviour motivation, we ran an analysis of variance test (ANOVA). The test did not show a significant result ($p = 0.54$). Testing the influence of goal activation on risk preventive behaviour motivation, through an ANOVA, results did not show a significant effect ($p = 0.50$). Checking the interaction effect through the ANOVA of the risk activation and the goal activation, no evidence was found for an interaction effect ($p = 0.97$). Since there is no significant effect, we could not analyse the mediation effect of security fatigue.

When not taking risk preventive behaviour motivation into account and measuring security fatigue as the dependent variable in the ANOVA, influenced by goal activation (high or low) and risk activation (high or low), we do not find any

significant effect for goal activation ($p = 0.83$) and risk activation ($p = 0.36$) on security fatigue.

The influence of perceived risk activation and goal activation on motivation

Although our manipulations appear to have been ineffective, we can still analyze the naturally occurring relation between participants' risk activation levels, goal activation levels and risk preventive behaviour motivation. To explore these relationships, we analyzed the correlations between these variables. As shown in the correlation matrix presented in Table 1, we find that all five variables (Specificity, Difficulty, Awareness, Perception and Fatigue), significantly correlate with Motivation. See Table 1 for specific correlation values. All variables, except for Fatigue, correlate positively with Motivation. Fatigue shows a negative correlation with Motivation and all other variables.

Table 1 Correlation effects between all variables

	Motivation	Fatigue	Awareness	Perception	Difficulty	Specificity
Motivation	1.0000					
Fatigue	-0.4199	1.0000				
Awareness	0.6656	-0.3680	1.0000			
Perception	0.6261	-0.4904	0.7086	1.0000		
Difficulty	0.5849	-0.5199	0.5060	0.5487	1.0000	
Specificity	0.5651	-0.3840	0.5315	0.5446	0.6656	1.0000

When running a regression analysis on all variables, we created a model which explained the variance by 55% (Rs = 0.55). Furthermore, we find a significant effect for Awareness ($p = 0.01$), Perception ($p = 0.01$), Difficulty ($p = 0.01$), Specificity ($p = 0.03$). We do not find a significant effect of Fatigue ($p = 0.30$) on Motivation. See Appendix B for the complete overview of the regression results.

Since the regression analysis does not provide evidence for a relation between Fatigue and Motivation, but we did find a significant correlation, we tested an interaction effect of fatigue with Perception, Awareness, Difficulty, and Specificity. Taking all interactions in the same regression model, we created a model that explains the variance of Motivation by 60% (Rs = 0.60), and we found a significant effect for the interaction of Fatigue with Awareness ($p = 0.01$) but no significant effects for the other interactions. See Appendix B for the complete overview of the regression analysis values. However, when analyzing the interactions per activation in a regression model, we see that Difficulty ($p = 0.93$) and Specificity ($p = 0.10$) show no evidence of a significant effect when interacting with security fatigue. Also, this model with solely interaction with goal activating variables, the Rs drops to 0.56. But for the interactions of Perception *(*$p = 0.04$) and Awareness ($p = 0.01$) with security fatigue do show a significant effect, and this model keeps the Rs = 0.60.

When we run a regression on the perceived risk activation and perceived goal activation on Motivation with an interaction of Fatigue, we do not find a significant effect of perceived goal activation with fatigue ($p = 0.28$). However, we do find evidence of an effect between the interaction of fatigue with perceived risk activation ($p = 0.01$). If we look at the perceived risk and goal activation solely in the regression model with Motivation, we find no evidence for perceived risk activation as a direct effect on Motivation ($p = 0.52$), but we do find evidence for perceived goal activation as an direct effect on Motivation ($p = 0.01$)

Comparing scenario 1 and scenario 2

Since the survey consisted of 2 scenarios of both the same questions, we can test the difference in results between scenario 1 and scenario 2. Taking scenario 1, running an ANOVA on the perceived goal activation in the high goal manipulation shows no evidence for a significant effect (p = 0.38) After conducting an ANOVA to test for perceived risk activation in the high risk manipulation, no significant results were found (p = 0.26). Taking scenario 2, running an ANOVA on the perceived goal activation in the high goal manipulation shows no evidence for a significant result (p = 0.69) After conducting an ANOVA to test for perceived risk activation in the high risk manipulation, no significant results were found (p = 0.95).

Demographics

Running a t-test for Gender and Motivation, we do not find a significant effect (p = 0.48, t = -0.72).

Running a correlation between Age and Motivation, we find a significant result (p = 0.01) for a positive correlation of r =0.16. Running a regression analysis, we find evidence (p = 0.01) for the influence of age on Motivation, showing a Rs =0.03. However, when adding more variables in the regression model such as Fatigue, Age changes to a non-significant variable in the model on Motivation (p = 0.08).

Running an ANOVA on Previous Experience (Yes/No) we find a significant effect on Motivation (p = 0.01, Rs = 0.03) However, if we rule out all participants that encountered a previous experience with a cyber-attack in the complete dataset, we still do not find any evidence of an effect when running an ANOVA. The ANOVA for no-experience only participants of Motivation and Risk activation then shows a p-value of

$p = 0.58$ and the test on Goal activation also results in non-significant with a p-value of $p = 0.85$.

Discussion

This study investigated the influence of risk activation and goal activation on risk preventive behaviour motivation in the context of cyber security, taking the mediation of security fatigue into account. Previous research has shown mixed findings on the effects of risk awareness and risk perception on risk preventive behaviour motivation in cyber security. These mixed findings included security fatigue. Security fatigue refers to the feeling of being overwhelmed and disinterested by elaborate and complicated security campaigns, leading employees to not comply with security standards. (Stanton et al., 2016). When employees fail to engage in risk prevention practices, companies become vulnerable to cyber security risks. Therefore, we investigated the effects of goal activation on risk preventive behaviour manipulation. Other research has shown significant effects of goal setting theory on behaviour manipulation but is not yet investigated in cyber context (Locke & Latham, 2019). Currently, security fatigue is one of the main reasons why individuals are not taking preventative measures against potential risks(Stanton et al., 2016). With this in mind, we also studied how security fatigue impacts goal activation and risk preventive behaviour motivation.

Hypothesis testing

Contrary to our expectations, results showed no effect of both manipulations (risk activation and goal activation) on risk preventive behaviour motivation. Also, results suggested that security fatigue did not mediate the relation between risk preventive behaviour motivation and one of the manipulations, because there was no relation indicated to begin with.

Importantly, the manipulation checks suggested that both manipulations were not effective. That is, results showed no effect of our risk activation manipulation on perceived risk activation, nor an effect of our manipulation of goal activation on perceived goal activation by the participant. As a result, we cannot assume that our manipulations affected how participants perceived the activations. It is important to note that since our manipulations did not significantly increase participants' risk activation and goal activation scores, we should be cautious in interpreting the results of the research question. Since it could be seen as a limitation that the manipulations were not perceived by participants, and therefore manipulations were not effective in relation to risk preventive behaviour motivation. However, it is also possible that the manipulations were (perceived or not) not effective in relation to risk preventive behaviour motivation.

The finding that the manipulations were not effective could have several reasons. It is possible that the manipulations were too subtle to be detected by the participant or to have a significant impact. As Marett, (2015), discusses, manipulations should be balanced between being too subtle and too great to be comparable. Furthermore, the overall mean of risk preventive behaviour motivation was in all conditions very high, which could also make it more difficult to find significant effects increasing this number. This might suggest a ceiling effect, this term is used when the scores that are measured are at or near the possible upper limit (Everitt, 1998), so that variance is not measured or estimated above a certain level (Cramer & Howitt, 2004). Additionally, since the sample consisted of participants that were frequently travelling employees, participants may have been very well informed and motivated on

cybersecurity measures since they could be at higher cyber risk when travelling. It is also possible that these employees receive more cybersecurity-related information through their (IT-related) department, and thus have more cyber security knowledge to begin with. Another reason why maybe the manipulations were not found effective in this research is that possibly employees already encountered numerous previous cyber security campaigns including risk activation and/or goal activation. Therefore, perhaps employees already had increased knowledge of risk or goal activations of cyber security. As Kahneman (2013) stated, the perceived severity and likelihood are influenced by the recall of knowledge and memories. And possibly the employee already experienced security fatigue before starting this experiment.

Nevertheless, we suggest that future research should pre-test manipulations on a random sample before starting the complete research. This way the chances that the manipulations are perceived are increased. The pre-test can include several measures of subtle and radical manipulations, to check when the manipulations start to be perceived. Tackling the above-mentioned possibilities, future research could include a 'before' measurement that measures the risk preventive behaviour motivation, knowledge, and fatigue of a participant before the manipulations take place. This way future research makes it more likely to measure the influence before and after a manipulation, which we are missing now to make any statements about the effects of the manipulations.

Exploratory Findings

Although our results did not reveal an effect of the manipulations, our explorations presented evidence for correlations of risk activation (risk perception and

risk awareness) and goal activation (goal specificity and goal difficulty) scores and risk preventive behaviour motivation. That is, in line with the theoretical insights described in the introduction, indicating that when goal specificity and achievability (since the difficulty score is turned around for positive sentiment means high 'difficulty' actually 'not difficult' but achievable) increase, risk preventive behaviour also increases (Lunenburg, 2011). Next, when risk perception and risk awareness increase, risk preventive behaviour motivation also increases which is in line with the findings of Rosoff and colleagues (2013). Interestingly, we also find evidence for a negative correlation between risk preventive behaviour motivation and security fatigue. Indicating that when security fatigue increases, risk preventive behaviour motivation decreases. This aligns with the findings of Furnell & Thomson (2009).

To gain more insights into these correlations, we measured risk preventive behaviour motivation in a regression model with security fatigue, goal specificity, goal difficulty, risk perception and risk awareness. We find that more than half of the variance of risk preventive behaviour motivation is explained by these variables. However, we see that security fatigue does not directly influence risk preventive behaviour motivation in this model. Although, when we include the interaction between risk perception and security fatigue, as well as risk awareness and security fatigue, we find that the explained variance of risk preventive behaviour motivation increases. This means that including these interaction effects improves the model and thus shows more explanation of what risk preventive behaviour motivation influences, indicating that we should take the interaction as an effective measure to indicate risk preventive behaviour motivation. We also find that when we include these interaction effects, which show a

slightly positive effect on risk preventive behaviour motivation, risk awareness changes to non-significant. This could indicate that risk awareness is always mediated by security fatigue before influencing risk preventive behaviour motivation. This is in line with our first hypothesis stating that risk awareness triggers security fatigue. However. We also see that if we include goal difficulty, we find that when the goal becomes more difficult, security fatigue also increases. Which can be explained by the findings of Stanton et al., (2016). However, when we analyse the goal variables, the interaction between difficulty and security fatigue disappears when risk activating variables are added. Another finding in line with Kahneman (2003), is that we found a significant difference in effect on risk preventive behaviour motivation when the participant has experienced a cyber-attack before, or when they did not have any cyber-attack experience. Possibly indicating that the recall of an experience could increase the risk-preventive behaviour motivation of a person.

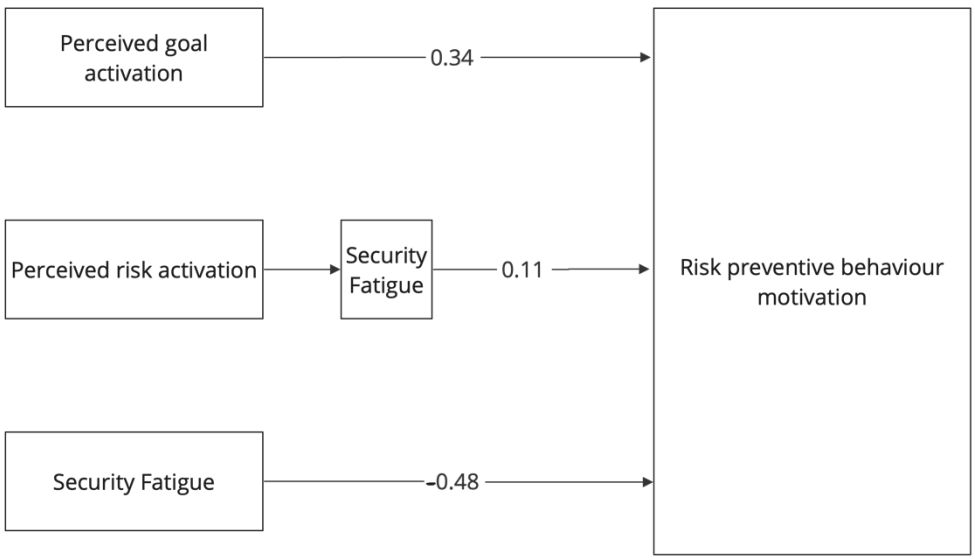
When we analyse the regression model of perceived risk activation, perceived goal activation, security fatigue and the interaction effects on risk preventive behaviour motivation. We find that perceived risk activation does not directly show an effect on risk preventive behaviour motivation, however, when we take the interaction effect of perceived risk activation and security fatigue, we do find a significant effect on risk preventive behaviour motivation. This finding is in line with our theoretical insights mentioned above and, in the introduction, indicating that participants who receive more difficult and technical information about cyber risks show higher security fatigue. This security fatigue mediates the effect between perceived risk awareness and risk preventive behaviour motivation. This suggests that when risk activating variables are

always mediated by security fatigue and do not interact with risk preventive behaviour without being mediated.

We find that perceived goal activation shows an effect on risk preventive behaviour motivation. However, the interaction of perceived goal activation and security fatigue does not show any effect on risk preventive behaviour motivation. This finding is in line with our hypothesis expecting that goal activation does influence risk preventive behaviour motivation and does not increase security fatigue. Meaning that goal activating variables do influence risk preventive behaviour motivation positively and are not mediated by security fatigue.

Thus, these findings indicate that there is a mediating effect of security fatigue on the relationship between perceived risk activation and risk preventive behaviour motivation. Next to, that perceived goal activation does indeed increases risk preventive behaviour motivation and does not interact with security fatigue to increase risk preventive behaviour motivation. See Figure 4 for a visualization of this finding.

Figure 4 presenting coefficients between the findings of perceived goal and perceived risk activation on risk preventive behaviour motivation mediated by security fatigue



Summary

Overall, the results provided no evidence that our manipulations were effective nor that our manipulations were able to influence risk preventive behaviour motivation. We need to be careful in interpreting these findings as the perceived activations did not show any effect with the manipulations. This suggests that the manipulations may have been too weak or there could have been other factors that limited their impact. Nevertheless, we did find interesting effects indicating that goal difficulty, goal specificity, risk awareness and risk perception do influence risk preventive behaviour motivation overall. Also analysing security fatigue, we find strong negative effects on awareness and difficulty, which is in line with the theory that if something is difficult or overwhelming, security fatigue is triggered (Stanton et al., 2016). We found that perceived goal activation influences risk preventive behaviour motivation, but perceived risk activation is mediated through security fatigue before influencing risk preventive behaviour motivation as also expected in our hypothesis. However, we measure that security fatigue overall, always negatively influences risk preventive behaviour motivation, which is in line with previous findings (Reeves et al., 2021, Furnell & Thomson, 2009)

Future research should test the manipulation effects more elaborate, meaning running pre-tests of manipulation checks and using baseline measures of participants before doing the manipulated experiment. This way, future research could ensure the manipulation effects of risk activation and goal activation.

This research presents evidence for the negative influence of security fatigue on risk preventive behaviour motivation. It shows how security fatigue can mediate the

relationship between risk awareness and risk perception on risk preventive behaviour motivation and how it mediates the perceived risk activation of the participant. Next, it shows how goal specificity is not directly mediated through cyber security. Meaning explaining a clear goal does not trigger security fatigue for the participant. Cyber security campaign designers should take security fatigue into account, and make sure they are not increasing this phenomenon. Because extreme security fatigue can have detrimental effects for cyber security (of companies), campaigns should find a way to bypass security fatigue among people. Since this research shows that perceived risk activation always interacts with security fatigue, future campaigns should use new ways to increase risk preventive behaviour motivation without intervening with security fatigue. Such as, we showed that by increasing goal specificity, and goal difficulty, risk preventive behaviour motivation is increased and not mediated by security fatigue. Meaning if future cyber security campaigns would shift their focus on achieving goals of correct behaviour, employees could show more risk preventive behaviour motivation without being decreased by security fatigue. This insight can have a huge impact on future cyber security knowledge, meaning people will learn how to behave instead of why they should behave a certain way. Surely companies who are dependent on their employee's cyber behaviour can have huge advantages of using goal activation in cyber security campaigns and bypassing employees' security fatigue.

References

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers and Security*, *100*. https://doi.org/10.1016/j.cose.2020.102090

Bada, M., Sasse, A. M., & Nurse, J. R. C. (n.d.). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*

Bargh, J. A. (2006). What have we been priming all these years? on the development, mechanisms, and ecology of nonconscious social behavior. In *European Journal of Social Psychology* (Vol. 36, Issue 2, pp. 147–168). https://doi.org/10.1002/ejsp.336

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Briggs, P., Blythe, J., & Tran, M. (n.d.). *Using behavioural insights to improve the public's use of cyber security best practices*.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Cramer, D., & Howitt, D. L. (2004). *The Sage dictionary of statistics: a practical resource for students in the social sciences*. Sage.

Custers, R., & Aarts, H. (n.d.). *The Unconscious Will: How the Pursuit of Goals Operates Outside of Conscious Awareness*. www.sciencemag.org

Cyberbewustwording. (n.d.).

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology*. www.irjet.net

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. In *Journal of Management Analytics* (Vol. 7, Issue 2, pp. 189–208). Taylor and Francis Ltd. https://doi.org/10.1080/23270012.2020.1731721

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667–4679. https://doi.org/10.1002/sec.1657

Everitt, B. (1998). The Cambridge dictionary of statistics. In *The Cambridge dictionary of statistics* (p. 360).

Furnell, S., & Thomson, K. L. (2009). Recognising and addressing "security fatigue." *Computer Fraud and Security*, *2009*(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. *American Economic Review*.

Kemmerer, R. A. (2003). *Cybersecurity*.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Locke, E. A., & Latham, G. P. (2019). The development of goal setting theory: A half century retrospective. *Motivation Science*, *5*(2), 93–105. https://doi.org/10.1037/mot0000127

Lunenburg, F. C. (2011). *Goal-Setting Theory of Motivation* (Vol. 15).

Marett, K. (2015). Checking the manipulation checks in information security research. *Information and Computer Security*, *23*(1), 20–30. https://doi.org/10.1108/ICS-12-2013-0087

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence Research Report 75 Cyber crime: A review of the evidence*.

Ng, B.-Y., & Xu, Y. (2007). *Users' Computer Security Behavior Using the Health Belief Model*. http://aisel.aisnet.org/pacis2007/45

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies.

Information and Computer Security, *24*(2), 228–240. https://doi.org/10.1108/ICS-01-2016-0009

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Reddy, G. N., & Reddy, G. J. U. (2014). *A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES*.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1). https://doi.org/10.1177/21582440211000049

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, *33*(4), 517–529. https://doi.org/10.1007/s10669-013-9473-2

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. *IT Professional*, *18*(5), 26–32. https://doi.org/10.1109/MITP.2016.84

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Weinstein, N. D. (1989). Effects of Personal Experience on Self-Protective Behavior. In *Psychological Bulletin* (Vol. 105, Issue 1).

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Appendix A:

This appendix shows the overview of asked questions in the survey. Below you can find the questions ordered per variable.

Demographics:
Please enter your age
Please enter your gender (Man/Woman/Prefer not to say)
Please enter your work department
Have you ever experienced a real cyber-attack before? (Yes/No/I don't know)

1. I feel overwhelmed when I read this information
2. This scenario shows a big risk in cyber security
3. Because the potential consequences I am motivated to behave in a secure way
4. I don't think this scenario is that important in cyber security
5. This scenario shows clear explanation of expected behaviour to prevent cyber risks
6. I want to act correctly to prevent cyber risks
7. I feel tired by the security measures I need to follow.
8. I am able to act correctly to prevent cyber risks
9. I understand what is expected from me to prevent risks
10. It is too difficult for me to behave risk preventive in this scenario
11. I feel that these security measures are an unnecessary burden on my daily activities.
12. I am motivated to take preventive measures to reduce risks

Risk Perception:
This scenario shows a big risk in cyber security
I feel that these security measures are an unnecessary burden on my daily activities.
Risk Awareness:
Because the potential consequences I am motivated to behave in a secure way
I don't think this scenario is that important in cyber security
Goal Specificity:
This scenario shows clear explanation of expected behaviour to prevent cyber risks
I understand what is expected from me to prevent risks
Goal Difficulty:
It is too difficult for me to behave risk preventive in this scenario
I am able to act correctly to prevent cyber risks
Risk preventive behaviour motivation:
I want to act correctly to prevent cyber risks
I am motivated to take preventive measures to reduce risks
Security Fatigue:
I feel tired by the security measures I need to follow.
I feel overwhelmed when I read this information

Appendix B

This appendix shows the regression model results done for the exploratory research. The following model shows the regression model between all variables on risk preventive behaviour motivation.

```
. regress Motivation Fatigue Awareness Perception Difficulty Specificity
```

The

Source	SS	df	MS	Number of obs	=	261
				F(5, 255)	=	63.55
Model	67.2413538	5	13.4482708	Prob > F	=	0.0000
Residual	53.9602746	255	.21160892	R-squared	=	0.5548
				Adj R-squared	=	0.5461
Total	121.201628	260	.466160109	Root MSE	=	.46001

Motivation	Coefficient	Std. err.	t	P>|t|	[95% conf.	interval]
Fatigue	-.0282092	.0268647	-1.05	0.295	-.0811141	.0246957
Awareness	.2830523	.0484488	5.84	0.000	.1876417	.378463
Perception	.1254596	.0492868	2.55	0.012	.0283986	.2225207
Difficulty	.1277101	.0403868	3.16	0.002	.0481759	.2072443
Specificity	.1067911	.0474923	2.25	0.025	.013264	.2003182
_cons	2.684158	.3087805	8.69	0.000	2.076073	3.292243

following model shows the regression model between all 6 variables and the interaction effect of fatigue with the risk or goal variables.

```
. regress Motivation Fatigue Awareness Perception Difficulty Specificity Fatigue_Awareness Fat:
```

Source	SS	df	MS	Number of obs	=	261
				F(9, 251)	=	41.46
Model	72.4625749	9	8.05139721	Prob > F	=	0.0000
Residual	48.7390535	251	.194179496	R-squared	=	0.5979
				Adj R-squared	=	0.5834
Total	121.201628	260	.466160109	Root MSE	=	.44066

Motivation	Coefficient	Std. err.	t	P>|t|	[95% conf.	interval]
Fatigue	-.637315	.1582274	-4.03	0.000	-.9489374	-.3256925
Awareness	-.2145281	.1156976	-1.85	0.065	-.4423899	.0133337
Perception	.3218346	.1126209	2.86	0.005	.1000323	.5436369
Difficulty	.1643985	.0890857	1.85	0.066	-.0110522	.3398491
Specificity	.0566384	.1134248	0.50	0.618	-.1667471	.280024
Fatigue_Awareness	.1499295	.0319332	4.70	0.000	.0870383	.2128206
Fatigue_Difficulty	-.0042444	.0266168	-0.16	0.873	-.0566651	.0481763
Fatigue_Perception	-.0564166	.0330388	-1.71	0.089	-.1214853	.0086521
Fatigue_Specificity	.0073731	.0331356	0.22	0.824	-.0578861	.0726322
_cons	4.701004	.5934278	7.92	0.000	3.532272	5.869737

The following model shows the regression model between all 6 variables and the interaction effect of fatigue and awareness, and fatigue and perception on risk preventive behaviour motivation.

```
. regress Motivation Fatigue Awareness Perception Difficulty Specificity Fatigue_Awareness
```

Source	SS	df	MS	Number of obs	=	261
				F(7, 253)	=	53.71
Model	72.4514975	7	10.3502139	Prob > F	=	0.0000
Residual	48.7501308	253	.192688264	R-squared	=	0.5978
				Adj R-squared	=	0.5866
Total	121.201628	260	.466160109	Root MSE	=	.43896

Motivation	Coefficient	Std. err.	t	P>|t|	[95% conf.	interval]
Fatigue	-.6287301	.1482229	-4.24	0.000	-.920638	-.3368222
Awareness	-.2176642	.1119968	-1.94	0.053	-.4382291	.0029007
Perception	.31888	.099958	3.19	0.002	.1220242	.5157357
Difficulty	.1515767	.0395218	3.84	0.000	.0737431	.2294103
Specificity	.079472	.0458571	1.73	0.084	-.0108382	.1697823
Fatigue_Awareness	.1515413	.0304957	4.97	0.000	.0914836	.2115991
Fatigue_Perception	-.0561451	.0270803	-2.07	0.039	-.1094766	-.0028135
_cons	4.674391	.5608474	8.33	0.000	3.569867	5.778915

The following model shows the regression model between risk preventive behaviour. motivation and perceived goal and perceived risk activation and their interaction with security fatigue.

```
. regress Motivation Fatigue perceived_goal perceived_risk fatigue_per_goal fatigue_per_risk
```

Source	SS	df	MS	Number of obs	=	261
				F(5, 255)	=	67.26
Model	68.9313308	5	13.7862662	Prob > F	=	0.0000
Residual	52.2702975	255	.204981559	R-squared	=	0.5687
				Adj R-squared	=	0.5603
Total	121.201628	260	.466160109	Root MSE	=	.45275

Motivation	Coefficient	Std. err.	t	P>|t|	[95% conf.	interval]
Fatigue	-.4587867	.1537802	-2.98	0.003	-.7616277	-.1559457
perceived_goal_activation	.3401589	.112411	3.03	0.003	.1187867	.561531
perceived_risk_activation	.0768496	.118632	0.65	0.518	-.1567737	.3104729
fatigue_per_goal	-.0360968	.0331959	-1.09	0.278	-.1014698	.0292763
fatigue_per_risk	.108977	.0360959	3.02	0.003	.0378929	.1800611
_cons	4.070027	.584289	6.97	0.000	2.91938	5.220673