sustainability

MDPI

Article

Developing and Validating a Behavioural Model of Cyberinsurance Adoption

Dawn Branley-Bell [1,*], Yolanda Gómez [2], Lynne Coventry [1], José Vila [2,3] and Pam Briggs [1]

[1] Department of Psychology, School of Life Sciences, Northumbria University, Newcastle upon Tyne NE1 8ST, UK; lynne.coventry@northumbria.ac.uk (L.C.); p.briggs@northumbria.ac.uk (P.B.)
[2] DevStat, 46005 Valencia, Spain; ygomez@devstat.com (Y.G.); jvila@devstat.com (J.V.)
[3] Intelligent Data Analysis Laboratory (IDAL), Center for Research in Social and Economic Behavior (ERI-CES), University of Valencia, 46022 Valencia, Spain
* Correspondence: dawn.branley-bell@northumbria.ac.uk

Abstract: Business disruption from cyberattacks is a growing concern, yet cyberinsurance uptake remains low. Using an online behavioural economics experiment with 4800 participants across four EU countries, this study tests a predictive model of cyberinsurance adoption, incorporating elements of Protection Motivation Theory (PMT) and the Theory of Planned Behaviour (TPB) as well as factors in relation to risk propensity and price. During the experiment, participants were given the opportunity to purchase different cybersecurity measures and cyberinsurance products before performing an online task. Participants likelihood of suffering a cyberattack was dependent upon their adoption of cybersecurity measures and their behaviour during the online task. The consequences of any attack were dependent upon the participants insurance decisions. Structural equation modelling was applied and the model was further developed to include elements of the wider security ecosystem. The final model shows that all TPB factors, and response efficacy from the PMT, positively predicted adoption of premium cyberinsurance. Interestingly, adoption of cybersecurity measures was associated with safer behaviour online, contrary to concerns of "moral hazard". The findings highlight the need to consider the larger cybersecurity ecosystem when designing interventions to increase adoption of cyberinsurance and/or promote more secure online behaviour.

Keywords: cybersecurity; cyberinsurance; protection motivation theory; theory of planned behaviour

Citation: Branley-Bell, D.; Gómez, Y.; Coventry, L.; Vila, J.; Briggs, P. Developing and Validating a Behavioural Model of Cyberinsurance Adoption. *Sustainability* **2021**, *13*, 9528. https://doi.org/10.3390/su13179528

Academic Editors: Lucia Porcu and Nuria Rodríguez-Priego

Received: 26 May 2021
Accepted: 16 August 2021
Published: 24 August 2021

1. Introduction

Cyberinsurance (sometimes also referred to as cyber risk or cyber liability insurance) is a form of insurance cover designed to protect an individual or business from digital threats (e.g., cyberattacks, hacking and data breaches). Cyberthreats can refer to intentional, malicious attacks or accidental breaches. Widespread cyberinsurance adoption has a number of potential benefits in a society facing increasing cybersecurity risk. Firstly, it could lead to market-based management of that risk by acting as a mechanism for spreading the risk amongst multiple stakeholders. Secondly, since obtaining insurance requires that certain cybersecurity standards are met, it could act as an incentive towards organisational investments in information security, which would reduce risk for the investing organisation and for their wider network. Here we are referring to additional protective behaviours that an individual or organisation can do to protect against cyber-risk (e.g., obtaining anti-virus software, installing regular security updates, using a firewall). In this sense, cyberinsurance and other security measures are complimentary goods. Thirdly, insurance investigators follow up on serious incidents to learn what went wrong, therefore uptake could also lead to data aggregation on best practices and better tools for assessing security—something that is currently lacking. In principle, a robust cyberinsurance offer could strengthen IT

security for society as a whole [1,2]. However, despite the growing risk of cyberattack, uptake of cyberinsurance as a mechanism to ameliorate risk (financial and otherwise) has not reached expectations, with some research reporting uptake rates as low as 10% in the UK [3].

There are also concerns around adverse selection and moral hazard in relation to insurance uptake. Adverse selection can occur if high risk individuals are more likely to adopt insurance policies than their lower risk counterparts. Adverse selection is possible when information asymmetries mean that the insurers are not fully aware of the risk level of the individual applying for an insurance policy, resulting in a premium that does not adequately reflect the insureds risk level [4]. In contrast, moral hazard refers to individuals increasing their exposure to risk (e.g., acting less cautiously) following adoption of insurance—due to feeling that they no longer personally bear the full costs of the risk as insurance coverage is in place [5]. More research is needed to identify whether these concerns are justified.

1.1. Theoretical Models

Recently, a number of studies have used traditional psychological models that define the relationships between attitudes, intentions and behaviours, to understand more about insurance uptake and/or information security protocol (ISP) compliance. There are three key theoretical models often applied in this field: the theory of planned behaviour (TPB), protection motivation theory (PMT) and general deterrence theory (GDT) [6,7]. The technology acceptance model (TAM) is also applied, but arguably not as often as the aforementioned [7].

In the context of ISP, TPB suggests that intention to comply with ISPs depends on the individual's overall evaluation of, and normative beliefs toward, compliant behaviour—including the degree to which they feel their compliance is within their control.

PMT suggests that an individual's attitude toward ISPs is shaped by the evaluation of two cognitive appraisals: threat appraisal and coping appraisal. Threat appraisal is dependent upon both the perceived severity of, and vulnerability to, a threatening event (e.g., security breach). Coping appraisal reflects the perceived efficacy of the recommended protective behaviour (i.e., ISP compliance) and the individual's perceived self-efficacy to implement this behaviour.

GDT states that individuals make rational decisions based upon weighing up the perceived severity of sanctions and perceived certainty of sanctions.

TAM states that an individual's intention to comply with ISP is predicted by the perceived usefulness and perceived ease-of-use of information security measures.

Within this field, published reviews consistently show the TPB is the most widely applied of the four models [6,7]. Described by Nasir et al. [7] as "the most dominant theory" with "the most significant main constructs in predicting and explaining employees' ISP compliance behavior" (p. 740). However, although TPB is the most prolific model in the field, that is not to say that its predictive ability cannot be improved. To further increase the explained variance, models are often combined. For example, Ifinedo's [8] widely cited study demonstrates that the inclusion of PMT constructs to the TPB model can increase explained variance in ISP compliance from 0.60 to 0.70. Ifinedo [8] suggests that "the fusion of both theoretical frameworks permits a better understanding of the sorts of factors that affect employees' ISP behavioural compliance as opposed to when each is used alone to investigate the theme" (p. 90). Similarly, Sommestad et al. [9] asked whether the TPB and/or PMT are sufficient to account for cybersecurity policy compliance in employees. They concluded that both models do a "fairly good job at prediction intentions and behaviour" (pp. 14–15), but also noted that the regression model of the TPB could be improved by the addition of threat appraisal constructs from PMT.

PMT covers similar factors to the two of the other more popular models: GDT and TAM. For example, threat appraisal can also include the threat of sanctions (as per GDT), and coping appraisal includes both the perceived efficacy of the protective behaviour

and self-efficacy (which has similarities to the TAM constructs of perceived usefulness and ease-of-use). For this reason, and to keep within the scope of this research, TPB and PMT were chosen as the two models to be applied. We describe these two models below, outlining their putative relationship to cyberinsurance uptake and then go on to a more careful critique of the predictive power of their constituting factors. We use this information to develop a hypothetical research model for cyberinsurance adoption.

1.1.1. Protection Motivation Theory

PMT was originally designed to explain engagement in protective actions in relation to health-related behaviours (Figure 1) [7]. However, as noted earlier, the theory has since been applied to the explanation of other protective actions, including uptake of insurance [10–13] and the adoption of secure online behaviours [14,15]. PMT proposes that people protect themselves by making both a threat appraisal and a coping appraisal. The threat appraisal is dependent upon both the perceived severity of a threatening event (in this instance a cyberattack) and the perceived vulnerability to the event (i.e., the perceived probability of that event occurring). The coping appraisal reflects the perceived efficacy of the recommended protective behaviour (cyberinsurance in this case) and the individual's perceived self-efficacy (e.g., their ability to successfully implement the requirements for a cyberinsurance policy). To explain: an individual considering whether to invest in cyberinsurance may firstly weigh up the likelihood that they will receive a cyberattack of a particular severity against (a) the cost of taking out cyberinsurance (finances, time, effort) and (b) how effective they believe that insurance will be (response efficacy) and/or how much confidence they have in their own ability to put insurance measures into place (self-efficacy).

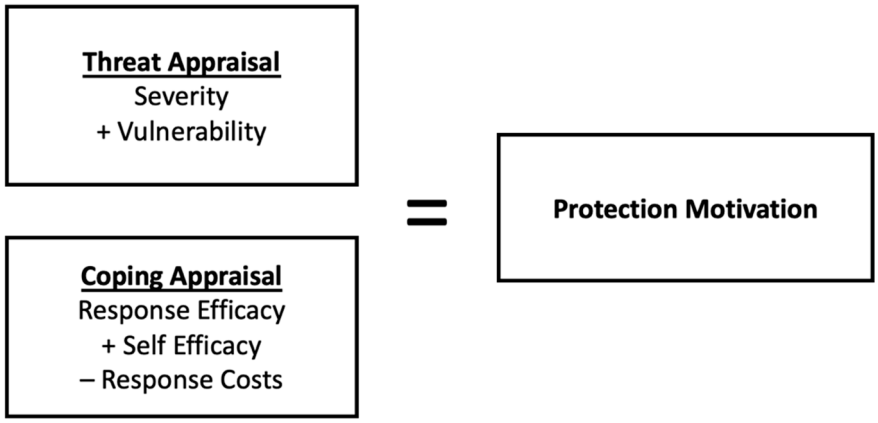

Figure 1. Protection motivation theory.

1.1.2. Theory of Planned Behaviour

TPB highlights additional factors which may influence insurance purchase decisions. TPB states that intention to perform a behaviour is the most immediate and important determinator of behaviour (although perceived control has also been shown to influence behaviour directly, as represented by the dashed line in Figure 2) [16,17]. Intention is influenced by the individual's attitude(s) towards the behaviour, subjective norm(s) and perceived control over the situation. Brahmana et al. [18] applied the TPB to explore intention to purchase health insurance. The TPB suggests that strengthening positive attitudes towards cyberinsurance (e.g., strengthening the belief that insurance companies would pay out in the event of a cyber-incident) could increase cyberinsurance uptake. Likewise strengthening perceived subjective norms around cyberinsurance may help to increase uptake (e.g., strengthening the perception that others believe cyberinsurance to be a worthwhile product). Perceived self-efficacy from PMT and perceived behavioural control from TPB are thought to measure the same construct [8].

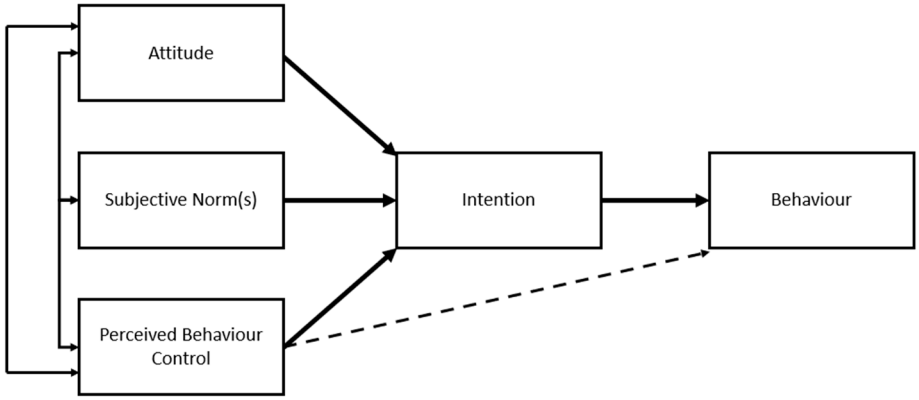

Figure 2. Theory of planned behaviour.

1.2. Our Research Model

Although widely used, these models are not without criticism. A systematic review by ENISA [19] found that the coping elements of PMT and the TPB were useful (p. 11), but questioned the predictive value of threat models, including PMT's threat appraisal. This is curious when we consider that Sommestad et al. [9] found added predictive value in the threat component, and concluded that no single PMT variable was able to explain more than a small portion of the variance within the studied populations. This in line with the underlying idea of PMT, which describes how six variables together determine intentions through cognitive processes. Sommestad et al. suggested that inconsistencies in how constructs are measured could lead to the discrepancy between studies (p. 15). We should also bear in mind that for the aforementioned systematic review by ENISA, the search terms included cybersecurity items but did not include "security" or "information security policy", therefore missing some of the studies cited above. That said, other recent work has also suggested that coping elements offer greater value than threat elements when trying to predict or improve online security behaviour [14].

Based on the existing literature, we feel confident in the hypothesis that the coping appraisal factors should be influential, but we are less certain about the predictive power of the threat appraisal components. In drawing up our hypothetical research model for the adoption of cyberinsurance (Figure 3), we have included all of the PMT factors (threat appraisal: perceived severity, perceived vulnerability; coping appraisal: response efficacy, self-efficacy, response costs) and TPB factors (attitudes and subjective norms) but have noted where the hypothesised links are weaker, indicating these by dashed lines in the model.

There are three other elements in our research model: risk propensity, insurance pricing strategy, and attack intentionality. We provide the rationales for including each of these elements below:

Firstly, we include risk propensity (sometimes referred to as risk preference or risk tolerance). Previous insurance research has shown that risk adverse individuals are more likely to purchase flood insurance [11,13], health insurance and life insurance [20,21]. This makes sense since insurance represents a means of risk mitigation. In our study we measure risk propensity using the seven item risk propensity scale [22] with the hypothesis that individuals who are more risk adverse would be more likely to purchase insurance, whereas individuals who are more willing to take risks may be less inclined to adoption of premium insurance.

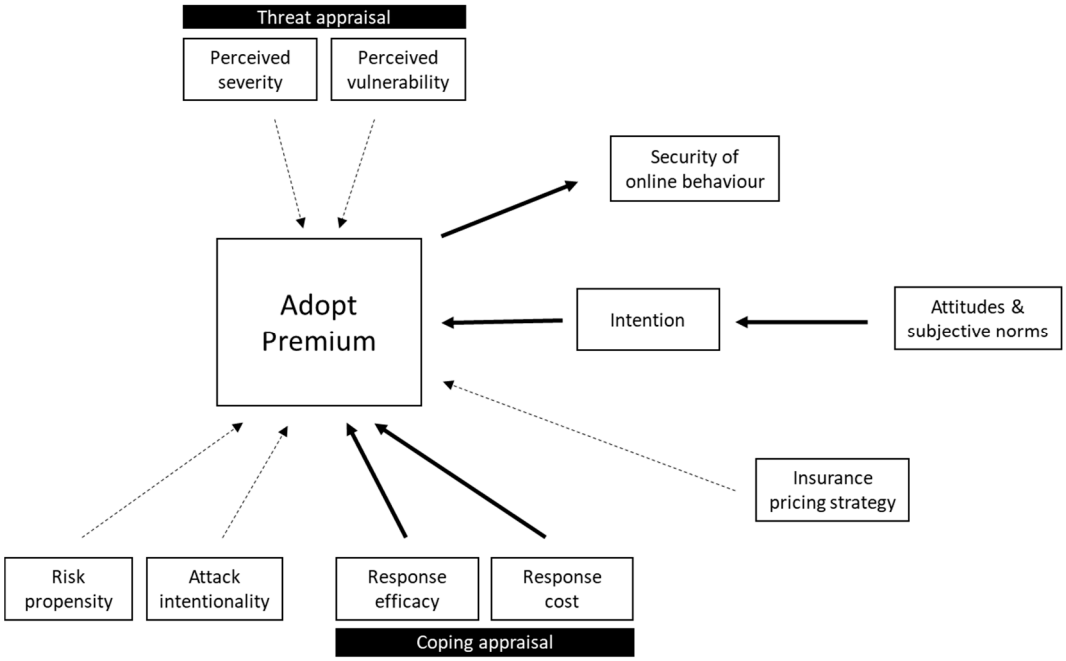

Figure 3. The research model. Strong hypothesised links are shown as solid lines. Weaker or less supported hypothesised links are shown as dashed lines.

Secondly, we include a factor that takes the insurance pricing strategy into account. Cyberinsurance is likely to adopt a heterogeneous pricing model, in part because the measures companies take to mitigate threats will vary. Under such circumstances, consumer perceptions about what price is reasonable and fair will vary, but are likely to influence willingness to adopt both protective measures (e.g., antivirus software, firewalls) and a premium insurance product [23]. Insurers will also want to reduce systemic risk (also known as correlated or aggregate risk) across their portfolio to avoid catastrophic losses that may arise from the interdependencies of networked organisations. Khalili et al. [24] have suggested that this can be partly achieved by setting the price to incentivised purchase of premium insurance products that themselves may be contingent upon the company's security posture. In terms of our own research model, we manipulated price to be either dependent or independent of the security measures in place (i.e., in the dependent category price of the insurance policy varied dependent upon the cybersecurity measures the individual had opted for). This is referred to as the insurance pricing strategy in Figure 3. This allowed an empirical assessment of the extent to which making insurance premiums contingent upon a company's security posture would improve or limit cyberinsurance uptake.

Thirdly, we added one further factor, Attack intentionality, relating to the context of a cyberattack, i.e., whether an attack is targeted or random [25], something explicitly recommended in the ENISA review [19]. This factor relates to a literature on cyber-risk communication [26] which shows that users are more likely to be persuaded by messages which describe their particular vulnerability to an attack, but also relates to a literature on the efficacy of targeted risk communication in order to nudge cybersecurity behaviour [27]. Our hypothesis is that risk framed in terms of an intentional, targeted attack will be more likely to result in the adoption of premium cyberinsurance.

1.3. The Value of Behavioural Data

The majority of existing studies into cybersecurity behaviours have relied upon self-reported measures rather than measuring actual behaviour [19]. Unfortunately, self-reporting does not always correlate with actual behaviour [28] and this has become something of a thorny problem for large-scale survey studies of ISP [6]. To address this, we

applied a behavioural economics experiment approach. This novel approach provides a scientific method to study how individuals interact within a controlled setting and enables the collection of behavioural data. In doing so, we also help to address some of the concerns identified by Botzen and van den Bergh [29] who noted that "measuring risk attitudes and risk perception at the individual level and estimating their influence on insurance demand, [. . .] is rarely possible in actual insurance decisions and has hardly been addressed in empirical work" (p. 152). With this in mind, our study analyses direct behavioural data, in combination with relevant attitude scales, to test our predicted model of cyberinsurance adoption. Mol, Botzen, and Blasch [30] applied a similar approach to investigate factors underlying uptake of insurance by home-owners in flood-risk areas. However, to the best of our knowledge this is the first study to apply an experimental, behavioural economics approach to understand decision-making in relation to cyberinsurance.

2. Materials and Methods

2.1. Sample and Recruitment

Participants (N = 4800) were recruited across four EU countries (Germany, Spain, Poland and UK) in June 2018 using an online panel. Participants were contacted online and invited to participate in the experiment. After informed consent, they were provided with a link to access the experimental software.

Participants ranged from 16–74 years of age (Table 1). Distribution by age and gender reflects Eurostat's data from the 2017 survey on ICT (Data given in this domain are collected annually by the National Statistical Institutes and are based on Eurostat's annual model questionnaires on ICT (Information and Communication Technologies) usage in households and by individuals. https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm, accessed on 10 May 2018) that was used to create the quota (a sample design that has been applied in previous research [14,31]). Most participants (91.6%) were educated to high school level or above. We present the data using two age division categories (16–34 years and 35–74 years), Greater age categorisation would not be appropriate for the sample size and as we do not present analysis per country—any differences in age distribution per country is not expected to affect the experimental results.

Table 1. Distribution of the participants by gender, age and country.

		Germany (*n* = 1200)		**Spain (*n* = 1200)**		**Poland (*n* = 1200)**		**UK (*n* = 1200)**	
		n	%	*n*	%	*n*	%	*n*	%
Gender	Male	617	51.42	600	50.00	552	46.00	595	49.58
	Female	583	48.58	600	50.00	648	54.00	605	50.42
Age	16–34 y	932	77.67	842	70.17	713	59.42	844	70.33
	35–74 y	268	22.33	358	29.83	487	40.58	356	29.67

2.2. Experimental Design and Procedure

An online behavioural economic experiment (BEE) was designed and implemented to measure participants' cybersecurity decisions in a controlled situation. The experimental design, including the form to ask for informed consent for participation, the experimental tasks and interventions and data management and analysis, was presented to the Ethical Committee of CYBECO, which considered that the proposed research protocols fully comply with the principles of the Declaration of Helsinki (1989), Universal Declaration of Human Rights (UNESCO, 1948) and the Agreement for the Human Rights Protection in Biology and Biomedicine (Oviedo, 1997) and approved them. The experiment is mainly composed of two tasks:

(i) Purchase decisions about cyberinsurance and security measures products (cybersecurity strategy);
(ii) Online behaviour whilst performing an online task.

The instructions clearly explained all tasks and decisions to be made during the experiment and their implications. Figure 4 shows the experiment blueprint.

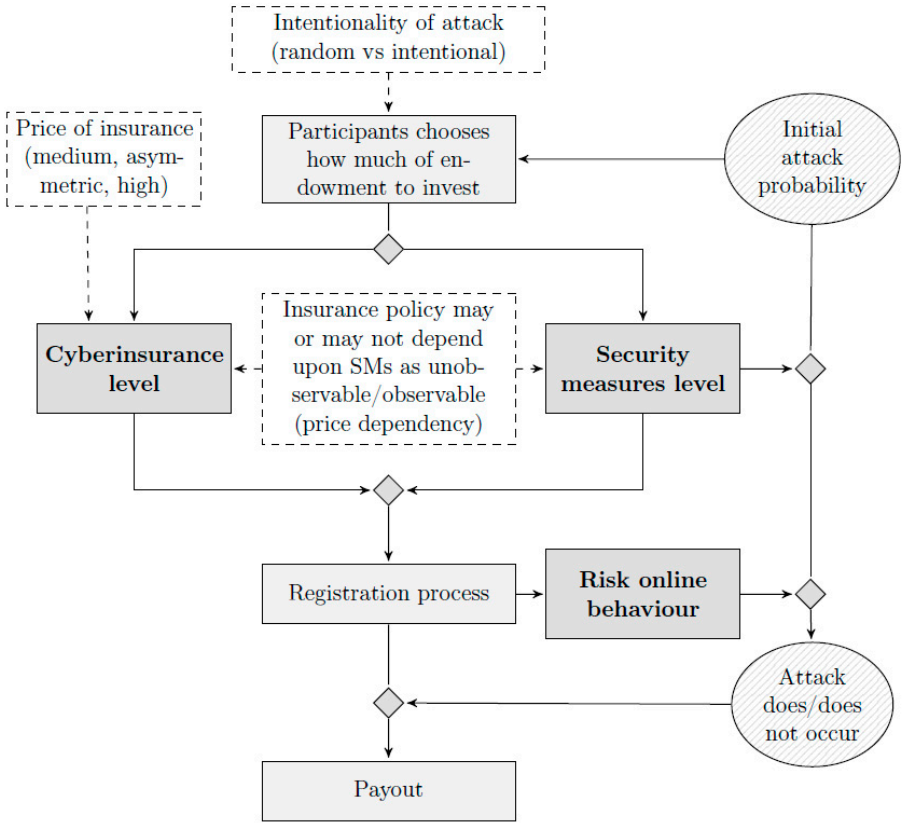

Figure 4. Experimental blueprint (SM = security measures).

Specifically, at the start of the experiment, each participant was provided with an initial endowment of 650 virtual coins (VC). They were informed that they could exchange VCs for Euros at the end of the experiment. Each participant was then informed that they were at risk of a possible cyberattack, which if suffered would have a detrimental impact on the value of their commercial data and therefore lower the variable payment they would receive at the end of the experiment. Depending on the experimental condition, participants were informed whether the possible cyberattack was random (i.e., randomly selecting targeted individuals/companies on the internet) or intentional (i.e., a hacker launching attacks targeting companies like theirs). After being provided with this information, participants were asked to visit an online "shop" (see Figure 5), where they were asked to make two decisions: 1. Whether to opt for basic or advanced security measures, and 2. Whether to opt for no insurance, basic insurance or premium insurance.

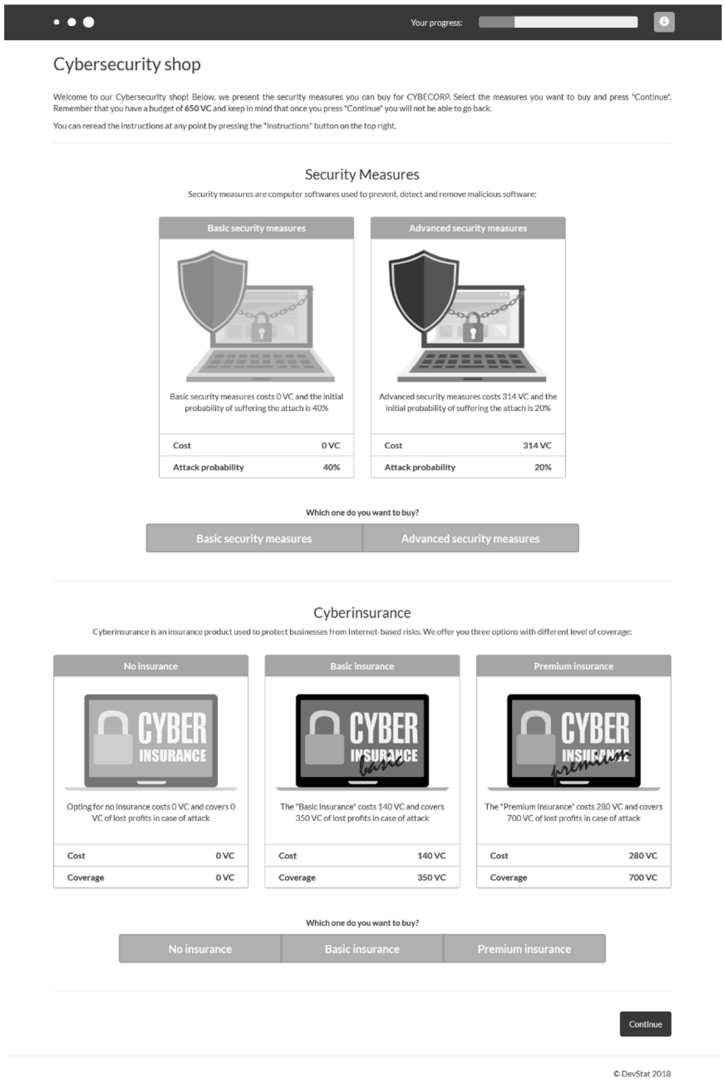

Figure 5. Mock-up online shop.

Note that the online shop presented participants with explicit information about the way that purchases would either reduce the likelihood of an attack (when buying security measures) or provide financial recompense in the event of an attack (in the case of cyberinsurance). The exact information shown to participants in shown in Figure 5, and summarised in Table 2. Depending on the condition to which they were allocated, the price of the insurance policy may or may not be dependent on the security measures chosen (i.e., in the dependent condition, the price of the insurance policy would decrease as level of security measures increases, with the cheapest price for individuals who opted for advanced security measures. In the independent condition, the price of the insurance did not alter regardless of the security measures chosen).

Table 2. Experimental purchase decisions and impact on attack probability and financial coverage (VC = virtual coins).

Factor/Decision	Levels	Price (VC, Deducted from Endowment)	Impact
Security Measures	Basic	0	Attack probability = 40%
	Advanced	314	Attack probability = 20%
Insurance	None	0	Financial amount insured = 0 VC
	Basic	140	Financial amount insured = 350 VC
	Premium	280	Financial amount insured = 700 VC

After making their purchases in the online shop, participants were then asked to complete an online task which involved registering for a conference. During the task, their possibility of suffering a cybersecurity attack was increased or decreased depending upon the security of their online behaviour. The security of their online behaviour was calculated using four behavioural measures obtained whilst participants were completing the online task: i. The strength of their chosen password, ii. Whether they logged out after the task, iii. Whether they read the website terms and conditions before registering, and iv. whether they disclosed any non-compulsory private information during the transaction. The final score was calculated as a continuous variable (The risk level is computed from the following binary variables, which are equal to 1 if they verify the following statements or 0 otherwise: Password, x_i^{pass} : Password does not contain capital letters; Password does not contain lowercase letters; Password does not contain numbers; Password does not contain special characters (['^£$%&*()}{@#~?><>,|=_+¬-]); Password is short (less than 8 characters); Password includes the username (case-insensitive). Registration, x_i^{reg}: The participant has filled the "First name" field; The participant has filled the "Last name" field; The participant has filled the "Occupation" field; The participant has filled the "Phone Number" field; The participant has filled the "Address" field; The participant has filled the "City" field; The participant has filled the "Zip" field. Privacy policy, x_i^{pp}: The participant has not opened the "Privacy Policy" window. Log out, x_i^{log}: The participant has not logged out of the website after the registration. The security level, RL, is obtained as a weighted average of the above variables: $RL = w_{pass} \sum_{i=1}^{6} x_i^{pass} + w_{reg} \sum_{i=1}^{7} x_i^{reg} + w_{pp} x^{pp} + w_{log} w^{log}$. Where w represents the weight of eachbinary variable, given by $w_{pass} = 0.4 \cdot 1/6$, $w_{reg} = 0.3 \cdot 1/7$, $w_{pp} = 0.15$ and $w_{log} = 0.15$.) between 0 (safest behaviour) and 1 (riskiest behaviour).

Following their completion of the conference registration task, participants were then informed whether they had, or had not, suffered a cyberattack and informed of their final payout. As detailed above, the final payment was influenced by the participants cybersecurity and cyberinsurance decisions, and whether they did, or did not, suffer a cyberattack (with the probability of the latter influenced by their security purchases and their online behaviour).

Following completion of the economic experiment, participants were presented with an online questionnaire measuring factors relating to the two psychological models (PMT & TPB).

2.3. Experimental Conditions

Participants were randomly allocated to one of 12 experimental conditions. The conditions are based on two experimental manipulations: Attack intentionality and Insurance pricing strategy.

Attack intentionality had two levels: Intentional attack (participants are informed that an attacker may specifically target their company) and random attack (participants are informed that there is a virus in the Internet that may randomly affect any user).

Insurance pricing strategy had six levels obtained from the combination of three different prices (low, medium, high) and two different relationships between the prices of the security measures and insurance policies (dependent price—i.e., the price of the insurance policy decreases if advanced cybersecurity measures are chosen, and independent price, i.e., the price of the insurance policy remains the same regardless of whether the participant opted for none, basic or advanced security measures).

2.4. Psychological Measures

Following completion of the experiment, participants were presented with an online questionnaire measuring factors relating to PMT: perceived severity, perceived vulnerability, response efficacy, response cost and self-efficacy. In addition to the PMT items, two other measures were included to fit with the TPB: attitudes towards insurance and subjective norms. The measure for attitudes towards insurance was based upon Anderson and Agarwal's [32] measure of attitudes toward security-related behaviour, amended to apply

specifically to insurance. While subjective norms were measured using the single item "People who are important to me think that I should have insurance". All PMT and TPB items were scored on a 5-point scale from strongly disagree (1) to strongly agree (5).

The final two measures related to risk propensity (an individual's natural tendency to take risks) and intention to purchase insurance. Risk propensity was measured using the risk propensity scale (RPS) [22]. This 7-item scale has been used to measure risk propensity in relation to online behaviour [33] and requires considerably less space than the other commonly used, but lengthy, domain-specific risk-taking scale [34]. The specific items used are shown in Table 3.

Table 3. Instrument items.

Construct	Items
Perceived Severity	If my online data/accounts were hacked, it would be severe
Perceived Vulnerability	a. My online data/accounts are at risk of being compromised b. It is likely that my online data/accounts will be breached c. It is possible that my online data/accounts will be compromised
Response Efficacy	a. Insurance is an effective method to protect against loss b. Insurers can be trusted to pay out in the event of a claim
Self-efficacy/Perceived Behavioural Control	a. I feel comfortable taking measures to secure my own computer(s) b. I feel comfortable taking security measures to limit the threat to other people and the Internet in general c. Taking the necessary security measures is entirely under my control d. I have the resources and the knowledge to take the necessary security measures e. Taking the necessary security measures is easy
Response Cost & Rewards	a. Insurance is financially costly for me b. Setting up insurance would require too much from me c. Insurance is burdensome for me d. Insurance is time consuming for me e. Insurance is not worth it f. Claiming on insurance could harm a business/organisations reputation
Attitudes	a. Insurance is a good idea b. Insurance is important c. I like the idea of taking out insurance to protect me
Subjective Norms	People who are important to me think that I should have insurance
Risk propensity	a. Safety first b. I do not take risks with my health c. I prefer to avoid risks d. I take risks regularly e. I really dislike knowing what is going to happen f. I usually view risks as a challenge g. I view myself as a . . . [risk avoider vs. risk seeker]
Intention	I am likely to purchase cyber insurance

2.5. Analysis

Preliminary analysis was carried out to confirm that the data was suitable for structural equation modelling (SEM). Correlation coefficients were used to examine relationships between all the variables. The structural model was tested using R (packages psych, semTools and lavaan). SEM is a method that combines and estimates two procedures

simultaneously: confirmatory factor analysis (CFA) and path analysis. CFA assesses the measurement component of the model, and path analysis assesses the relationship between latent variables [35]. SEM allows us to include numerous endogenous variables and also to control for systematic and random measurement error [36].

3. Results

3.1. Descriptive Statistics for Behavioural Measures

The majority (83.4%) of participants opted for a high level of protection by purchasing the advanced security measures, and 93% decided to purchase cyberinsurance. The descriptive statistics are shown in Table 4.

Table 4. Descriptive statistics.

	Levels	***n***	**%**
Security Measures	Basic	797	16.6
	Advanced	4003	83.4
Insurance	None	336	7.0
	Basic	2054	42.8
	Premium	2410	50.2

As only 7% of participants did not opt for any cyberinsurance, we collapsed the 'no insurance and basic insurance' categories and focused upon modelling the adoption of premium insurance in subsequent analyses.

3.2. Measurement Model Analysis

Using exploratory factor analysis, a test of reliability was conducted for each construct. During this analysis, items for attitudes and subjective norms loaded on the same factor and therefore were combined in the subsequent analyses. Some items of response cost (Table 3: Items a, e, f) and risk propensity (item e) were eliminated to improve construct reliability.

Means, standard deviations, and Cronbach's alpha scores for the remaining constructs are shown in Table 5. All Cronbach's alpha scores are greater than 0.7 indicating good reliability [37,38].

Table 5. Construct means, variances, and Cronbach's alpha (α) scores.

	M	**SD**	**α**
Perceived vulnerability	3.5	0.95	0.86
Response efficacy	3.5	1.00	0.74
Perceived behavioural control	3.7	0.78	0.84
Response cost	3.0	0.85	0.83
Attitudes & Subjective norms	3.8	0.84	0.87
Risk propensity	3.5	1.30	0.74

3.3. Structural Equation Modelling

The SEM model for premium cyberinsurance adoption is shown in Figure 6. Solid lines represent significant pathways ($p < 0.05$). There are four significant pathways influencing premium insurance adoption: Perceived response efficacy and the TPB pathway (social norms and attitudes, via intention) both positively influence premium insurance adoption. Whilst, risk propensity and insurance pricing strategy negatively influence premium insurance adoption. Attack intentionality does not appear to have any significant effect upon adoption.

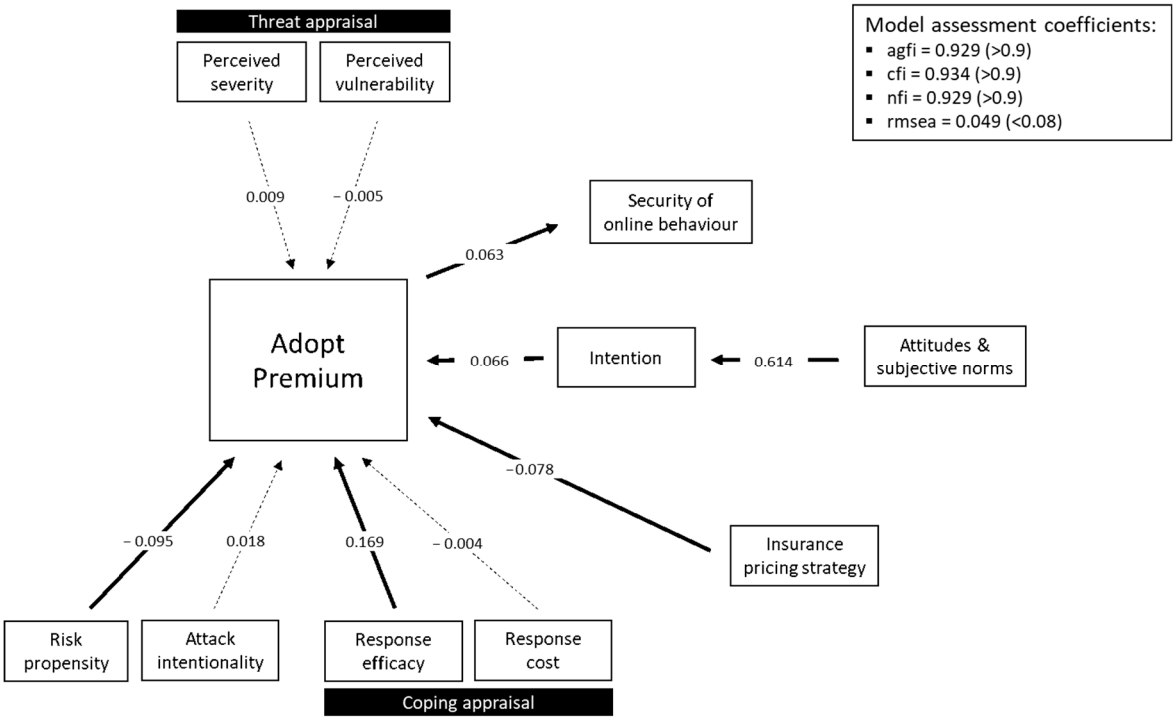

Figure 6. SEM model of cyberinsurance adoption (standardised coefficients).

Adoption of premium insurance also shows a positive relationship with secure online behaviour. However, it is important to note that the decision to purchase cyberinsurance does not usually occur in isolation—it is likely to coincide with the decision to purchase additional security measures (e.g., antivirus, firewalls). This is further reinforced by the likelihood that insurance companies will require a minimum level of security before insurance will be granted. Therefore, a second model was created which includes the purchase of security measures—shown in Figure 7.

The second model shows a significant positive pathway that links the adoption of advanced security measures to the adoption of premium insurance. Thus, individuals who adopted advanced security measures were more likely to also adopt premium insurance. This is the strongest pathway in the model. The adoption of advanced security measures was also significantly positively related to security of online behaviour; those who adopted advanced security measures were also more likely to behave securely online. The pathway between insurance adoption and online behaviour, although positive, failed to reach significance once adoption of security measures was introduced into the model.

Response efficacy (part of PMT coping appraisal) and the TPB factors (attitudes and norms) were positively related to adoption of premium insurance, i.e., those who perceived insurance to be more effective, and those who had positive attitudes and positive subjective norms, were more likely to adopt premium cyberinsurance. Perceived self-efficacy and perceived threat severity (part of PMT threat appraisal) both positively fed into the adoption of advanced security measures rather than adoption of premium insurance directly. Those who had higher perceptions of their ability to put cybersecurity measures into place, and those who perceived the threat of the cyberattack as more severe, were more likely to adopt advanced security measures (which as aforementioned then subsequently fed into premium insurance adoption).

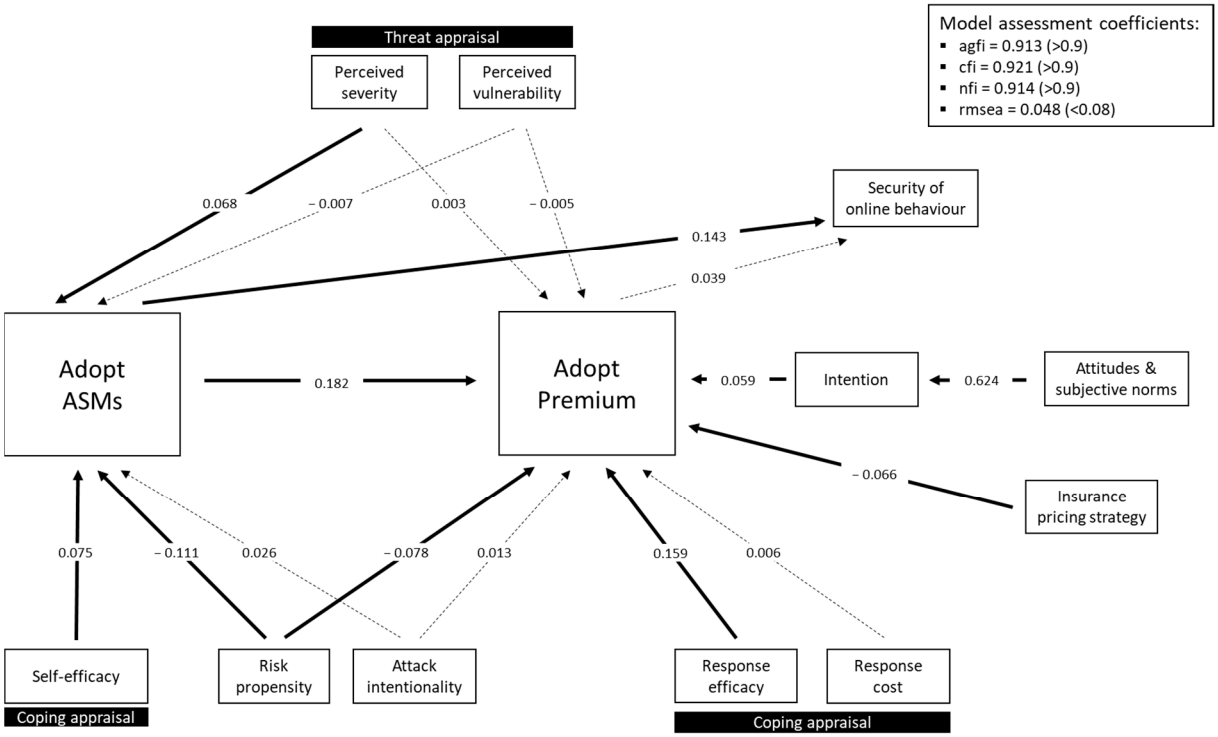

Figure 7. SEM model including security measure adoption (standardised coefficients).

Risk propensity was negatively related to both adoption of security measures and adoption of insurance, i.e., a risk-seeking individual was less likely to adopt advanced security measures and premium insurance.

As found in the first model, attack intentionality (i.e., targeted vs. random) had no significant effect upon insurance adoption, nor upon purchase of security measures.

4. Discussion

The current study used SEM to test a model of cyberinsurance adoption and address a significant gap in the existing literature. Despite a fast-growing interest in, and industry around, cybersecurity—there is an overwhelming lack of knowledge in relation to understanding the mechanisms behind cybersecurity decision-making. The results support the model as a good fit to the data therefore providing important knowledge of the factors influencing cybersecurity decisions—including uptake of security measures and insurance.

Our findings highlight that cyberinsurance adoption is only one factor in a larger, more complex security ecosystem. The decision to adopt premium cyberinsurance was directly influenced by the adoption of other advanced security measures i.e., those who invested in advanced security measures were more likely to also purchase premium insurance. Interestingly, adoption of advanced security measures was also predictive of more secure online behaviour. Suggesting that concerns over moral hazard (i.e., that an individual may increase their exposure to risk if they do not bear the full costs of that risk) may be unfounded. On a related note, our results suggest that risk-seeking individuals are less likely to adopt advanced security measures and premium cyberinsurance—which suggests that concerns over adverse selection may also be unfounded.

The adoption of advanced security measures was positively influenced by perceived severity of an attack and perceived self-efficacy (i.e., confidence in one's own ability to implement security measures). Again, risk propensity was negatively related to adoption, with risk-seeking individuals being less likely to adopt security measures.

Taken together, the findings suggest that, in order to adequately target insurance uptake, it is important to account for the wider portfolio of security measures available to an individual or organisation. It is also vital that future research accounts for this

interdependency between insurance and security measures. This conclusion is entirely consistent with the ENISA [19] recommendations for organisational contexts to be more carefully considered.

Outside of security measure adoption, uptake of premium insurance was negatively influenced by risk propensity and insurance pricing strategy, and positively influenced by response efficacy, and positive attitudes and social norms. These results are relatively unsurprising: individuals with a higher propensity for risk were less likely to adopt premium insurance, and an insurance pricing strategy based on higher premium policy pricing (comparative to basic insurance) led to lower premium insurance uptake. In keeping with PMT, those who perceived insurance to be an effective method to protect against loss were more likely to adopt premium insurance; and in line with TPB, positive attitudes towards insurance (e.g., perceiving insurance as a good thing) and strong social norms (i.e., perceptions that other people think they should have cyberinsurance) were linked with intention to adopt premium insurance.

Interestingly, perceived vulnerability (one element of PMT threat appraisal) was not a significant predictor of advanced security measures or premium insurance adoption. Attack intentionality, also thought to relate to perceptions of vulnerability, was also non-significant. These are troubling findings for the appropriateness of PMT for explaining cyber-risk, and beg the question as to why perceived severity of an attack (the other element making up PMT threat appraisal) may be influential, but perceived vulnerability less so. To a certain extent, this adds to the existing debate, described earlier, around the limited value of the "threat assessment" component in predicting cybersecurity behaviours. PMT, like so many behaviour-change models, was largely developed as a means of understanding health behaviours, where the health threats are experienced at a personal level and where vulnerability can clearly be understood in personal terms. For cybersecurity, this connection is sometimes broken and whilst participants might be able to understand the severity of an attack in general terms, their own vulnerability to an attack can remain uncertain. It is also possible that threat factors may be sensitive to demographic differences such as age, gender or country, that are outside of the scope of this study, but that could be explored in future work.

The weak influence of perceived vulnerability may also be exacerbated in an experimental study such as this. Behavioural economics experiments have a good track record of capturing real world, policy-relevant behaviours [39] and the use of incentives, as in the current study, is also a well-validated method used to help enhance the ecological validity of the experiment [39,40]. However, vulnerability judgements require an assessment of the likelihood that a particular organisation will succumb to a threat, but in our experimental set up, little is offered in the way of organisational context to help make this assessment. True, we sought to manipulate context by describing the threat as either targeted or not, but we provided no background information as to the resilience of the organisation at the start of the study. Simply put, how could our participants determine vulnerability? This is worth considering in future studies and indeed such experimental effects may help to account for the ENISA report [19] observation that threat information tends to be relatively ineffective in driving behaviour. That said, this study still helps to address the relative lack of experimental approaches to cybersecurity behaviour; of which there are even fewer that combine subjective and objective measures (despite some evidence that hybrid approaches may provide a useful new source of evidence around cybersecurity and cyberinsurance behaviours [14,41]).

5. Conclusions

In this study we identified the key factors underlying decision-making around cybersecurity. The model presented here, which combines factors from PMT and TPB, could be used to guide future interventions aimed at increasing cyberinsurance (and cybersecurity) uptake. Our findings show that it is vital to consider the larger cybersecurity ecosystem, rather than attempting to focus upon insurance adoption in isolation (as insurance uptake

appears to be directly influenced by adoption of other security measures). This focus upon the wider ecosystem could help to improve societal cybersecurity, although we note that context rich studies of cybersecurity remain limited. Positively, our findings suggest that individuals who invest in cybersecurity may tend to be more risk adverse, which may help to abate insurers concerns around moral hazard and adverse selection.

Our study also adds to existing debates around the usefulness of the threat appraisal elements of the PMT model (e.g., [14,19]), by suggesting that the coping appraisal elements may be more influential when applying the model in this space.

Author Contributions: Conceptualisation, D.B.-B., Y.G., L.C., J.V. and P.B.; data curation, Y.G. and J.V.; formal analysis, Y.G. and J.V.; funding acquisition, J.V. and P.B.; investigation, D.B.-B., Y.G., J.V. and P.B.; methodology, D.B.-B., Y.G., J.V. and P.B.; project administration, J.V. and P.B.; Resources, D.B.-B., Y.G. and J.V.; software, Y.G. and J.V.; supervision, J.V. and P.B.; validation, D.B.-B., Y.G., J.V. and P.B.; visualisation, D.B.-B. and Y.G.; writing—original draft, D.B.-B.; writing—review and editing, D.B.-B., Y.G., L.C., J.V. and P.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union's Horizon 2020 research and innovation programme under the CYBECO grant agreement No 740920.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Ethics Committee of DevStat (protocol code DVS03) on 30 April 2018.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data is available at: [CYBECO-WP6_Exp1_data.xlsx] Yolanda Gomez, Jose Vila, Dawn Branley-Bell, Pam Briggs. 2019. H2020 CYBECO WP6—Behavioural-Experimental Analysis of Cyber Insurance Tools; ZENODO; doi:10.5281/zenodo.3240473.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Baer, W.S.; Parkinson, A. Cyberinsurance in IT Security Management. *IEEE Secur. Priv. Mag.* **2007**, *5*, 50–56. [CrossRef]
2. Kuru, D.; Bayraktar, S. The effect of cyber-risk insurance to social welfare. *J. Financ. Crime* **2017**, *24*, 329–346. [CrossRef]
3. Low, P. Insuring against cyber-attacks. *Comput. Fraud Secur.* **2017**, *2017*, 18–20. [CrossRef]
4. Cohen, A.; Siegelman, P. Testing for Adverse Selection in Insurance Markets. *J. Risk Insur.* **2010**, *77*, 39–84. [CrossRef]
5. Dwyer, R.E. Expanding Homes and Increasing Inequalities: U.S. Housing Development and the Residential Segregation of the Affluent. *Soc. Probl.* **2007**, *54*, 23–46. [CrossRef]
6. Lebek, B.; Uffen, J.; Neumann, M.; Hohler, B.; Breitner, M.H. Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev.* **2014**, *37*, 1049–1092. [CrossRef]
7. Nasir, A.; Arshah, R.A.; Ab Hamid, M.R. The Significance of Main Constructs of Theory of Planned Behavior in Recent Information Security Policy Compliance Behavior Study: A Comparison among Top Three Behavioral Theories. *Int. J. Eng. Technol.* **2018**, *7*, 737–741. [CrossRef]
8. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **2012**, *31*, 83–95. [CrossRef]
9. Sommestad, T.; Hallberg, J.; Lundholm, K.; Bengtsson, J. Variables influencing information security policy compliance. *Inf. Manag. Comput. Secur.* **2014**, *22*, 42–75. [CrossRef]
10. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol.* **1975**, *91*, 93–114. [CrossRef] [PubMed]
11. Dittrich, R.; Wreford, A.; Butler, A.; Moran, D. The impact of flood action groups on the uptake of flood management measures. *Clim. Chang.* **2016**, *138*, 471–489. [CrossRef]
12. Beck, K.H. The Effects of Risk Probability, Outcome Severity, Efficacy of Protection and Access to Protection on Decision Making: A Further Test of Protection Motivation Theory. *Soc. Behav. Personal. Int. J.* **1984**, *12*, 121–125. [CrossRef]
13. Grahn, T.; Jaldell, H. Households (un)willingness to perform private flood risk reduction—Results from a Swedish survey. *Saf. Sci.* **2019**, *116*, 127–136. [CrossRef]
14. van Bavel, R.; Rodríguez-Priego, N.; Vila, J.; Briggs, P. Using protection motivation theory in the design of nudges to improve online security behavior. *Int. J. Hum. Comput. Stud.* **2019**, *123*, 29–39. [CrossRef]

15. Tsai, H.-Y.S.; Jiang, M.; Alhabash, S.; LaRose, R.; Rifon, N.J.; Cotten, S.R. Understanding online safety behaviors: A protection motivation theory perspective. *Comput. Secur.* **2016**, *59*, 138–150. [CrossRef]
16. Ajzen, I. From Intentions to Actions: A Theory of Planned Behavior. In *Action Control*; Springer: Berlin/Heidelberg, Germany, 1985. [CrossRef]
17. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. [CrossRef]
18. Brahmana, R.; Brahmana, R.K.; Memarista, G. Planned Behaviour in Purchasing Health Insurance. *South East Asian J. Manag.* **2018**. [CrossRef]
19. ENISA. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*; ENISA: Attiki, Greece, 2018.
20. Barsky, R.B.; Juster, F.T.; Kimball, M.S.; Shapiro, M.D. Preference Parameters and Behavioral Heterogeneity: An Experimental Approach in the Health and Retirement Study. *Q. J. Econ.* **1997**, *112*, 537–579. [CrossRef]
21. Pierre, A.; Jusot, F. The likely effects of employer-mandated complementary health insurance on health coverage in France. *Heallth Policy* **2017**, *121*, 321–328. [CrossRef]
22. Meertens, R.M.; Lion, R. Measuring an Individual's Tendency to Take Risks: The Risk Propensity Scale. *J. Appl. Soc. Psychol.* **2008**, *38*, 1506–1520. [CrossRef]
23. Pal, R.; Golubchik, L.; Psounis, K.; Hui, P. Security Pricing as Enabler of Cyber-Insurance A First Look at Differentiated Pricing Markets. *IEEE Trans. Dependable Secur. Comput.* **2017**, *16*, 358–372. [CrossRef]
24. Khalili, M.M.; Liu, M.; Romanosky, S. Embracing and controlling risk dependency in cyber-insurance policy underwriting. *J. Cybersecur.* **2019**, *5*, 5. [CrossRef]
25. Insua, D.R.; Couce-Vieira, A.; Rubio, J.A.; Pieters, W.; Labunets, K.; Rasines, D.G. An Adversarial Risk Analysis Framework for Cybersecurity. *Risk Anal.* **2021**, *41*, 16–36. [CrossRef] [PubMed]
26. Blythe, J.; Camp, J.; Garg, V. Targeted risk communication for computer security. In Proceedings of the 16th International Conference on Intelligent User Interfaces, Palo Alto, CA, USA, 13–16 February 2011; pp. 295–298.
27. Egelman, S.; Peer, E. The Myth of the Average User: Improving Privacy and Security Systems through Individualization. In Proceedings of the 2015 New Security Paradigms Workshop, Twente, The Netherlands, 8–11 September 2015; pp. 16–28.
28. Wash, R.; Rader, E.; Fennell, C. Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017.
29. Botzen, W.; Bergh, J.V.D. Risk attitudes to low-probability climate change risks: WTP for flood insurance. *J. Econ. Behav. Organ.* **2012**, *82*, 151–166. [CrossRef]
30. Mol, J.M.; Botzen, W.W.; Blasch, J. Behavioral motivations for self-insurance under different disaster risk insurance schemes. *J. Econ. Behav. Organ.* **2020**, *180*, 967–991. [CrossRef]
31. Rodríguez-Priego, N.; Van Bavel, R.; Vila, J.; Briggs, P. Framing Effects on Online Security Behavior. *Front. Psychol.* **2020**, *11*, 527886. [CrossRef]
32. Anderson, C.L.; Agarwal, R. Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Q.* **2010**, *34*, 613–643. [CrossRef]
33. Branley, D.B.; Covey, J. Is exposure to online content depicting risky behavior related to viewers' own risky behavior offline? *Comput. Hum. Behav.* **2017**, *75*, 283–287. [CrossRef]
34. Blais, A.-R.; Weber, E.U. A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations. *Judgm. Decis. Mak.* **2006**, *15*, 263–290.
35. Maccallum, R.C.; Austin, J.T. Applications of Structural Equation Modeling in Psychological Research. *Annu. Rev. Psychol.* **2000**, *51*, 201–226. [CrossRef]
36. Bollen, K. *Structural Equations with Latent Variables*; John Wiley & Sons: Hoboken, NJ, USA, 1989; ISBN 978-04-7101-171-2.
37. Cortina, J.M. What is coefficient alpha? An examination of theory and applications. *J. Appl. Psychol.* **1993**, *78*, 98–104. [CrossRef]
38. Nunnally, J.C. *Psychometric Theory*, 2nd ed.; McGraw-Hill: New York, NY, USA, 1978.
39. Smith, V.L. *Papers in Experimental Economics*; Cambridge University Press (CUP): Cambridge, UK, 1991.
40. Holt, C.A.; Laury, S.K. Risk Aversion and Incentive Effects. *Am. Econ. Rev.* **2002**, *92*, 1644–1655. [CrossRef]
41. Addae, J.H.; Sun, X.; Towey, D.; Radenkovic, M. Exploring user behavioral data for adaptive cybersecurity. *User Model. User Adapt. Interact.* **2019**, *29*, 701–750. [CrossRef]