

D6.1: Concept note with the design of the economic experiments

CYBECO

Supporting Cyberinsurance from a Behavioural Choice Perspective

D6.1: Concept note with the design of the economic experiments

Due date: M8

Abstract:

This concept note summarises our review of the current literature around cyberinsurance; highlighting key barriers to good cybersecurity and cyberinsurance uptake and relevant models of consumer behaviour. We then introduce two economic experiments. The first experiment tests the CYBECO model of cybersecurity and decision-making; and the second tests the CYBECO toolbox and identifies methods to nudge users towards optimal cybersecurity.

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

D6.1: Concept note with the design of the economic experiments

Document Status

Document Title	Concept note with the design of the economic experiments
Version	1.6
Work Package	6
Deliverable #	6.1
Prepared by	UNN & DEVSTAT
Contributors	Pam Briggs, Dawn Branley, James Nicholson & Lynne Coventry (UNN) José Vila, Yolanda Gómez, Jose Luis Cervera (DEVSTAT)
Checked by	
Approved by	
Date	December 22, 2017
Confidentiality	PU

D6.1: Concept note with the design of the economic experiments

Document Change Log

Each change or set of changes made to this document will result in an increment to the version number of the document. This change log records the process and identifies for each version number of the document the modification(s) which caused the version number to be incremented.

Change Log	Version	Date
First draft (UNN)	0.1	Oct 24, 2017
Updated to add Well Sorted Information and shorten summary table of barriers to insurance (UNN)	0.2	Oct 25, 2017
Updated to include literature on nudging (UNN)	0.3	Nov 6, 2017
Updated to refine literature review and include preliminary model for experiments (UNN)	0.4	Nov 8, 2017
Added literature around health and insurance calculators (UNN)	0.5	Nov 9, 2017
Added draft experimental design information (UNN)	0.6	Nov 10, 2017
Added new literature to review (UNN)	0.7	Nov 15, 2017
Amended literature following Skype phone call, updated experiment 1 figure and added draft abstract and conclusion (UNN)	0.8	Nov 20, 2017
Added details of Experiment 1 provided by DEVSTAT	0.9	Nov 21, 2017
Amended according to internal feedback (UNN)	1.0	Nov 22, 2017
Added details of Experiment 2 provided by DEVSTAT	1.1	Nov 24, 2017
Edit prior to circulation of draft document for comments (UNN)	1.2	Nov 29, 2017
Edited following DEVSTAT feedback (UNN)	1.3	Dec 4, 2017
Edited following group feedback from DELFT and ICMAT (UNN)	1.4	Dec 12, 2017
Consolidated feedback and final edits (UNN & DEVSTAT)	1.5	Dec 18, 2017
Final version complete	1.6	Dec 22, 2017



D6.1: Concept note with the design of the economic experiments

Table of Contents

1	Introduction	6
1.1	Objective and Scope	6
1.2	Background	6
2	Economic Experiments	25
2.1	Collaboration across Work Packages	25
2.2	Research Questions	26
2.3	Experimental Designs	28
2.3.1	Experiment 1: Testing the model (Defender)	31
2.3.2	Experiment 2: Optimising the CYBECO tool.....	36
3	Conclusion.....	42
4	References	43
5	Acronyms and Abbreviations	49

D6.1: Concept note with the design of the economic experiments

List of Figures

Figure 1: The Theory of Planned Behaviour model (Ajzen, 1991)	18
Figure 2: The Technology Acceptance Model (Davis, 1985).....	18
Figure 3: The Protection Motivation Model (Rogers, 1975)	19
Figure 4: Results of the Well Sorted collaborative task	25
Figure 5: Preliminary model of cyberinsurance decision making and behaviour	26
Figure 6: Design of Experiment 1	33
Figure 7: Life insurance calculators (Left to right: AXA; Sainsbury's Bank; Legal & General, 2017)	37
Figure 8: Life Insurance Calculator (Aviva, 2017)	37
Figure 9: Design of Experiment 2	39

D6.1: Concept note with the design of the economic experiments

1 Introduction

1.1 Objective and Scope

This concept note begins by summarising our review of the current literature around cyberinsurance; highlighting key barriers to cyberinsurance uptake and adherence to good Information Security Protocol (ISP). We then present an outline of relevant models of consumer behaviour and decision-making, drawn from the behavioural economics and psychology literatures. This literature review was one of four sources of information that was used to drive the design of two economic experiments. The other three sources were (i) the CYBECO use cases; (ii) the CYBECO model and (iii) the output from a collaborative exercise in which CYBECO members were polled in regard to the key research issues and questions around cyberinsurance (using a collaborative tool called 'well sorted' which is described in section 2.1). Two economic experiments are then described. These address cybersecurity behaviours and attitudes and those factors that affect cyberinsurance decision-making. The first experiment is designed to test the major CYBECO cybersecurity model, whilst the second experiment is focussed on the design of the CYBECO cybersecurity toolbox.

1.2 Background

Last year, 80% of European companies experienced at least one cyber breach or attack (European Commission, 2017). This rose to 66% amongst medium firms and 68% amongst large firms. Almost all businesses in the survey were exposed to cyber security risks (Klahr, Shah, Sheriffs, Rossington, & Pestell, 2017). Breaches are said to be increasing by around 20% every year, with their cost increasing by around 30% (Corner, 2014). The estimated cost of a cybersecurity breach has been estimated at £75,000-311,000 for SMEs and £1.46m-3.14m for larger organisations (*UK HM Government 2015 Information Security Breaches Survey*, 2015). Estimated global costs of cyber risk vary widely, with estimates ranging from US\$100bn to \$1000bn when accounting for secondary costs such as reputational costs. It is important to note that the majority of estimates are calculated by security and consultancy firms therefore bias is possible (Eling & Schnell, 2016). However, cybersecurity remains an important global issue.

In February 2000, hackers launched a Denial of Service (DDoS) attack, shutting down eBay, Amazon.com, CNN.com and other major Web sites for several hours. The attack cost the companies approximately \$1.2 billion (Gohring, 2002). In 2017, ransomware attacks cost companies \$5 billion (Cybersecurity Ventures, 2017). Severe cyber events such as this (i.e., occurring within major companies and resulting in big losses) are one of the main drivers of the cyber insurance market. However, whilst the companies that experienced these disasters became much more interested in purchasing cyber insurance policies to mitigate future losses

D6.1: Concept note with the design of the economic experiments

(Experian, 2013); many other companies seem unconvinced that investing in cyber insurance is necessary (Bandyopadhyay, Mookerjee, & Rao, 2009; Srinidhi, Yan, & Tayi, 2015).

Whilst organisations typically employ antivirus and anti-spam software, firewalls and intrusion-detection systems, it is impossible to achieve perfect security protection (Pal, Golubchik, Psounis, & Hui, 2017). This creates the market for cyberinsurance. Current cyberinsurance policies tend to provide three basic types of coverage: liability as a result of data theft; a means to remedy the breach; and legal and regulatory fines (Bandyopadhyay et al., 2009; Romanosky, Ablon, Kuehn, & Jones, 2017). The ideal scenario is that organisations will invest in both self-protection (e.g., firewalls and up to date antivirus software) and cyberinsurance (Pal et al., 2017). Cyberattacks can include many different types of risk, e.g., hacking, phishing, DDoS attacks, worms and viruses (Pal et al., 2017). One of the most common sources of security breaches are fraudulent emails sent to staff (Klahr et al., 2017), highlighting the need to also ensure that staff are aware and capable of detecting and dealing with attacks.

If widely adopted and well-functioning, cyberinsurance has the potential to encourage market-based risk management for information security, with a mechanism for spreading risk amongst multiple stakeholders. It also has the potential to act as an incentive towards organisational investments in information security; which would reduce risk for the investing organisation and for their wider network. Uptake could also lead to data aggregation on best practices and better tools for assessing security – something that is currently lacking in relation to cyberinsurance. In principle, cyberinsurance could strength IT security for society as a whole (Baer & Parkinson, 2007; Kuru & Bayraktar, 2017). However, despite proposed benefits and the increasing risk of cyberattack, uptake of cyberinsurance has not reached expectations. Low (2017) found that less than 10% of UK companies take out specific cyber insurance; although the Cyber Security Breaches Survey 2017 found that almost two-fifths (38%) of businesses reported having insurance (Klahr et al., 2017). Either way, this number is considerably lower than would be expected. However, Lloyd's of London reported an increase in uptake of 50% in 2016 and they have recently introduced 15 different types of cyberinsurance products for a predicted boom in uptake (Sanchez, 2017) – suggesting that the market is increasing but at a slower rate than predicted.

Since many companies are not currently buying cyberinsurance (Deloitte, 2017; Low, 2017), it is assumed that they are bypassing the insurance market and relying on alternative methods, such as lines of credit, balance sheet funding, and/or other assets. More than two-thirds (67.6%) of organisations have planned for sources of funding in the event of a cyber-attack but the adequacy of these methods is questionable when just 35.4% of them have conducted or estimated the financial impact (*UK Cyber Risk Survey Report*, 2016). Without an idea of the quantum of a potential loss, many of these could prove to be too large or, more likely, too small for what is required. Unfortunately, very little research has been conducted in the

D6.1: Concept note with the design of the economic experiments

economics and business literature on cyberinsurance (Eling & Schnell, 2016), however there have been some attempts to identify those factors that influence cyberinsurance uptake.

1.2.1 Factors influencing cyberinsurance uptake

There are many factors that may influence the uptake of cyberinsurance. We investigate these factors in more detail in the following section and in Table 1.

1.2.1.1 Low awareness and inaccurate perceptions of risk:

In 2014, the UK Governmental Department for Business, Innovation and Skills (BIS) introduced Cyber Essentials: a cybersecurity certification scheme that sets out a good baseline of cyber security suitable for all organisations. The scheme addresses five key controls that, correctly implemented, can prevent around 80% of cyberattacks. In addition to firewalls and antivirus, Cyber Essentials certification also requires a patching policy, a user access policy, and ability to configure devices. The Cyber Security Breaches survey 2017 found that over half (52%) of the firms included in the survey had enacted basic technical controls in the five areas laid out under the Cyber Essentials scheme. However, many of the businesses still did not have any basic protections or formalised approaches to cyber security (Klahr et al., 2017); something also reflected by Henson & Garfield (2015) who found that many SMEs in the UK have not heard of Cyber Essentials. Alarming the Cyber Security Breaches Survey 2017 found that only 21% of UK businesses are aware of ISO 27001 (the Government's Cyber Aware campaign) and only 13% were aware of the Government's 10 steps guidance. Some businesses, especially smaller ones, were also not aware of the existence of cyberinsurance at all (Eling & Schnell, 2016; Klahr et al., 2017).

In some cases inaccurate perceptions of risk may contribute to low uptake (Marotta, Martinelli, Nanni, Orlando, & Yautsiukhin, 2017). The limited research into cyberinsurance has tended to focus upon the supply side of insurability, however the demand side (including behavioural elements) is also vital. It is possible that optimism bias or latent fatalism may result in some individuals/businesses assuming that cyberattacks will not happen to them ("my data is not interesting enough", Eling & Schnell, 2016). Advisen (2015) found that SMEs view cyberattacks as less probable and are thus less likely to engage with cyber insurance. Although contrary to popular belief, the majority of cyberattacks target small to medium businesses (Meland, Tondel, & Solhaug, 2015; Needleman, 2012). Previous studies have shown that the ISO27001 Information Security Management standard is very rarely contemplated by SMEs (Barlette & Fomin, 2008; Coles-Kemp & Overill, 2007). It has been suggested that this may be due to smaller companies generally not having the expertise or understanding to appreciate the risk to their business as a result of not having secured their data (Henson & Garfield, 2015).

However, low awareness around vulnerability does not entirely explain the low uptake in

D6.1: Concept note with the design of the economic experiments

cyberinsurance. The ISACA/RSA Conference survey found that 74% of respondents stated that their organisations are “very likely” or “likely” to experience a cyberattack in 2016. Likewise, a recent report by Marsh (2016) shows that understanding of exposure to cyberattacks (i.e. companies being aware that they are a target) has increased up to 83.3% - again perhaps partly due to a series of high-profile breaches. Therefore, suggesting that despite increased awareness, many organisations are still not taking the next steps to addressing this issue. Organisations are not investing time in understanding their vulnerabilities (Marsh, 2016) nor providing adequate funding for cybersecurity (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016). This is perhaps because many organisations still see cybersecurity as being the IT department’s problem rather than an issue for the board (Advisen, 2015; Eling & Schnell, 2016). This is unfortunate as it positions security as a technical issue rather than a business concern (Nexus, 2016). There are some signs that this may be beginning to improve: The Nexus State of Cybersecurity survey found that most organisations (82%) reported that their board of directors was ‘concerned’ or ‘very concerned’ about cybersecurity and information security. The Cyber Security Breaches survey also found that 74% of UK businesses stated that cyber security was high priority for senior management, with 31% saying it was a *very high* priority (Klahr et al., 2017); suggesting that recognition of cybersecurity as an issue for the board may be increasing.

1.2.1.2 Policy Exclusions and Limits

According to the survey of Enterprise-Wide Cyber Risk Management Practices in Europe (Advisen, 2015), the majority of respondents said that they do not purchase cyber insurance because insurance does not provide adequate coverage for their exposures (47%). The second and third popular answers were: it is too expensive (20%) and adequate limits are not available in the market (7%). These results support the findings of Betterley (2010) which found that existing insureds reported that they would be willing to pay higher premiums if their primary coverage objectives were included in the cyber policy. Although some companies are still hesitant about buying policies due to exclusions, restrictions (e.g., capped policies) and uninsurable risks (Baer, 2003; Betterley, 2010, 2014; LLC, 2013; Schwartz, Shetty, & Walrand, 2010; Torgas & Zahn, 2014 - as cited by Marotta et al., 2017). For example, many policies contain exclusions around self-inflicted losses, access to unsecure websites or terrorism (Eling & Schnell, 2016). Many policies do not cover physical damage or bodily harm resulting from cyber-induced incidents (Romanosky et al., 2017; Young, Lopez Jr., Rice, Ramsey, & McTasney, 2016). Despite these issues, those that have adopted insurance policies report being satisfied (Experian, 2013). An example decision making model for purchasing cyber insurance is proposed by Bandyopadhyay & Shidore (2011), who suggest that the Chief Information Security Officer and the Chief Risk Officer work together to maximize the coverage of the insurance. Other organisations may also make the error of assuming that general business insurance will cover them for all eventualities, however by 2002, insurers had excluded coverage of “electronic data”, “computer code” and similar terms as tangible property (Baer & Parkinson, 2007; Eling & Schnell, 2016; Young et al., 2016).

D6.1: Concept note with the design of the economic experiments

It is hard to specify precisely what a business wants/needs to be covered, and what an insurer is willing to cover (Biener, Eling, & Wirfs, 2015; Crane, 2001; Crowther et al., 2013; ENISA, 2012). This is further confounded by a lack of agreed-up terminology and no standardisation of products, making policies difficult to compare (Eling & Schnell, 2016). Coverage is often too small for large corporations, like Google. Also, as many cyber-attacks occur undetected (and sometimes take place over prolonged periods of time), breaches may not be noticed until sometime after the initial attack. It has been estimated that breaches can take around 246 days on average to be detected (4-5 days in businesses with gold standard security management systems: Corner, 2014). With some sources quoting an average of more than a year. Therefore, it is not clear how insurers should reimburse the expenses (Meland, Tondel, & Solhaug, 2015).

1.2.1.3 Policy Pricing

The global cyberinsurance business is currently worth around \$2 billion (USD). In comparison, the total cost of security breaches worldwide is around \$445 billion (Pal et al., 2017). Unfortunately, insurers are currently unable to effectively estimate agents risk due to an inability to anticipate the secondary losses of organisations. The market operates in a state of *information asymmetry*, where the insurer does not have all the information about the company's security protections, and is unable to check these. This results in *adverse selection*, i.e., the inability of an insurer to distinguish between different client types, those who have risk-appropriate behaviours and those who do not (Young et al., 2016). The risk to insurers is also increased by the opportunity for another form of information asymmetry: *moral hazard*, i.e., the change of behaviour by the insured after purchasing insurance such as reduced incentive to invest in self-protection measures or necessary updates (Eling & Schnell, 2016; Young et al., 2016). This change may be due to dishonesty or alternatively due to behaviour from the client that unintentionally increases the chance and/or severity of loss (Young et al., 2016). As insurers will not run at a loss, this leads to a stalemate situation whereby insurance companies increase their policy prices in an attempt to mitigate risk, however this then deters consumers from purchasing these policies. Bandyopadhyay, Mookerjee, & Rao (2009) explored the reluctance of IT Managers to purchase cyber insurance products, and found that this was largely due to the price of the insurance contracts. As the majority of cyberattacks are aimed at SMEs, high policy prices could be particularly detrimental to insurance uptake (Aguilar, 2015).

In order to address the issues of adverse selection, insurers need to invest in an underwriting process that screens clients to avoid risk behaviour that is beyond the insurers tolerance. Whilst to address moral hazard, insurers need to develop methods to allow continuous monitoring of cyber security practices (Young et al., 2016). Moral hazard can also be improved by incentivising increases in security posture through reduced premiums (and/or requiring minimum controls before insurance will even be offered; (Bailey, 2014). Alternatively, or additionally, there is also the possibility of penalising through imposing deductibles so that the insured suffers some loss in the event of an accident (Young et al., 2016).

D6.1: Concept note with the design of the economic experiments

Romanosky, Ablon, Kuehn, & Jones (2017) have found that insurance providers ‘guess’ the premiums for coverage, due to their lack of experience in the area (and also due to difficulty predicting intangible consequences such as loss of brand value, Young et al., 2016). Some will use reports (usually old) to extrapolate the potential threat likelihood. Additionally, many insurers follow a flat rate policy, where insurants pay the same monthly premium regardless of personal circumstances. Only 31% of insurers in Romanosky et al’s study used information about the clients’ security posture in the premium calculation process. Even those insurers who did apply factors based on security behaviours (e.g. Privacy Controls, Network Security Controls, Content Liability Controls, Laptop and Mobile Device Security Policy, and Incident Report Plan) used very broad categories, and the ratings for the behaviours were vague (e.g. average, above average, below average). Only once information symmetry is reached (i.e., both parties fully informed) will premiums accurately reflect the risks. Mukhopadhyay, Chatterjee, Saha, Mahanti, & Sadhukhan (2013) tested mathematical models for determining the correct insurance premiums in order to become more competitive. Their model takes into consideration the size and wealth of the organisation, as well as their risk profile, although information asymmetry remains a problem in practice.

Survey data of 237 organisations revealed that only 18.6% allocated more than 10% of their IT budget to security, with a third of the organisations allocating 5% or less (Richardson, 2010). SMEs have been shown to have an overall negative view towards information assurance (practice of assuring information and managing risks related to the use, storage, and transmission of data and the systems and processes used for those purposes) particularly due to cost (Henson & Garfield, 2015). Businesses, particularly SMEs, can often be heavily restricted by the budget they have available for cybersecurity; because of this they are forced to make trade-offs regarding how they defend their systems (Fielder et al., 2016). When making this trade-off, the organisation has to make a decision based upon the direct cost of implementing a particular safeguard and the impact that the safeguard may have on the business (e.g., indirect costs such as a reduction in productivity speed, system performance speed, morale cost or re-training cost; Fielder et al., 2016). At a certain level of protection, implementing additional controls/safeguards may only reduce the impact of a vulnerability by a fraction of its maximum efficiency. Conversely, the cost of implementation remains the same, therefore there becomes a diminishing return for each control that you add to the system (Fielder et al., 2016). This is when being able to identify the optimum level of protection is crucial. Young, et al. (2016) propose a preliminary framework to suggest optimal levels of investment in cybersecurity and insurance to minimise risk for critical infrastructure. The framework incorporates insurance in three key ways: Firstly, by using insurance as an incentive to increase the level of investment in self-protection (e.g., by incentivising investment in self-protection by reducing premiums); Secondly, by emphasising the importance of gathering and sharing data; and thirdly, by leveraging the quantitative models used by the insurance industry. They recognise that the framework is based on limited data and that assumptions have to be made about company scenarios. They encourage future research to

D6.1: Concept note with the design of the economic experiments

improve upon the accuracy of these outputs and suggest that the resulting framework can be continually refined through time.

Although cost plays a role in the uptake of cyberinsurance, Bandyopadhyay et al. (2009) argue that the demand-side problem with cyber insurance is deeper than the supply-side problem; as overly priced premiums would normally correct through time as experience and knowledge of risk is gained due to actual claims (Young et al., 2016). However, this is not possible unless demand for cyberinsurance increases.

1.2.1.4 Time, resources & expertise

The Cyber Security Breaches survey found that only a fifth (20%) of businesses had staff attend any form of cyber security training in the last 12 months. Yet it can take just a single employee to cause a breach (Klahr et al., 2017). Good security practices take time and effort, this can mean the motivation to engage in good practice is low (Das, 2017). Alternatively, motivation to have good security may be present but this may not be put into action due to a lack of resources, or lack of confidence regarding where to start.

Complexity has also been identified as a barrier to good practice (Henson & Garfield, 2015). Less complex information assurance standards suitable for SMEs (e.g., IASME and BIS 2014) have still not helped to tackle this problem. Statistics consistently show that more small businesses are being breached every year (Henson & Garfield, 2015). The State of Cybersecurity survey (Nexus, 2016) found that 62% of organisations reported having too few information security professionals, and a tendency for sub-par applicants for such job vacancies; suggesting an insufficient pool of suitable, skilled candidates. When asked “Are you comfortable with your cybersecurity/information security team’s ability to detect and respond to incidents?” the majority of respondents said yes but only for small incidents.

If SMEs are not engaging in practices to manage risks related to the use, storage and transmission of data, they are unlikely to show interest in cyberinsurance.

1.2.1.5 Correlation of risk and business interconnectivity

IT systems, networks, risks and the protection against these are not something that can usually be contained within a single organisation. Alarming, the UK Cyber Risk Survey Report (2016) found that only 26.5% of respondents report that their organisations’ supply chains are assessed for cyber risks (up slightly from 22.2% in 2015), leaving the overwhelming majority of companies exposed to attack from third parties (from service providers to customers). Target experienced a major security breach in November 2013 which resulted in the theft of 70 million customers’ personal information. This breach was a result of access being gained by attackers penetrating the network of a small business that Target used for heating and air cooling services (Perlroth, 2014). Cyberattacks can affect a large amount of businesses at once, on a global scale and this is not simply restricted to interconnected businesses; once a security leak has been identified it can often be exploited in a multitude of systems due to similar IT systems being utilised (Eling & Schnell, 2016; Lloyds of London,

D6.1: Concept note with the design of the economic experiments

2017). Therefore correlation of risk is another reason why it is difficult for insurance companies to identify liability and calculate coverage (Meland et al., 2015).

Ogut, Menon, and Raghunathan (2005) investigated the effect of interdependency of threats and security investments. The authors concluded that security investments fall with an increase of interdependency. Similar conclusions were supported by Eling and Schnell (2016) and Shim (2012); a potential reason for this is due to free riding on other organisations' security measures. This can result in organisations assuming they do not need to invest in their own security measures as others in their supply chain will have security measures in place. Whilst in economic terms, it is individually rational to free ride, when multiple compromised machines are within the same network – this represents a 'public bad' (Varian, 2004).

1.2.1.6 Concerns about breach disclosure

Organisations also fear the fallout from disclosing a breach (e.g., stock price drop, loss of customer trust and damage to reputation; (Eling & Schnell, 2016; Low, 2017; Young et al., 2016). According to the 2014 Forbes report, almost half (46%) of companies have suffered reputational damage due to a data breach. Often secondary damages such as these are not taken into account by the policy, meaning that the claim payout may not be sufficient. In some circumstances, organisations may benefit more from *not* claiming off insurance; unless the breach happens to be systematic (an unknown threat and thus not possible to protect against, e.g. unpatched OS vulnerability) and public. Private, symptomatic breaches (breaches that happen due to firm-specific vulnerabilities) are very unlikely to be disclosed. The CSI/FBI computer crime and security survey found that only a fraction of identified breaches are publicly disclosed. Organisations are therefore unlikely to claim on such breaches as this may lead to public knowledge (due to dealing with multiple organisations).

Another potential disadvantage of public disclosure is the potential for system vulnerabilities to be exploited whilst the organisation is still trying to patch the original breach – exposing the organisation to further attacks. This raises questions over when the organisations should inform their insurance company (which may not match when the insurance company would like to be informed; Meland, Tondel, & Solhaug, 2015).

D6.1: Concept note with the design of the economic experiments

Table 1. Summary of factors affecting cyberinsurance uptake, from both an organisational and individual level.

Barrier	Organisational Level	Individual Level
Negative attitudes towards cybersecurity and/or cyberinsurance	<ul style="list-style-type: none"> Regarding cybersecurity as a 'blocker' rather than an 'enabler'. Perceived as an obstacle to business goals. Senior management feel that they are too busy/too important to be bothered by 'petty' security policies (Sasse & Flechais, 2005). Attitude that security is an IT problem. Lack of executive management backup (Hiscox, 2017). Mistrust of insurers: <ul style="list-style-type: none"> High cost not clearly justified. No clear method for calculating premiums. Too many limitations imposed by insurers. "Cyberinsurance policies are so complicated – I don't understand what they would cover me for" (Hiscox, 2017). Do not trust insurer to pay out (Hiscox, 2017). Feel there is not enough robust data and no standardised procedures to back up investing in cyberinsurance (Betterley, 2010; Low, 2017; Majuca, Yurcik, & Kesan, 2005; Toregas & Zahn, 2014). Perceived benefit counteracted by potential damage to reputation if breach publicly leaked (due to third parties). Secondary losses not adequately covered by insurance. 	<ul style="list-style-type: none"> Feeling that personal competence is being challenged (not trusted to behave responsibly). "only amateurs fall victims to attacks" (Pfleeger & Caputo, 2012). Conflicts with self-image "only nerds and paranoid people comply with information security policy (ISP)" (Sasse & Flechais, 2005). Feel security should not be something they have to worry about (i.e., the business should ensure they are protected). Cybersecurity viewed as an obstacle delaying/restricting productivity (Turland, Coventry, Jeske, Briggs, & van Moorsel, 2015). Cost-benefit analysis influenced by time restraints (i.e., do not have time to think through benefits on a deeper level). Feel that security policy is unfair on the workforce – e.g., individuals do not see the benefits themselves nor are they rewarded for compliance to protocol (in comparison, they would be rewarded for greater productivity that could be gained through time saved from non-adherence).
Normative beliefs about cybersecurity (social influence)	<ul style="list-style-type: none"> Do not perceive other businesses to be engaging in good ISP and/or purchasing insurance cover. Particularly as these behaviours are not often visible to outsiders. 	<ul style="list-style-type: none"> Complying with ISP conflicts with desirable social norms, e.g., concerns of being perceived as 'paranoid' or 'anal' to colleagues (Sasse and Flechais, 2005). Influenced by behaviour of peers.

D6.1: Concept note with the design of the economic experiments

Low perceived severity & vulnerability to cyber attacks	<ul style="list-style-type: none"> Underestimate vulnerability: e.g., “We wouldn’t get phished/attacked/targeted”, “it wouldn’t happen to us”. Feel that cyberinsurance is not relative to them. 	<ul style="list-style-type: none"> Inaccurate perceptions: “It won’t happen to me” (Optimism bias), “We haven’t been attacked yet” (Confirmation bias). Not identifying security threats as their concern. Not feeling personally at risk (Sasse & Flechais, 2005). Perhaps due to feeling that this is an organisational level concern.
High perceived control over attacks	<ul style="list-style-type: none"> Inaccurate perceptions around organisation’s ability to deal with attacks, e.g., 75% of businesses state that they are “very confident” with their cyber security readiness (Hiscox, 2017) suggesting that there may be a sense of complacency). May feel ISP is a replacement for insurance (and vice versa). 	<ul style="list-style-type: none"> Overestimated perceived control & self-efficacy, e.g. “I could easily detect a threat”, “I wouldn’t fall for a scam” (Control Bias, Pfleeger & Caputo, 2012)
Low perceived self-efficacy re: implementing ISP	<ul style="list-style-type: none"> Issues around setting up insurance, e.g., not clear what is covered or how to assess risk. Overwhelmed by implementation (Hiscox, 2017). Requirement to engage in additional security measures prior to taking out insurance (Hiscox, 2017). Also, uncertainty regarding how to maintain a good level of cybersecurity over the longer term (especially given ever changing landscape of risk, (ENISA, 2012; Rosen, Steinberg, Kearney, O’Connor, & Rubin, 2014; Tondel, Meland, Omerovic, Gjaere, & Solhaug, 2015). 	<ul style="list-style-type: none"> Doubts over self-efficacy in relation to ability to comply with ISP (e.g., lack of technology literacy). Lack of access (actual or perceived) to necessary organisational resources, e.g., training, policies etc. Tendency to look for workarounds/shortcuts especially if unaware how their behaviour comprises security (Sasse & Flechais, 2005) and/or due to time restraints on work load/productivity.
Low perceived severity and/or certainty of sanctions from non-compliance	<ul style="list-style-type: none"> Lack of legislation regarding cyberinsurance requirements and sanctions for breaches. Perception that cyberinsurance is unlikely to result in sanctions. (This could change with new legislation such as the EU’s new general data protection regime in 2018). 	<ul style="list-style-type: none"> Consequences for non-compliance perceived as low (perhaps due to low awareness of sanctions or lack of organisational policy for noncompliance). Do not believe that they will be held accountable for not following ISP (Sasse & Flechais, 2005).
Free riding	<ul style="list-style-type: none"> Perception that cybersecurity is not a big issue as the other businesses/organisations in their network all have good ISP. 	<ul style="list-style-type: none"> Feel that they are only one individual and they will not make much difference to the security of the overall organisation.
Lack of reporting behaviour	<ul style="list-style-type: none"> Businesses may not report cybercrimes for fear of 1). Secondary damages to reputation or repeat attacks if a leak becomes public knowledge; 2). Lack of trust that the offender will be identified/prosecuted (“little to be gained from reporting”, 	<ul style="list-style-type: none"> Individuals may not be aware of formal plans for reporting and responding to e-crimes. Alternatively, they may be wary of reporting due to fear that some fault will be placed with their

D6.1: Concept note with the design of the economic experiments

	Sukhai, 2004); 3). Investigation process disrupting business; 4) Lack of formal plans for responding to e-crimes (Sukhai, 2004)	own actions and/or the investigation process disrupting productivity.
Moral hazard	<ul style="list-style-type: none"> Businesses may change security behaviours once insurance is in place (e.g., investing less than optimal time, effort and finances into good ISP). This could be due to cyberinsurance de-incentivising good security behaviour (by reducing perceived benefits of investing in self-protection measures) and displacement of responsibility ("risks covered by insurance"). 	<ul style="list-style-type: none"> If individuals feel that everyone else is adhering to cybersecurity protocol and/or that insurance is in place to cover cyberattacks, they may be less inclined to engage in good self-protection measures – particularly if they do not perceive any benefit for doing so (and/or perceive disadvantages such as barriers to productivity).

D6.1: Concept note with the design of the economic experiments

1.2.2 Addressing the need for change

Henson and Garfield (2015) suggest that a change in perception and culture is necessary to increase uptake of information assurance and cyberinsurance, suggesting that there is a *need* for cyberinsurance, but not a *want* (potentially due to the aforementioned issues). Cyberinsurance has helped to raise awareness and protect the supply chain in the US (Garrie & Mann, 2014). However, many states in the US now have legislation that makes it law to disclose security breaches (National Conference of State Legislatures, 2017). Legislation has been identified as one of the main drivers for cyberinsurance uptake (Henson & Garfield, 2015; Low, 2017). The existence of further legislation may bring about a change in attitudes towards cyberinsurance. There are currently no global laws in place for cyberinsurance, although obligations to report data breaches are due to be introduced to the European Union in 2018 (Eling & Schnell, 2016; Low, 2017). Nevertheless, it is necessary to look at other means to increase insurance uptake. More empirical evidence is needed, focusing on both the demand and the supply sides of insurability (Eling & Schnell, 2016).

It is important that businesses are encouraged to also employ good security management policies outside of investing in cyberinsurance (Low, 2017). Cyberattacks generally follow the life cycle of five stages: research, infiltration, discovery, capture, and exfiltration of information. Whilst money may be invested in trying to stop cyberattacks infiltration the system, 100% protection is not possible (Low, 2017). It is vital that adequate investment is also allocated to the other stages of the attack life cycle, for example investing in systems and staff to detect malicious activity before anything is stolen. As the attacker who breaches the system is generally not the one to steal the data/goods (instead they sell the access points to the system), there is generally a delay between attack and theft – meaning security measures employed to detect breaches quickly can significantly minimise losses (Corner, 2014). Successful interventions will incorporate the need for good security practice and insurance cover, potentially through rewarding good practice. There is no established model for cyber risk (Eling & Schnell, 2016). However, some of the main psychological theories can provide a theoretical basis for the design of such interventions:

1.2.2.1 Theory of Planned Behaviour

One of the dominant theories in this research area, the Theory of Planned Behaviour (TPB) states that intention to perform a behaviour is the most immediate and important determination of behaviour (Ajzen, 1991; Figure 1). Intention is anteceded by the individual's attitudes towards the behaviour, subjective norm(s) and perceived control over the situation. This theory suggests that strengthening positive attitudes towards cybersecurity (e.g., strengthening perceived benefits compared to perceived costs) could increase better security practices, potentially including cyberinsurance uptake. Likewise strengthening subjective norms may help to increase uptake of cyberinsurance (e.g., strengthening the perception that others believe that cyberinsurance may help to manage residual risks not fully treated by other security countermeasures). Lastly, perceived behavioural control relates to the agents

D6.1: Concept note with the design of the economic experiments

perceived control over negative circumstances (e.g., if a cyberattack occurs). Perceived control could also relate to self-efficacy around engaging in cybersecurity protocol. Low perceived control over cyberattack consequences, may increase intention to purchase cyberinsurance (due to a desire to increase control over consequences) but low perceived self-efficacy around implementing good practice may hinder this intention (e.g., if individuals/organisations feel they are not capable of implementing the technological requirements of cyberinsurance).

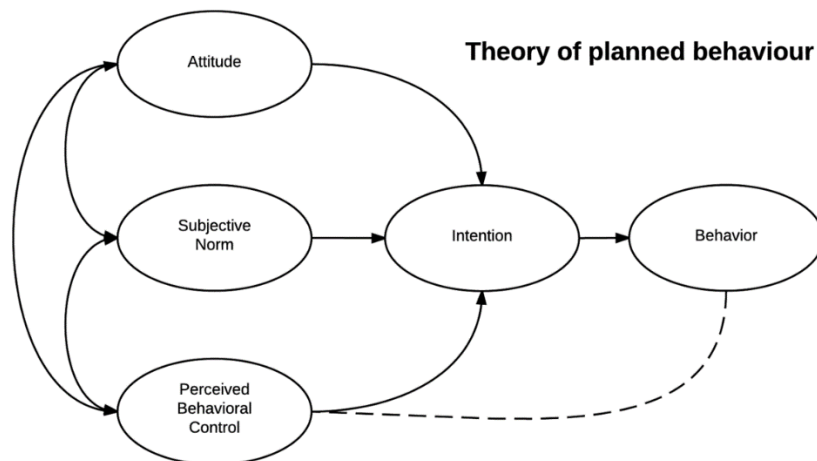


Figure 1: The Theory of Planned Behaviour model (Ajzen, 1991)

1.2.2.2 Technology Acceptance Model

Like the TPB, the Technology Acceptance Model (TAM; Figure 2) also focuses upon an individual's intention to perform a behaviour (Davis, 1985). The TAM model predicts that acceptance of technology will depend upon two factors: perceived usefulness of the technology (the degree to which a person believes that using a particular system would enhance his or her job performance") and perceived ease of use (the degree to which a person views using a system as being within their capabilities). If cybersecurity is perceived as useful to the individual/organization *and* perceived as within their capabilities (e.g., easy to set up) then they are more likely to invest in cyberinsurance.

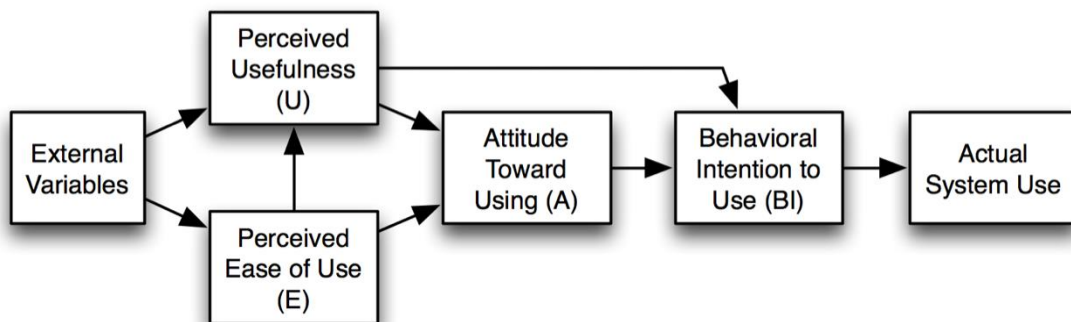


Figure 2: The Technology Acceptance Model (Davis, 1985)

D6.1: Concept note with the design of the economic experiments

1.2.2.3 Protection Motivation (PM) Theory

Protection Motivation theory (Rogers, 1975; Figure 3) proposes that people protect themselves based upon four factors: the perceived severity of a threatening event (in this instance a cyberattack), the perceived probability of the event occurring (including perceived vulnerability), the efficacy of the recommended protective behaviour (e.g., cyberinsurance) and their perceived self-efficacy.

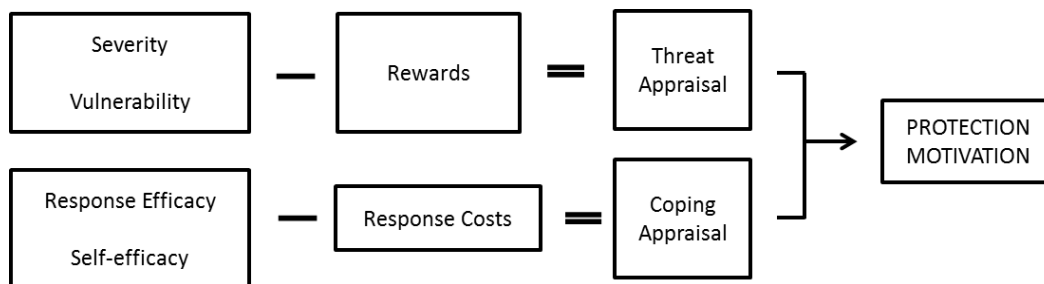


Figure 3: The Protection Motivation Model (Rogers, 1975)

Perceived severity and perceived probability are weighed up against the rewards of the behavior. Therefore, an organisation considering whether to invest in cyberinsurance may weigh up the perceived probability and severity of suffering a cyberattack attack (and the associated consequences) against the perceived benefit of *not* investing in cyberinsurance, i.e., costs saved due to not paying for the insurance policy. This will feed into the agent's *threat appraisal* regarding how serious the situation is. Threat appraisal is then weighed up against the agent's *coping appraisal* which comprises of efficacy of the protective behaviour and self-efficacy, weighed up against the costs of the protective behaviour (i.e., insurance costs: financial or secondary). If the threat appraisal considerably outweighs the coping appraisal, the agent is more likely to invest in cyberinsurance.

It is apparent that awareness raising and knowledge building are at the core of addressing many of the identified barriers to cyberinsurance uptake. However, changing behaviour requires more than simply providing information about good and bad behaviours. The organisations must be able to understand and apply the advice, and importantly they must *want* to act upon it. Motivation and intention to perform a behaviour (in this instance to engage in risk assessment and insurance uptake) are key factors to behaviour change. Influencing these factors requires changes to attitudes as identified in the psychological models discussed.

When considering whether to purchase cyberinsurance, organisations will calculate the benefit-risk trade-off (also referred to as the benefit to loss ratio). This involves weighing up the pros (e.g., protection against attacks) and cons of insuring (e.g., high price) against the pros and cons of not insuring (e.g., saves policy cost, but less protection). The benefit to loss

D6.1: Concept note with the design of the economic experiments

ratio will depend upon the organisations perceived cost of safeguards (e.g., time, effort, money) compared to the cost of impacts over assets and market share following a cyberattack. Interventions that can influence this benefit to loss ratio may be effective in encouraging or 'nudging' organisations towards investing in cyberinsurance. Past behaviour and/or past experiences have also been shown to impact upon future willingness and behaviour. This is reflected in previous research that has found a relationship between demand for insurance and recent experience of loss. For example, flood insurance purchases increase significantly after a recent flood (Browne & Hoyt, 2000) and a similar trend was observed for earthquakes (Kunreuther, 1996). Without past experience of an attack, organisations may fail to identify that they are at risk. Gordon, Loeb, Lucyshyn, and Zhou (2015) highlight the need for cyber insurance uptake to become a proactive response rather than a reactive response to a breach or incident; and to minimise the tendency for firms to defer cyber security investment. Recent work has found that when people become aware of the risks by being given information, they show increased willingness to purchase insurance cover (Zhou-Richter, Browne, & Gründl, 2009).

1.2.2.4 The rational-behavioural model

Many behavioural models rely upon the assumption that people are rational decision makers and therefore these models are not always effective (Hanoch, Barnes, & Rice, 2017). Decision making is often influenced by biases and the use of heuristics (rule of thumb processes) that can lead to less than optimal choices (Gilovich, Griffin, & Kahneman, 2002). For example, low probability events are vastly overweighed or ignored when making a decision whether to purchase insurance (Tversky & Kahneman, 1992). Individual may interpret insurance as a *certain* expense for a *non-certain* benefit (Baicker, Congdon, & Mullainathan, 2012). Also, lack of knowledge about benefits and coverage results in consumers frequently making poor insurance decisions (Loewenstein et al., 2013).

There is another difference between the rational-behavioural approaches to decision making under risk, that has a critical implication in the design, analysis and interpretation of the economic experiments in CYBECO. Specifically, the rational approach models risky decision making according to the Expected Utility model. Under this approach, the shape of the utility function completely determines risk attitude. However, within the behavioural economics framework, risk attitude does also depend on how probabilities are transformed to be applied in decision-making (Abdellaoui, L'Haridon, & Paraschiv, 2011; Alventosa, Gómez, Martínez-Molés, & Vila, 2016; Tversky & Kahneman, 1992). A formalization of such a transformation from the viewpoint of the rank-dependent utility theory, is included in Appendix A.

1.2.3 Nudging towards good cybersecurity decisions

Decision support systems, such as the CYBECO toolbox, aim to guide and support the decision maker. The system, including the way that choices are presented, can be designed

D6.1: Concept note with the design of the economic experiments

to maximize persuasiveness/encourage users towards good decision making (Parkes, 2009). This is often referred to as *choice architecture* and *nudging*. Nudging is the process of influencing decision making by altering choice architecture or framing (Thaler & Sunstein, 2008). For example, perceptions of difficulty can influence decision making. If a behaviour is regarded as difficult then use of a decision support system is likely to increase (Parkes, 2009). As cybersecurity and cyberinsurance is often regarded as complex (Henson & Garfield, 2015) then this suggests that decision support systems in this field would be well received. However, when using a decision support system, it is important to make choices as easy as possible for the user and/or increase users' feelings of self-efficacy. Other nudges can include framing the choice in relation to the benefits of the behaviour, referring to social norms (e.g., "the majority of businesses similar to yours have cyberinsurance") and the use of choice architecture such as a traffic light system (e.g., highlighting optimum choices in green and less rational choices in red; Thorndike, Riis, Sonnenberg, & Levy, 2014). The personalisation of nudges has also been shown to increase the effectiveness of decision support systems (e.g., "a business like yours has a high threat of cyberattack", "Taking into account the size and nature of your business, you could protect against most cyberattacks/lower your risk of a cyberattack by..."). Nudges have been used in many different fields, e.g., consumer behaviour, health behaviour, environmental behaviour (e.g., encouraging environmentally friendly behaviour; Perren, Yang, He, Yang, & Shan, 2016). Table 2 provides examples of the type of nudges that can be applied to the decision-making process. We envisage that the first experiment will apply more of the 'framing' nudges, whereas the second experiment will apply more of the 'choice architecture' nudges. More detail on the experiments is included in Section 2.

D6.1: Concept note with the design of the economic experiments

Table 2. Nudge techniques

<u>Manipulation</u>	<u>Description & Potential Nudge Techniques</u>	<u>Implications for Behavioural Experiments</u>
Framing: Positive vs Negative Outcomes / Coping vs Threat <i>(fits with attitudes and perceived behavioural control from TPB, perceived usefulness from TAM, and threat/coping appraisal from PM)</i>	<p>Framing can be used to influence an individual's reference point (as described by prospect theory), which makes it possible to nudge people towards investing in insurance by describing the benefits and losses. E.g.:</p> <ul style="list-style-type: none"> • Manipulating positive/negative outcome salience by focusing on the probability of a positive outcome or the probability of a negative outcome (probability framings) • Explaining how a scenario would unfold with and without insurance (could tap into anticipated regret. Emotive responses can increase efficacy of behaviour change techniques – see emotive response framing below) • Illustrate how the individual can take steps to protect themselves (coping messages). Also raise awareness of threat level and/or highlight the risks of their insecure behaviour and how this is increasing their likelihood of a cyberattack/breach (threat messages. similar to the mobile privacy nudges by Almuhimedi et al., 2015). Coping messages shown to have more influence on behaviour (adding threat appraisal was no more effective than coping message alone). 	<p>Experiment 1: Framing the tasks involved in the experiment (and potentially framing the payout) may influence behaviour. E.g., if awareness of threat/vulnerability is heightened (threat appraisal) individuals may act more securely. Likewise, if awareness of coping mechanisms (coping appraisal) or positive benefits to good cybersecurity are heightened, individuals may act more securely. This could guide the framing used for Experiment 2.</p>
Framing: Normative Messages (‘normative nudge’) <i>(fits with norms from TPB)</i>	<p>Social norms refer to customary rules of behaviour that are considered acceptable in a group or in society. The Social Norms Approach (SNA) posits that an individual should be significantly more motivated to engage in the target behaviour when they receive feedback that informs them than more people approve and/or perform the behaviour than they previously believed.</p> <p>E.g., Inform participants of the % of similar organisations that have invested in cyberinsurance and/or the percentage of people that believe cyberinsurance is good investment (could also tap into ‘social comparison’ and ‘others’ approval’ as a form of behaviour change technique).</p>	<p>Experiment 1 & 2: Normative nudges can increase the perception that more people approve and/or purchase cyberinsurance/cybersecurity. This in turn may influence individuals to act more securely.</p> <p>Experiment 2: Normative messages could also be used to encourage uptake of specific policies offered by the toolbox (e.g., “the majority of people choose this policy level”).</p>

D6.1: Concept note with the design of the economic experiments

	Testimonial from colleague? “After an unexpected breach, I got my money back” etc.	
Framing: Emotive response (fits with attitudes from TPB and TAM, and threat/coping appraisal from PM)	Highlighting emotions associated with a particular behaviour leads to more effective warning messages, e.g., ‘to avoid future disappointment’ (Esposito, Hernández, van Bavel, & Vila, 2017), ‘in order to relax, safe in the knowledge that..’	Experiment 1: If the potential for a negative emotional response to a breach is made salient, the individual is more likely to act securely. Likewise, if positive emotive responses are anticipated following insurance purchase then the individual may be more likely to purchase insurance. Experiment 2: Could use emotive language to guide the wording for the toolbox.
Framing: Highlight discrepancies (fits with intentions from TPB)	Draw attention to discrepancies between current behaviour (e.g., no insurance) and perceptions of their behaviour or ‘goal’ behaviour (e.g., providing a good service to customers, doing everything to protect customers’ data).	Experiment 2: Incorporating an item in the toolbox asking the user to think about what aspects of customer care are important to them (and how this aligns with their current protection level), may influence their intention to act more securely.
Framing: Presentation on the information on the levels of risk (fits with Prospect Theory)	The information selected to present the information on the probabilities to suffer a cyberattack have a critical impact in the form of the value and weighting functions considered in the Prospect Theory (and presented in Appendix 1), and then in the risk attitude and the final results of the decision making. <ul style="list-style-type: none"> Abdellaoui, M., L’Haridon, O., & Paraschiv, C. (2011) show that when this information is presented through a gamification, weighting function is closer to that considered under expected utility than in those cases where this information is just described. Gómez, Y., Martínez-Molés, V., & Vila, J. (2016) show how the addition of simple labels summarizing the information about risk level have a deep impact on the weighting function, generating misperceptions of actual risk levels. 	Experiment 1: the risk weightings in phase 1 should influence decision-making in phase 2. Experiments 2: The presentation of the level of risk of the subject, to be obtained from the information provided to the calculator, will be presented in different framings to identify the most effective nudges toward normative optimal decision-making.
Choice Architecture: Item placement	<ul style="list-style-type: none"> Item location: Items at the top or end of a list may be attended to/remembered more (primacy and recency effects). The stage which information is displayed may alter the effect this has upon behaviour, e.g., whether information is presented at the start or very end of the 	Experiment 2: The layout of the toolbox/calculator could be guided by these nudges. For example, information encouraging secure behaviour placed at the start or end of the process/list; Favourable options/behaviours

D6.1: Concept note with the design of the economic experiments

	<p>process (Esposito et al., 2017; Turland, Coventry, Jeske, Briggs, & van Moorsel, 2015).</p> <ul style="list-style-type: none"> • Traffic light system: E.g., highlight more favourable options in green and less favourable in red (Thorndike, Riis, Sonnenberg, & Levy, 2014; Turland et al., 2015) • Smart defaults: Common to choose dominated options (Bhargava, Loewenstein, & Sydnor, 2015). This also helps address decision inertia (Johnson et al., 2012). 	highlighted (e.g., with traffic light system); use of smart defaults.
<p>Choice Architecture: Reduce complexity and increase perceived self-efficacy <i>(fits with attitudes and perceived behavioural control from TPB, perceived ease of use from TAM, and coping appraisal from PM)</i></p>	<ul style="list-style-type: none"> • Reducing information overload so the choice is less complex/daunting (and reduce choice overload) • Increasing salience (and reduce complexity) by highlighting key information and downplaying less important information • Increase ease of set up by reducing steps/time/info required to put policy into place, e.g., one click purchasing (similar to option for 'quick enrollment decision' for health insurance, Choi, Laibson, & Madrian, 2006) 	<p>Experiment 2: Uptake of insurance and other cybersecurity could be increased by reducing the complexity of the tool and increasing perceived ease of use (whether in relation to using the tool itself, purchasing a policy and/or continued usage of associated security measures)</p>

D6.1: Concept note with the design of the economic experiments

2 Economic Experiments

2.1 Collaboration across Work Packages

Two CYBECO deliverables were considered in developing the economic experiments: 4.1 (Cyberinsurance Use-Cases and Scenarios) and 3.1 (Modelling Framework for Cyber Risk Management). In addition, as part of WP6 we used *Well Sorted*, an online tool designed to aid collaboration, to gather ideas and potential research questions from all CYBECO collaborators¹. At the first stage of the Well Sorted task, all collaborators were asked to submit up to three key ideas and/or research questions. Once everyone had completed the first stage, a second task asked everyone to group all the submitted ideas into themes. Five key themes emerged: *Social Norms* around cyberinsurance and cybersecurity, *Beliefs* about cyber insurance and personal cyberattack vulnerability, *Decision Making* regarding cybersecurity strategy (whether to invest in cyberinsurance), *Online Behaviour* including compliance with security strategy, unintentional behaviour change and moral hazard following commencement of cyberinsurance policy, and *Reporting Behaviour* including whether individuals and organisations report security incidents. The results are illustrated in Figure 4.²

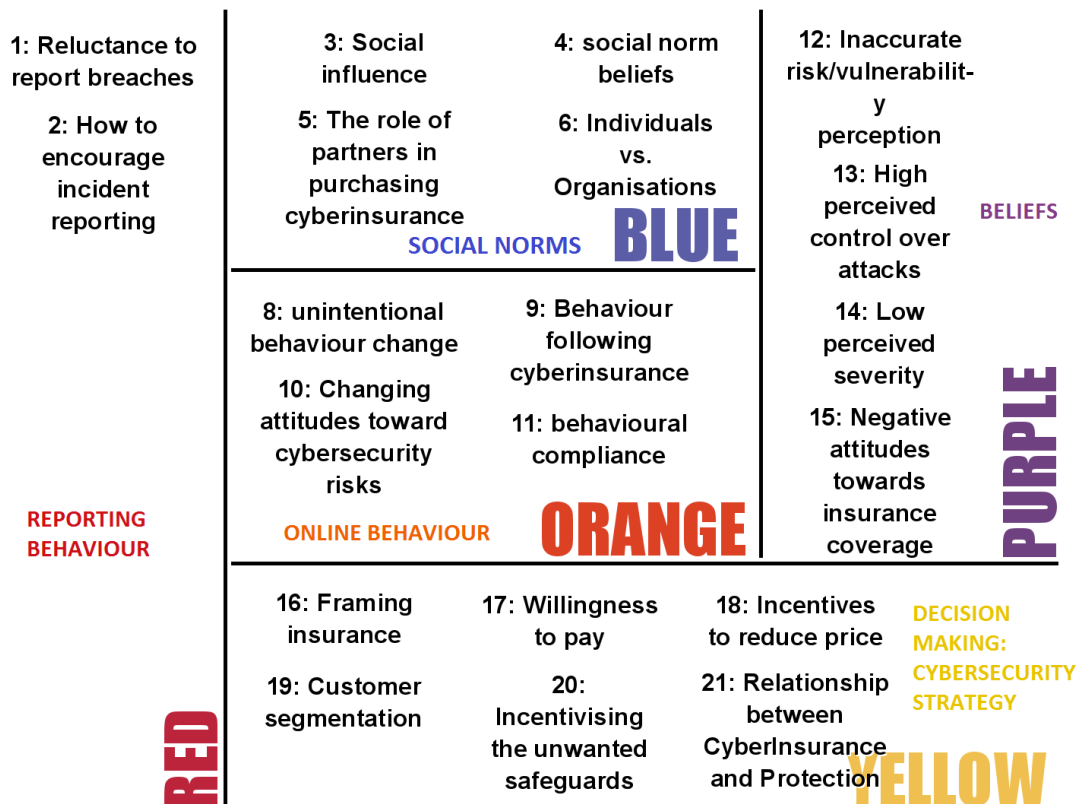


Figure 4: Results of the Well Sorted collaborative task

¹ *Well Sorted* was created by Heriot Watt University and funded by the EPSRC and Digital Economy

² Number 7 is excluded from the figure as one participant entered a blank response in error

D6.1: Concept note with the design of the economic experiments

The Well Sorted results were presented at the second plenary meeting in Valencia, 6-7th October 2017. Group discussion, including in-depth discussion with the DEVSTAT team, guided formation of a preliminary model of the decision-making process involved in the purchase (or not) of cyberinsurance and adherence to good cybersecurity behaviour. This model is shown in Figure 5 (Each of the five stages relate to the groups identified using the Well Sorted task, refer to Figure 4).

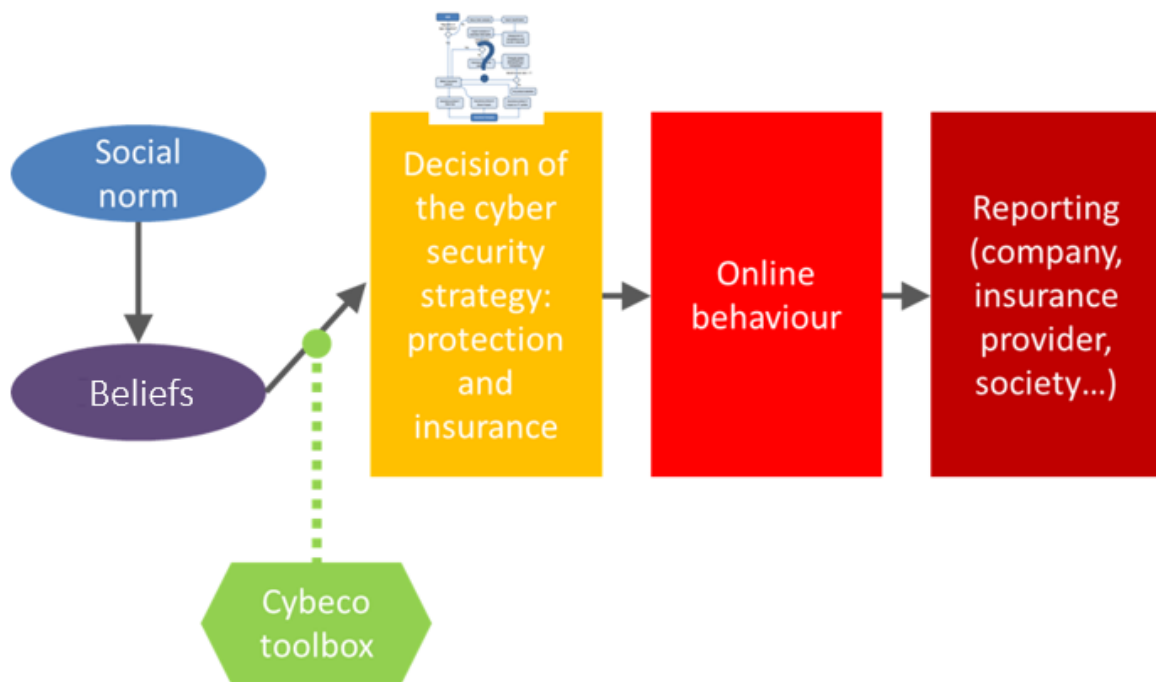


Figure 5: Preliminary model of cyberinsurance decision making and behaviour

This model was used to drive the following research questions for the two economic experiments:

2.2 Research Questions

1. How does actual cybersecurity decision-making compare to the predictions of the rational/normative model? (Experiment 1)
2. What nudges can be used to encourage optimal cybersecurity choices, and how effective are these? (Experiment 2)
3. What is the effect of experiencing a cyberattack on future likelihood to purchase cyberinsurance? (Experiments 1 & 2)
4. Which is the optimal pricing strategy for cyberinsurance products? (Experiments 1 & 2)

D6.1: Concept note with the design of the economic experiments

As described in section 2.3, the design of the experiments will allow for establishing the willingness to pay (WTP) for the different options of coverage of cyberinsurance products. The analysis of the WTP provides information on the maximum price that the potential insurance takers are willing to pay and can be understood as a measure of the actual value assigned by each participant to the different insurance products. Moreover, the different experimental conditions will allow for comparing the purchase decision under different pricing schemes (such as making the price depend upon the protection level of the firm or not). These two pieces of information will be used to establish the effect of pricing strategy of cyberinsurance products on purchase intention, and will support the definition of optimal pricing strategies for insurance companies.

The information collected through the questionnaires embedded in both experiments will identify critical features of the participant (such as risk attitude in experiment 1 or the profile of the SME in experiment 2) that will be used to check potential differences in behavioural responses (included the WTP). These behavioural insights will be used to define a segmentation of potential buyers and the most appropriate pricing strategy for each segment. Due to the sample sizes of both experiments, a statistical evidence-based segmentation analysis could be implemented for experiment 1, meanwhile the segmentation information from experiment 2 will be obtained from a more qualitative approach.

D6.1: Concept note with the design of the economic experiments

2.3 Experimental Designs

As described in CYBECO proposal, the project includes the implementation of two different experiments. The first one, with a large sample of general participants, is focused in the testing of the CYBECO model for cyber risk management. The second experiment, with a smaller sample of highly qualified participants, will be focused on the optimisation of the CYBECO tool. The first experiment will test different treatments related to how participants react to different features of the attack environment, as well as the protection and cyberinsurance products. It will also analyse how the attack expectations depend on the attack environment. The second experiment will be focused on the impact of the framing effects in the interface of CYBECO toolset and will support the design of nudges to help users to adopt the optimal combination of cyberinsurance and protection.

This concept note presents the main features of both experiments, that need to be calibrated and fine-tuned during the pilot phase of the experiment to be done with the beta version of the experimental software in the next phase of the project. Depending on the results of the experiments, additional experimental tests could be considered in the future, specifically in the topic of belief formation of the defender.

2.3.1 Rationale for economic experiments

The Experimental-Behavioural approach is an alternative and complementary method to traditional approaches – such as survey-based and qualitative methodologies - that allows studying consumer and citizen behaviour. This approach is based in the collection of information through economic experiments. An economic experiment is a scientific method of inquiry for studying how individuals interact in controlled settings defined by a specific set of rules. As in any other experimental science, an economic experiment is an orderly procedure carried out with the goal of verifying, refuting, or establishing the validity of a hypothesis. In comparison to simple statistical correlations, controlled experiments can help to provide insight into 'cause-and-effect'. An experiment can also control possible confounding factors, i.e., factors that could affect the accuracy or repeatability of the experiment or the ability to interpret the results. Confounding is commonly eliminated by randomly assigning participants to experimental conditions.

According to Smith (1991) every behavioural experiment is defined by three elements: environment, institutions and behaviour. The *environment* specifies the initial endowments and costs of the participants. This environment is controlled using monetary rewards to induce the desired specific value/cost configuration. The *institution* defines the language for communication with and among the subject (bids, offers, acceptances), the rules that govern the exchange of information, and the rules under which messages become binding contracts. The institution is defined by the experimental instructions, which describe the messages and procedures of the experiment, and are usually computer controlled. Finally, there is the observed *behaviour* of the participants in the experiments as a function of the environment.

D6.1: Concept note with the design of the economic experiments

Not all the behavioural experiments can be considered as economic experiments. There are two strict requirements that the experiment needs to fulfill to be considered as economic experiments, namely:

- Application of economic incentives
- Specific ethical considerations

2.3.2 The role of economic incentives

In general, methodologies to research about human behaviour (psychological experiment, quantitative surveys and test, qualitative research, etc.) do not apply economic incentives in the form of monetary rewards, with the only exception of a fixed payment to motivate participation, whose amount does not depend on the actual behaviour of the participant during the research session. This approach is usually known as *non-incentivised research methodology*. Non-incentivised research is based on the reaction of the consumers to hypothetical stimulus and such reactions have no real impact on the respondent. For instance, when participating in a standard survey-based conjoint analysis to determine the optimal configuration of an innovative product, the potential consumer is asked to order a series of different configurations of the product according to her or his preferences and questioned which of these configurations she or he would actually purchase. The information provided by the participant has no real impact on her or him: they just say how they would behave in a situation like that but no actual behaviour is observed. Moreover, since no real purchase decision is actually made, her or his state of mind is quite different from that when actual purchasing decision-making is involved. From the authors own experience when developing transfer of knowledge projects to industry – for instance in the finance sector – there is a generalised feeling of lack of reliability (not to say the accuracy) in the translation of the forecasting of some of these non-incentivised methods to actual consumer decision-making in the real world. For example, one of the authors recalls a private conversation with the head of investment products at a multinational Spanish bank during a knowledge transfer project, “one cannot avoid the feeling of being riding a wild horse when trying to apply survey predictions to what investors will actually do when facing innovative investment products”.

To cope with the issue of choosing hypothetical alternatives, the central feature of an economic experiment is the application of an *incentivised research methodology* or, in other words the use of economic rewards to generate a system of incentives for the experimental participants to respond to the factors presented in the different treatments in a realistic way. As discussed above when referring to the case of fixed monetary payments for participation, the simple presence of a reward is not enough for a method to be considered as incentivised. According to Smith (1991), three conditions are required for a monetary incentive to induce value: monotonicity, salience and dominance.

- *Monotonicity* implies that participants will always prefer a large incentive (and that they can also reach saturation). This condition is easily fulfilled if the reward is paid in actual currency. Monotonicity motivates participants to make the decision that maximises their

D6.1: Concept note with the design of the economic experiments

final reward (in our example the money available in cash at the end of the session and a complementary pair of sunglasses if the purchase takes place).

- *Salience* implies that a participant's reward is not fixed and will depend on her or his behaviour during the experiment (individual choice experiments) and even on the other participants' behaviour (collective choice experiments). Treatment 2 of the example experiment does not fulfill this condition.
- The requirement of *dominance* establishes that any change in the utility of participants is mainly determined by a change in her or his rewards and any other influence can be ignored. It is clear that this condition is the most difficult to achieve and constitutes the keystone for the success of any economic experiment.

From the seminal work of Holt & Laury (2002), the literature has confirmed the existence of significant differences between the results that are obtained in a very same situation when non-incentivised and incentivised methodologies are applied. Other instances closer to consumer behaviour, differences between incentivised and non-incentivised methods for the measurement of the maximum prize – willingness to pay (WTP) that a consumer would pay for a specific design of an innovative product or service are presented in the literature. For instance, in the absence of explicit and controlled motivation, participants may declare a higher willingness to pay for politically correct goals and social welfare-enhancing projects than they would otherwise reveal in an incentivised scenario (Nyborg, 2000). Hernández & Vila (2014) present a formal analysis of the impact of the use of experimental-behavioural economics in the measurement of the WTP. To the best of our knowledge, even the application of contingent and incentivised methodologies can be found in the literature, but there is no other example of a measurement of WTP in comparable conditions (same good and attributes) to test the existence of significant differences between the measurements obtained by experimental-behavioural methods and non-incentivised surveys.

2.3.3 Specific ethical considerations

Economic experiments need to respect all the ethical considerations - related both to the use of human participants and reporting and publishing results - that are applied in other disciplines involving research with human beings: experimental-behavioural methods can never cause negative implications for the researcher, the human participants, the sponsors, the implementers, future researchers, the potential beneficiaries of the research, and the public at large. However, experimental economics need to fulfill an additional consideration, that is not required in other fields such as clinical trials or psychological experiments, namely, non-deception of the participants and anonymity.

- *Deception* occurs when experimenters convey false or intentionally misleading information to participants. The use of deception in economic experiments is essentially forbidden (by virtue of the impossibility of getting deception past journal referees), and, as a matter of course, the discipline's distaste for deception is often the first thing

D6.1: Concept note with the design of the economic experiments

participants are told in economics experiments (Farinha, Ferreira, Smith, & Bagchi-Sen, 2015, p.133). The requirement of non-deception makes the design of some experiments more complex but enhance the validity of their results.

- *Anonymity.* In experimental-behavioural economics, researchers must always preserve the anonymity of the experiment participants. Researchers should announce that the data is used anonymously calculating averages and never with the aim to carry out a study of a particular participant with the aim to know his/her evolution along different experiments.

2.3.4 Validity of economic experiments

Validity refers to whether a study is able to scientifically address the questions that it intends to answer. The design of experimental research is crucial: without a valid design, accurate scientific conclusions cannot be drawn. Two different types of validity - internal and external – should be considered in any economic experiment:

- Internal validity is an inductive estimate of the degree to which conclusions about causal relationships can be made (e.g. cause and effect), based on the measures used, the research setting, and the whole research design. In other words, internal validity refers to the reliability of the conclusions obtained in the experiment when applied to the sample of participants participating in the session and to the specific framing of the experiment.
- External validity concerns the extent to which the (internally valid) results of a study can be extrapolated for other beyond the experimental session, for example to different people, places or times. In other words, it is about whether conclusions can be validly generalised.

Summarising, internal validity is focused on the research design and its causal relation, while external validity focuses on the findings obtained. Researchers must look for an optimal equilibrium between both types of validity that allows them to elucidate the pertinent question.

2.4 Experiment 1: Testing the model (Defender)

Experiment 1 aims to test the CYBECO model from a behavioural-experimental viewpoint. Specifically, experiment 1 will compare the 'rational optimal' behaviour forecasted by the CYBECO model with the 'human actual behaviour' when purchasing cyber protection and insurance. The information of this experiment will be applied to identify effective behavioural levers in the design and communication of these product in order to nudge towards optimal cybersecurity behaviour.

The rationale of this experiment is as follows. Participants will be invited to make decisions related to the purchase of cyber insurance and protection products in an online controlled economic experiment. In a role of IT heads in a SME, participants will perform a simple task

D6.1: Concept note with the design of the economic experiments

online, specifically they will access a travel comparison website to check the price of a return flight to Brussels. To enter the comparison website, they will create a password provide some personal information (compulsory and non-compulsory fields) and log out after finding the information. Before accessing the comparison site, participants will be informed that they may suffer a cyberattack, depending on how safely they behave when browsing. After that, participants will be offered the chance to buy a protection measure (to reduce the probability of suffering the attack) and/or a cyberinsurance product, that will pay back in case of cyberattack.

The experiment will include two independent phases, each of them presenting the opportunity to buy cyberinsurance and protection measures and to navigate to find the flight information. At the end of each phase, participants will obtain a payoff that will depend on all their decisions during the experiment and the fact of suffering or not the cyberattack.

Experiment 1 is proposed to be implemented with 4000 participants to be recruited through an online panel and representative of general population of internet users in four European countries. However, the sample could be extended to 4.800 to allow for a 3X4 factorial design, i.e. 12 experimental condition, with 100 participants³ in each country in each of the 12 experimental conditions in the design, as described in Table 3. The average payoff to be received by each subject, as a consequence of her or his decisions during the experiment, need to be calibrated in the final design of the experiment.

2.4.1.1 Description of the behavioural experiment

Experiment 1, as illustrated in Figure 6, will be structured in the following steps:

- Participants will receive an e-mail invitation to participate in the experiment. The invitation will include:
 - The description of the experiment (objectives, supporting institution, etc.)
 - Duration of the experiment
 - Fixed incentive and maximum variable incentive they can get, depending on their decisions during the experiment.
 - Consent form to be completed before participation.
- If they accept to participate, they will be invited to complete a brief questionnaire (Questionnaire 1) with their socio-demographic profile and basic question of their internet usage. After that, they are then automatically sent to the experimental software.

³ This design provides a sample size of 400 subjects per experimental condition, which guaranties a sampling error for the estimation of the percentage of subjects in each treatment following a given behavioural response lower than 5% (with a confidence level of 95%).

D6.1: Concept note with the design of the economic experiments

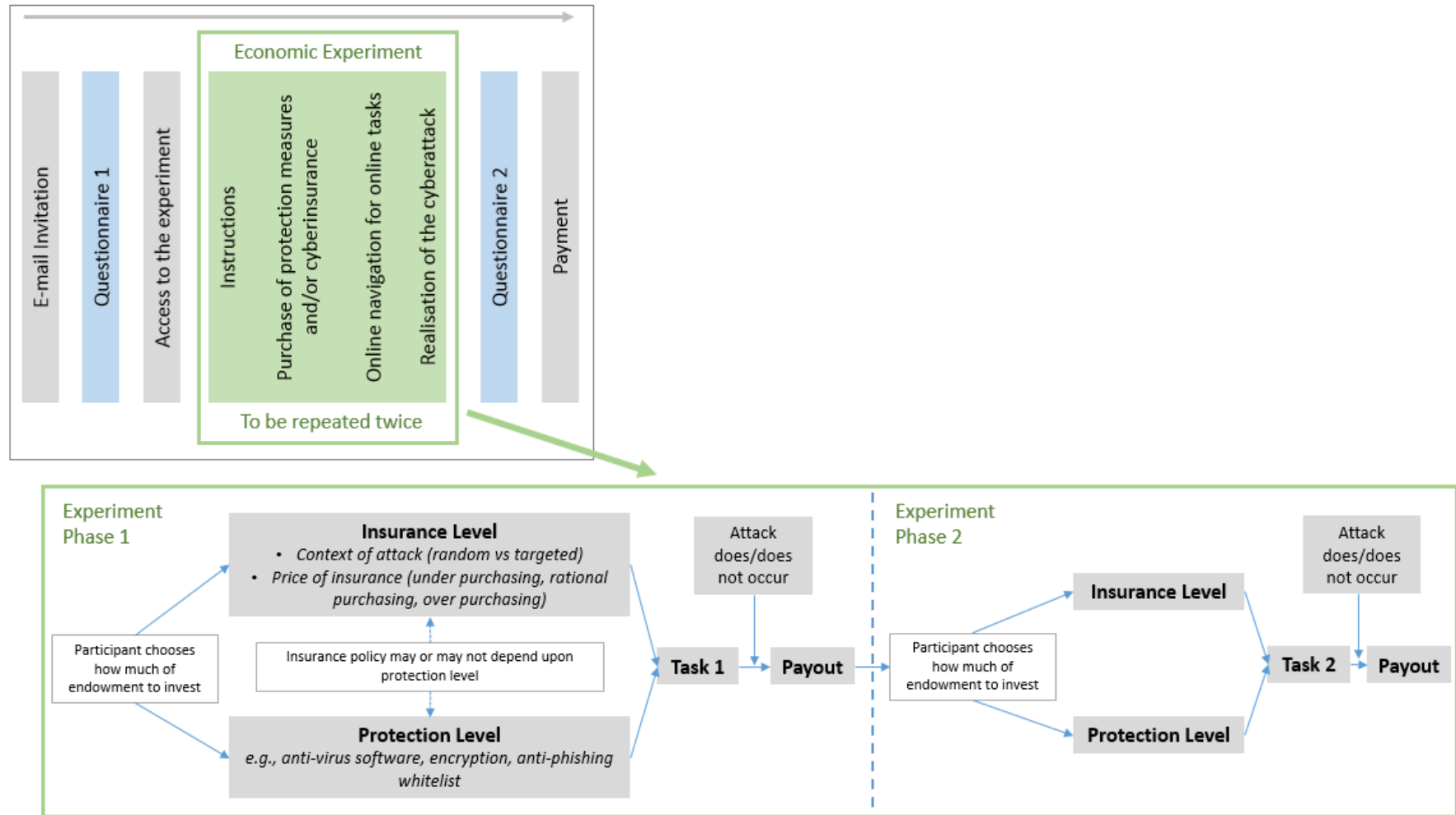


Figure 6: Design of Experiment 1

D6.1: Concept note with the design of the economic experiments

- A screen with instructions will be shown, explaining that:
 - The participant will play the role of IT head of a medium SME
 - The experiment will be structured in two phases. In each of them, the participant will be asked to perform simple tasks online. Each phase (and its corresponding payoff) is completely independent from the other.
 - The participant will be provided with an initial endowment for each phase.
 - The participant will be informed that, in each phase of the experiment, she or he may suffer a cyberattack and lose all their endowment. It will be clearly established that the cyber-attack will take place within an experimental setup and cannot affect them in any way beyond losing the endowment at each of the phases. The participant will know that the likelihood of the attack will depend on their level of security when navigating in the website.
- After understanding how the experiment works, the participant will be offered to purchase:
 - A protection measure (such as an antivirus or firewall) which will reduce the likelihood of suffering the attack.
 - Cyberinsurance products with different coverage levels, i.e. these products will cover totally or partially the loss of the endowment in case of attack.

They can buy or not buy the protection measure and the cyberinsurance independently. The price of the insurance may depend on whether they purchased the protection measure or not. Participants will decide what to purchase and the price will be discounted from their initial endowment

- The participant will be asked to proceed to a comparison website and check the prices of a round flight from Moscow to Brussels Zaventem and report which is the cheapest flight. If they do not report this information properly, they will not receive the final variable payoff corresponding to this phase of the experiment.
- The participant will be required to complete a registration form to access the comparison website. To this end, she or he needs to create a password and provide several pieces of private information, some of them compulsory and other not. They can also read the information on cookies and security policy of the website by clicking in the corresponding link.
- Once on the comparison website, the participant will look for the information and report the cheapest flight. After completing the task, she or he will have the chance to log-out from the site.
- Steps 4 to 7 will be repeated in the second phase of the experiment.
- Questionnaire 2, with self-revealed information on beliefs, cybersecurity levels and social norms. Depending on the length of the questionnaire, a test to calibrate value and weighting functions, such as Holt and Laury test (Holt & Laury, 2002), could be included in this second questionnaire.

D6.1: Concept note with the design of the economic experiments

- The participant will receive the payoffs obtained in phases 1 and 2 of the experiment, given by:
 - Endowment
 - - Costs of insurance in step 1 (if any) - Costs of protection in step 1 (if any) - Costs of cyberattack in step 1 (if any) + Coverage of the cyber insurance policy in step 1 (if any)
 - - Costs of insurance in step 2 (if any) - Costs of protection in step 2 (if any) - Costs of cyberattack in step 2 (if any) + Coverage of the cyber insurance policy in step 2 (if any)

2.4.1.2 Behavioural measures

Experiment 1 will include the following behavioural measures to be analysed in terms of the different experimental conditions:

- Purchase of cyberinsurance products in phases 1 and 2 of the experiment.
- Purchase of the protection measure in phases 1 and 2 of the experiment.
- How safely they behave during online navigation, measured through the security level of the password, provision or not of non-compulsory private information, consultation of the terms and conditions and log out.

The first two behavioural measures will allow for comparing the actual behaviour of the participants with the optimal normative behaviour established by the CYBECO model. To this end, a simulation of the CYBECO model will be run with the specific parameters considered in the experimental setting. The result of the simulation will provide the normative optimal protection-insurance strategy that can be compared with the strategy actually implemented in the experiments by the participants. Additionally, they will allow testing which design of the insurance product (see treatments P1, P2, I1, I2 and I3 in the next subsection) minimises such a difference. A last goal of these measures, for these participants who suffered a cyberattack in the first phase of the experiment, is to analyse how the experience of the attacks affects their willingness to purchase insurance products and protection measures.

The last measure will quantify how safely the online behaviour of the participant is and will be used to identify how this level is affected by the purchase of the protection measure and cyberinsurance and, in the second phase of the experiment, how this behaviour changes after suffering a cyberattack.

2.4.1.3 Experimental conditions

The 12 experimental conditions will be based on different features of the insurance / protection elements, as well as the potential context of the cyberattack. Specifically, the experiment will follow a complete factorial design with three factors (context, protection, insurance), the first and second with two levels and the last one with three. Table 3 presents the proposed treatments:

D6.1: Concept note with the design of the economic experiments

Table 3. Proposed treatments for Experiment 1.

Factors	Levels
Context of the cyberattack (C)	<ul style="list-style-type: none"> • C1: The attack is random (there is a virus in the Internet that may affect randomly to any user). Subject is informed of the average probability of suffering an attack as the percentage of similar users that have suffered the random virus attack in the last week. • C2: The attack is intentional (in an adversarial analysis framework, the attack is intentionally launch by a cyber-criminal). Subject is informed of the average likelihood of suffering an attack as the percentage of similar users that have suffered the intentional attack in the last week
Relation of the protection measure and the price of the cyber insurance product (P)	<ul style="list-style-type: none"> • P1: The price of the insurance does not depend on the protection level • P2: The price of the insurance does depend on the protection level
Features of the cyber insurance product (I)	<ul style="list-style-type: none"> • I1: Low price (under purchasing price considering rationality) • I2: Medium price (purchasing price considering rationality) • I3: High price (over purchasing price considering rationality)

Factor C1 is introduced in the experiment to analysis a critical and innovative element of the CYBECO model, specifically how the participant creates her or his believes in the chances to suffer an attack and how these believes change when moving from a random approach (the victims of the attack are selected and random as a consequence of a virus) to the adversarial approach (the victims of the attack are selected intentionally by a cybercriminal).

Factors P and I are related to the design of the cyberinsurance products. They refer to two critical features of the product, specifically of the pricing strategy, as the relation of the prime with the security level of the company (factor P) and the value of the prime (factor I) in comparison with the actuarially fair price. Factor P will help to define the pricing strategy, in order to define the optimal pricing schemes to nudge towards the normative protection/insurance strategy.

Notice that, beyond the three factors in Table 3, the questionnaires will provide additional information of the subjects (socio-demographic profile including country, previous experiences in cybersecurity issues, risk attitude, etc.) that can be used for segmentation of users.

2.4.2 Experiment 2: Optimising the CYBECO toolbox

Experiment 2 aims to test the CYBECO toolbox: asking users to report on their cybersecurity situation and suggesting the optimal insurance/protection strategy for their SME. The toolbox takes the form of an online calculator to guide the user through analysing their current cybersecurity risk level and deciding the optimal cybersecurity strategy for their needs. The calculator will be a multi-step form which asks pertinent questions (e.g., SME size, characteristics, relevant threats, available security measures) and offers the best option for the SME based on the outcomes of CYBECO cyber risk management models.

D6.1: Concept note with the design of the economic experiments

Online tools in the form of calculators have been used widely for other purposes such as health and life insurance (examples provided in figures 7 & 8). These tools are designed to guide users step by step through the quotation and application process and claim to provide an accurate calculation of how much insurance an individual should purchase (Adelman, Dorfman, & Wells, 2003).

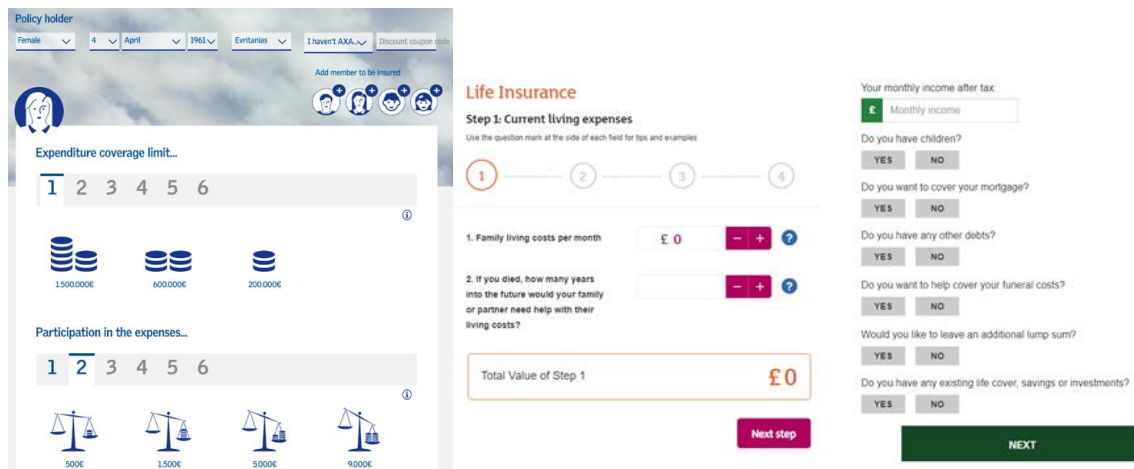


Figure 7: Life insurance calculators (Left to right: AXA; Sainsbury's Bank; Legal & General, 2017)

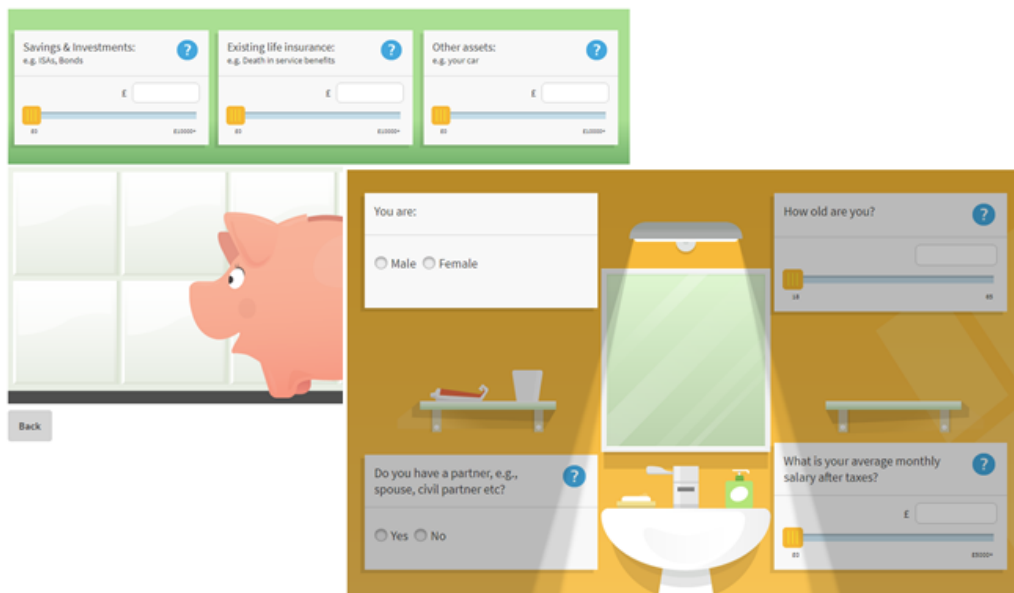


Figure 8: Life Insurance Calculator (Aviva, 2017)

Online calculators have not yet been widely applied to the cybersecurity market, with many insurance providers currently requesting that cyberinsurance quotations are conducted via telephone (e.g., Swinton Insurance). Of the limited tools that do exist (e.g., cyberguru.co.uk), most enable the user to request a quotation and ask the user specifically what level of cover

D6.1: Concept note with the design of the economic experiments

(£) they require, rather than helping with the actual calculation and decision-making process (including how to decide how much to invest in cyberinsurance versus self-protection measures). Some insurer brokers have set up websites to help calculate overall cyber risk level and vulnerability to breaches (e.g., privacyriskadvisors.com and hubinternational.com). However, the theory behind these tools is unclear. It is important that online tools are supported by a solid theoretical background. There are concerns that some health insurance calculators may oversimplify the calculation and decrease understanding of the theories behind it (Elger, 2003). Whilst some research suggests that recommendations provided by online calculators can be variable and inaccurate, this has been attributed to inadequate input (e.g., due to ambiguous instructions, omission of key requests and inflexible input formats) and inaccurate or illogical underlying mathematical models (Adelman et al., 2003; Dorfman & Adelman, 2002). Tools must be well designed to limit variation from poor quality input variables.

Another potential role of insurance calculators, from a behavioural economics perspective, is to *nudge* the purchaser to adopt the optimal solution. For instance, in the field of life insurance, purchasers tend to select insurance coverages that are under the optimal value, mainly due to loss aversion (i.e., perceiving the insurance policy premium as a loss to their income) and hyperbolic time discount/present bias (i.e., tendency to give stronger weight to payoffs in the present time, e.g., saving cost of policy, compared to future payoffs, e.g., family's future gain)). Manipulating the framing of the information requested/presented by the calculator can change the final decision of the insurance taker, in terms of the selected coverage. A similar effect is expected to arise in a cyberinsurance calculator, where the framing of information may affect the selected combination of protection and cyberinsurance measures.

2.4.3 Description of behavioural experiment 2

The sample for experiment 2 (Figure 9) will consist of either actual decision makers of SMEs or autonomous workers (entrepreneurs, freelancers, etc.). Due to the complexity to access this profile of respondents, the experiment will be run on a small sample of 200 participants to be recruited from online panels. The average payoff to be received by each subject, as a consequence of her or his decisions during the experiment, need to be calibrated in the final design of the experiment.

Participants will be invited to use a calculator to help guide their simulated purchase of cyberinsurance products and/or protection measures. This calculator will be the core of the CYBECO tool. This will be a two-phase experiment. In the first phase, participants will use the calculator to provide basic information on their cybersecurity status and will receive a suggestion of which should be their optimal combination of protection measures and insurance products. This optimal suggestion will be calculated based upon the CYBECO model (as detailed in WP3.1). In the second phase, participants will be assigned an initial endowment and will be asked to participate in an incentivised simulation where they can purchase a combination of insurance and protection measures. Their choice will impact their experimental payoff (if they suffer a cyberattack during the experiment). The experiment will also include

D6.1: Concept note with the design of the economic experiments

pre- and post- questionnaires to provide classification information and evaluate the cyberinsurance calculator respectively.

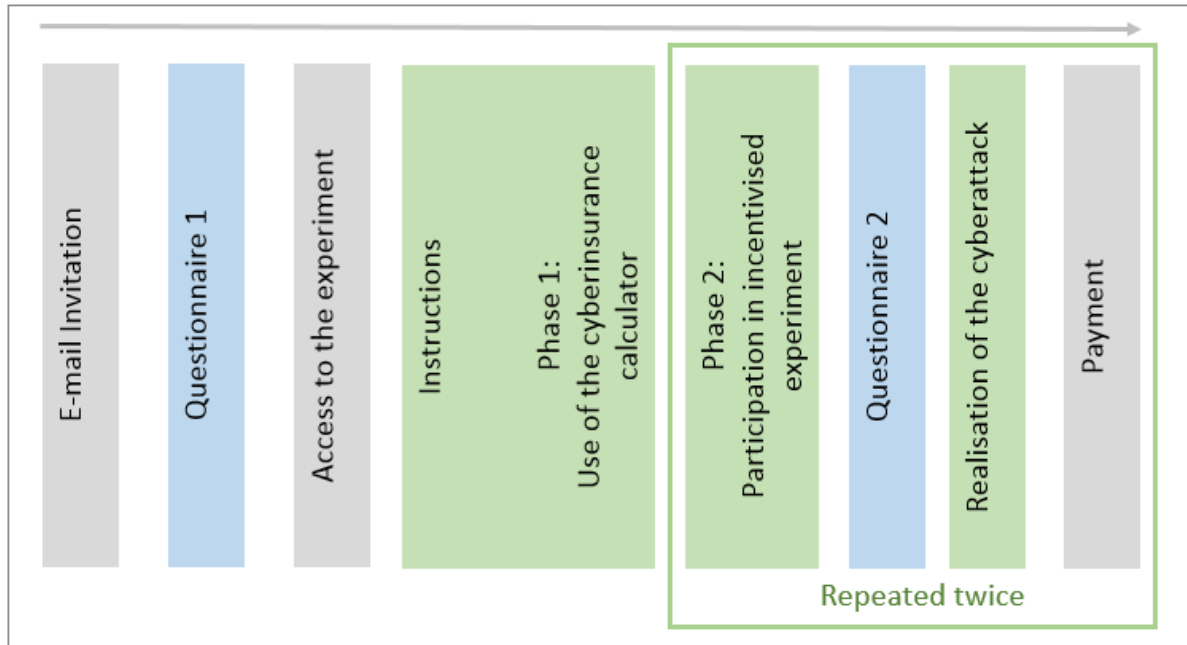


Figure 9: Design of Experiment 2

1. Participants will receive an e-mail invitation to participate in the experiment. The invitation will include:
 - a. An overview of the experiment (e.g., objectives, supporting institution, duration of experiment)
 - b. Information regarding the incentives they can receive (including a fixed incentive, and the maximum variable incentive that they can potentially receive depending upon their decisions during the experiment).
 - c. Consent form to be completed before participation.
2. If they consent to participate, they will be invited to complete a brief questionnaire (questionnaire 1) with their socio-demographic profile and basic classification questions about their SMEs (activity, size, etc.). After that, they will be automatically re-directed to the experimental software.
3. A screen with instructions will be shown, explaining that:

The experiment will be structured in two phases. In the first phase, the participant will test a cyberinsurance calculator. In the second phase, they will be invited to participate in an incentivised game. They will be provided with an initial endowment, and asked to choose their preferred level of cyber protection and/or cyberinsurance. They will be

D6.1: Concept note with the design of the economic experiments

informed that there is a possibility that they may suffer a cyberattack and depending upon their level of protection/insurance they may lose all of their endowment. It will be clearly established that the cyberattack will take place within an experimental setup and cannot affect the participant in any way beyond affecting the level of endowment they receive from the experiment. The participant will be aware that the likelihood of a successful attack will depend upon their level of security (i.e., the combination of protection/insurance that they chose).

4. Phase 1:

The participant will use the cyberinsurance calculator:

- a. To provide information on current cybersecurity and security requirements in relation to their SME/self-employment.
- b. To obtain a recommendation of the optimal protection-insurance strategy for their business.

The participant will receive their initial endowment and will be present with instructions to complete the second phase of the experiment.

5. Phase 2 (First pass):

The participant will be offered the opportunity to use some of their endowment to purchase a protection measure(s) - consisting of self-protection measures and/or cyberinsurance. The options will include those suggested by the calculator, among others. After choosing their protection measure(s), the participant will complete an online questionnaire. During this process, they may be alerted that they have suffered a random cyberattack generated by a virus in the network. The probability of the attack is influenced by their level of self-protection measures. If the attack takes place, the participant will lose all the endowment, except for any value which has been covered by cyberinsurance. The parameters of the game will be adjusted to the information provided by the participant to the calculator.

6. Phase 2 (Second pass):

After receiving information about whether an attack was suffered in the first pass of phase 2, the participant will be asked to make another decision regarding how much of their endowment they wish to use to purchase self-protection measures and/or cyberinsurance.

7. The participant will complete another online questionnaire (Questionnaire 2: self-revealed information on beliefs, cybersecurity levels and social norms in cyberinsurance and a user-evaluation of the calculator)
8. The participant will be informed if they have or have not suffered another cyberattack and advised on their remaining endowment.

D6.1: Concept note with the design of the economic experiments

9. The participant will receive the payoff obtained in phases 1 and 2 of the experiment. This payoff will consist of their endowment minus any costs of self-protection measures and/or cyberinsurance, minus any costs as a result of experienced cyberattacks (if any). In the case of an attack being experienced but cyberinsurance being purchased, the participant will also receive any lost value that was subsequently covered by the insurance policy

i.e., $\text{Payoff} = \text{endowment} - \text{any costs of insurance} - \text{any costs of protection} - \text{any costs of cyberattack(s)} + \text{any experienced losses covered by cyberinsurance policy}.$

Behavioural measures

The following behavioural measures will be analysed for the different experimental conditions:

- Differences between the strategy suggested by the calculator (optimal choice) and participant decision making (actual choice) in the incentivised experimental situation. This will identify the effectiveness of the CYBECO calculator for nudging towards optimal cybersecurity levels.
- How cybersecurity decision-making is affected by the experience of a prior cyber-attack
- Valuation of the cyberinsurance calculator from the perception of the user(s).

Experimental conditions

The experimental conditions in Experiment 2 will consist of the combination of two alternative framings for data collection and two alternative framings for the presentation of the insurance/protection strategy suggested by the calculator. The specific framing will be guided by protection-motivation theory (PM) as this model is particularly useful when we are aiming to encourage individuals/organisations to *protect* their business and/or assets from cyber-threat (Briggs, Jeske, & Coventry, 2016), but the precise design will depend in part on the outcome of behavioural experiment 1. The decision to invest in self-protection and/or insurance depends upon how threat is appraised: both in relation to severity of (and vulnerability to) the *threat* and ability to *cope* with the threat.

D6.1: Concept note with the design of the economic experiments

3 Conclusion

This concept note outlines the current literature around cyberinsurance to support the design of CYBECO economic experiments, including the need for positive interventions to increase good cybersecurity behaviour. Having highlighted this current need, we have designed and introduced two economic experiments that will be conducted as part of the CYBECO project. The first experiment tests the CYBECO model of cybersecurity behaviour and decision-making, whilst the second experiment tests the CYBECO toolbox (also designed as part of this project) and identifies potential nudges to encourage increased cybersecurity and cyberinsurance uptake. We note that the final design of the second experiment will critically depend upon some of the emerging design features incorporated into an early prototype of the toolbox and would therefore be subject to some (minor) change.

D6.1: Concept note with the design of the economic experiments

4 References

- Abdellaoui, M., L'Haridon, O., & Paraschiv, C. (2011). Experienced vs. Described Uncertainty: Do We Need Two Prospect Theory Specifications? *Management Science*, 57(10), 1879–1895. <https://doi.org/10.1287/mnsc.1110.1368>
- Adelman, S. W., Dorfman, M. S., & Wells, B. (2003). A grading system for evaluating Internet life insurance needs calculators - ProQuest. *Financial Services Review*, 12(3), 239–255. Retrieved from <https://search.proquest.com/docview/212004762?pq-origsite=gscholar>
- Advisen. (2015). *2015 Network Security & Cyber Risk Management: The Fourth Annual Survey of Enterprise-Wide Cyber Risk Management Practices in Europe*.
- Aguilar, L. A. (2015). *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*. Retrieved from <https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., ... Agarwal, Y. (2015). Your Location has been Shared 5,398 Times! In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15* (pp. 787–796). <https://doi.org/10.1145/2702123.2702210>
- Alventosa, A., Gómez, Y., Martínez-Molés, V., & Vila, J. (2016). Location and Innovation Optimism: a Behavioral-Experimental Approach. *Journal of the Knowledge Economy*, 7(4), 890–904. <https://doi.org/10.1007/s13132-015-0291-2>
- Baer, W. S. (2003). Rewarding IT security in the marketplace. *Contemporary Security Policy*, 24(1), 190–208. <https://doi.org/10.4324/9780203005859>
- Baer, W. S., & Parkinson, A. (2007). Cyberinsurance in IT Security Management. *IEEE Security & Privacy Magazine*, 5(3), 50–56. <https://doi.org/10.1109/MSP.2007.57>
- Baicker, K., Congdon, W. J., & Mullainathan, S. (2012). Health insurance coverage and take-up: lessons from behavioral economics. *The Milbank Quarterly*, 90(1), 107–34. <https://doi.org/10.1111/j.1468-0009.2011.00656.x>
- Bailey, L. M. (2014). Mitigating Moral Hazard in Cyber-Risk Insurance. *3 J.L. & Cyber Warfare*, 3(1), 42. <https://doi.org/10.1525/sp.2007.54.1.23>
- Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, 52(11), 68. <https://doi.org/10.1145/1592761.1592780>
- Bandyopadhyay, T., & Shidore, S. (2011). Towards a Managerial Decision Framework for Utilization of Cyber Insurance Instruments in IT security Towards a Managerial Decision Framework for Utilization of Cyber Insurance Instruments in IT security. In *In Proc of AMCIS 2011*.
- Barlette, Y., & Fomin, V. V. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 308–308). IEEE. <https://doi.org/10.1109/HICSS.2008.167>
- Betterley, R. (2010). *Understanding the cyber risk insurance and remediation services marketplace*.
- Betterley, R. (2014). *Cyber/privacy insurance market survey*.
- Bhargava, S., Loewenstein, G., & Sydnor, J. (2015). *Do Individuals Make Sensible Health Insurance Decisions? Evidence from a Menu with Dominated Options*. Cambridge, MA.

D6.1: Concept note with the design of the economic experiments

<https://doi.org/10.3386/w21160>

- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131–158. <https://doi.org/10.1057/gpp.2014.19>
- Briggs, P., Jeske, D., & Coventry, L. (2016). Behavior Change Interventions for Cybersecurity. In *Behavior Change Research and Theory: Psychological and Technological Perspectives* (pp. 115–136). <https://doi.org/10.1016/B978-0-12-802690-8.00004-9>
- Browne, M. J., & Hoyt, R. E. (2000). The Demand for Flood Insurance: Empirical Evidence. *Journal of Risk and Uncertainty*, 20, 3–291. <https://doi.org/10.1023/A:1007823631497>
- Choi, J., Laibson, D., & Madrian, B. (2006). *Reducing the Complexity Costs of 401(k) Participation Through Quick Enrollment(TM)*. Cambridge, MA. <https://doi.org/10.3386/w11979>
- Coles-Kemp, L., & Overill, R. E. (2007). On the role of the Facilitator in information security risk assessment. *Journal in Computer Virology*, 3(2), 143–148. <https://doi.org/10.1007/s11416-007-0040-6>
- Corner, S. (2014, April 3). Billions spent on cyber security and much of it “wasted.” *The Sydney Morning Herald*. Retrieved from <http://www.smh.com.au/it-pro/security-it/billions-spent-on-cyber-security-and-much-of-it-wasted-20140402-zqprb.html>
- Crane, M. (2001). International liability in cyberspace. *Duke Law & Technology Review*, 1(1).
- Crowther, J., Dabbs, D., Dakin, S., Freed, A. M., Herold, R., Kam, R., ... Messing, I. E. (2013). *Data privacy, information security and cyber insurance trend*.
- Cybersecurity Ventures. (2017). *Ransomware Damage Report*. Retrieved from <https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/>
- Das, S. (2017). *Social Cybersecurity: Reshaping Security Through An Empirical Understanding of Human Social Behavior*. Retrieved from <http://repository.cmu.edu/dissertations>
- Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results. *Management, Ph.D.*, 291. <https://doi.org/oclc/56932490>
- Deloitte. (2017). *Demystifying cybersecurity insurance*. Retrieved from <https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html>
- Dorfman, M. S., & Adelman, S. W. (2002). An Analysis of the Quality of Internet Life Insurance Advice. *Risk Management & Insurance Review*, 5(2), 135–154. <https://doi.org/10.1111/1098-1616.00012>
- Elger, J. F. (2003). Calculating life insurance need: Don’t let the tools fool you - ProQuest. *Journal of Financial Service Professionals*, 57(3), 38–40. Retrieved from <https://search.proquest.com/docview/209616832?pq-origsite=gscholar>
- Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5). <https://doi.org/10.1108/JRF-09-2016-0122>
- ENISA. (2012). Incentives and barriers of the cyber insurance market in Europe, (June), 45.
- Esposito, G., Hernández, P., van Bavel, R., & Vila, J. (2017). Nudging to prevent the purchase of incompatible digital products online: An experimental study. *PLOS ONE*, 12(3), e0173333. <https://doi.org/10.1371/journal.pone.0173333>
- Experian. (2013). *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*.
- Farinha, L. M., Ferreira, J. J. M., Smith, H. L., & Bagchi-Sen, S. (2015). *Handbook of Research on Global*

D6.1: Concept note with the design of the economic experiments

Competitive Advantage through Innovation and Entrepreneurship. Handbook of Research on Global Competitive Advantage through Innovation and Entrepreneurship.
<https://doi.org/10.4018/978-1-4666-8348-8>

- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13–23.
<https://doi.org/10.1016/J.DSS.2016.02.012>
- Garrie, D., & Mann, M. (2014). Cyber-Security Insurance: Navigating the Landscape of a Growing Field. *John Marshall Journal of Information Technology and Privacy Law*, 31. Retrieved from <http://heinonline.org/HOL/Page?handle=hein.journals/jmjcila31&id=380&div=19&collection=journals>
- Gilovich, T., Griffin, D., & Kahneman, D. (2002). *Heuristics and Biases The Psychology of Intuitive Judgment*. London: UK: Cambridge University Press. Retrieved from <http://www.cambridge.org>
- Gohring, N. (2002, July). Cyberinsurance may cover damage of computer woes. *Seattle Times*.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 34(5), 509–519. <https://doi.org/10.1016/J.JACCPUBPOL.2015.05.001>
- Hanoch, Y., Barnes, A., & Rice, T. (2017). *Behavioral Economics and Healthy Behaviors: Key Concepts and Current Research*. Retrieved from https://books.google.co.uk/books?hl=en&lr=&id=YTgkDwAAQBAJ&oi=fnd&pg=PT210&dq=nudges+for+insurance+purchjases&ots=YGzKMqAcJF&sig=_-cswuZ3pbk4fDaV7RyXft1xue8#v=onepage&q=nudges+for+insurance+purchjases&f=false
- Henson, R., & Garfield, J. (2015). What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security ? In *ATINER, 12th Annual International Conference on SME's, Entrepreneurship and Innovation: Management –Marketing – Economic – Social Aspects*, 27-30 July 2015, Athens, Greece. (pp. 1–19).
- Hernández, P., & Vila, J. (2014). Measuring value levers: Experimental and contingent approaches. *Journal of Business Research*, 67(5), 775–778. <https://doi.org/10.1016/j.jbusres.2013.11.043>
- Hiscox. (2017). *The Hiscox Cyber Readiness Report*. Retrieved from <https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf>
- Holt, C. A., & Laury, S. K. (2002). Risk aversion and incentive effects. *American Economic Review*, 92(5), 1644–1655. <https://doi.org/10.1257/000282802762024700>
- Johnson, E. J., Shu, S. B., Dellaert, B. G. C., Fox, C., Goldstein, D. G., Häubl, G., ... Weber, E. U. (2012). Beyond nudges: Tools of a choice architecture. *Marketing Letters*, 23(2), 487–504. <https://doi.org/10.1007/s11002-012-9186-1>
- Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., & Pestell, G. (2017). *Cyber security breaches survey*. Retrieved from <http://www.ipsos-mori.com/terms>.
- Kunreuther, H. (1996). Mitigating Disaster Losses through Insurance. *Journal of Risk and Uncertainty*, 12, 171–187.
- Kuru, D., & Bayraktar, S. (2017). The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime The Journal of Risk Finance Iss Journal of Financial Crime*, 24(2), 329–346. <https://doi.org/10.1108/JFC-05-2016-0035>
- LLC, P. I. (2013). *Managing cyber security as a business risk: Cyber insurance in the digital age*.
- Lloyds of London. (2017). *Counting the cost: cyber exposure decoded. Emerging Risks Report*. Retrieved from <https://www.lloyds.com/news-and-insight/risk->

D6.1: Concept note with the design of the economic experiments

insight/library/technology/countingthecost

- Loewenstein, G., Friedman, J. Y., McGill, B., Ahmad, S., Linck, S., Sinkula, S., ... Volpp, K. G. (2013). Consumers' misunderstanding of health insurance. *Journal of Health Economics*, 32(5), 850–862. <https://doi.org/10.1016/j.jhealeco.2013.04.004>
- Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud and Security*, 2017(4), 18–20. [https://doi.org/10.1016/S1361-3723\(17\)30034-9](https://doi.org/10.1016/S1361-3723(17)30034-9)
- Majuca, R. P., Yurcik, W., & Kesan, J. P. (2005). The evolution of cyberinsurance. *Information Systems Frontiers*, 1–16.
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*. <https://doi.org/10.1016/j.cosrev.2017.01.001>
- Meland, P. H., Tondel, I. A., & Solhaug, B. (2015). Mitigating Risk with Cyberinsurance. In *Economics of Information Security (Advances in Information Security)* (Vol. 13, pp. 38–43). <https://doi.org/10.1109/MSP.2015.137>
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, 56(1), 11–26. <https://doi.org/10.1016/j.dss.2013.04.004>
- National Conference of State Legislatures. (2017). *Security Breach Notification Laws*. Retrieved from <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>
- Needleman, S. E. (2012, July 5). Cybercriminals Sniff Out Vulnerability. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/SB10001424052702303933404577504790964060610>
- Nexus. (2016). *The State of Cybersecurity: Implications for 2016*. Retrieved from https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf
- Nyborg, K. (2000). Homo Economicus and Homo Politicus: interpretation and aggregation of environmental values. *Journal of Economic Behavior and Organization*, 42(3), 305–322. [https://doi.org/10.1016/S0167-2681\(00\)00091-3](https://doi.org/10.1016/S0167-2681(00)00091-3)
- Ogut, H. U., Menon, N., & Raghunathan, S. (2005). Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. In *In Proc of the 4th Workshop on the Economics of Information Security* (pp. 1–30).
- Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2017). Security Pricing as Enabler of Cyber-Insurance A First Look at Differentiated Pricing Markets. *IEEE Transactions on Dependable and Secure Computing*, 1–1. <https://doi.org/10.1109/TDSC.2017.2684801>
- Parkes, A. (2009). Persuasive Decision Support: Improving Reliance on Decision Support Systems. *PACIS 2009 Proceedings*. Retrieved from <https://aisel.aisnet.org/pacis2009/11>
- Perloth, N. (2014, February 5). Heat System Called Door to Target for Hackers. *The New York Times*.
- Perren, K., Yang, L., He, J., Yang, S.-H., & Shan, Y. (2016). Incorporating persuasion into a decision support system: The case of the water user classification function. In *2016 22nd International Conference on Automation and Computing (ICAC)* (pp. 429–434). IEEE. <https://doi.org/10.1109/IConAC.2016.7604957>
- Pfleeger, S. L., & Caputo, D. D. (2012). *Leveraging Behavioral Science to Mitigate Cyber Security Risk*. Retrieved from <https://ai2-s2-pdfs.s3.amazonaws.com/e755/aa8baf01ef655ef7b1472ceba505b7c45b91.pdf>
- Preston, M. G., & Baratta, P. (1948). An experimental study of the auction-value of an uncertain

D6.1: Concept note with the design of the economic experiments

- outcome. *The American Journal of Psychology*, 61(2), 183–193. <https://doi.org/10.2307/1416964>
- Quiggin, J. (1982). A theory of anticipated utility. *Journal of Economic Behavior and Organization*, 3(4), 323–343. [https://doi.org/10.1016/0167-2681\(82\)90008-7](https://doi.org/10.1016/0167-2681(82)90008-7)
- Richardson, R. (2010). *CSI Computer Crime and Security Survey*. Retrieved from www.GoCSI.com
- Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). *Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk?*
- Rosen, P. K., Steinberg, B., Kearney, M. K., O'Connor, M. L., & Rubin, N. A. (2014). *Cyber insurance: A last line of defence when technology fails*.
- Sanchez, A. (2017, January). Lloyd's predicts surge in cyber insurance uptake in 2017 | Insurance Business. *Insurance Business UK*. Retrieved from <http://www.insurancebusinessmag.com/uk/news/breaking-news/lloyds-predicts-surge-in-cyber-insurance-uptake-in-2017-42266.aspx>
- Sasse, M., & Flechais, I. (2005). Usable Security: Why Do We Need It? How Do We Get It? In *Security and Usability: Designing secure systems that people can use*. (pp. 13–30). Retrieved from <http://discovery.ucl.ac.uk/20345/>
- Schwartz, G., Shetty, N., & Walrand, J. (2010). Cyber-Insurance: Missing market driven by user heterogeneity. In *In Proc. of WEIS 2010* (pp. 1–17).
- Shim, W. (2012). An Analysis of Information Security Management Strategies in the Presence of Interdependent Security Risk *. *Asia Pacific Journal of Information Systems*, 22(1).
- Smith, V. L. (1991). Rational Choice: The Contrast between Economics and Psychology. *Journal of Political Economy*, 99(4), 877–897. <https://doi.org/10.2307/2069710>
- Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, 75, 49–62. <https://doi.org/10.1016/j.dss.2015.04.011>
- State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks*. (2017). Retrieved from http://europa.eu/rapid/press-release_IP-17-3193_en.htm
- Sukhai, N. B. (2004). Hacking And Cybercrime. In *InfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development* (pp. 128–132). Retrieved from http://delivery.acm.org/10.1145/1060000/1059553/p128-sukhai.pdf?ip=212.219.32.63&id=1059553&acc=ACTIVE_SERVICE&key=BF07A2EE685417C5.3459FC42C4D3CA19.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=984185912&CFTOKEN=67736162&__acm__=1505309667_c5227eb7c663cc9ba2866
- Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Focus.
- Thorndike, A. N., Riis, J., Sonnenberg, L. M., & Levy, D. E. (2014). Traffic-Light Labels and Choice Architecture: Promoting Healthy Food Choices. *American Journal of Preventive Medicine*, 46(2), 143–149. <https://doi.org/10.1016/J.AMEPRE.2013.10.002>
- Tondel, I. A., Meland, P. H., Omerovic, A., Gjaere, E. A., & Solhaug, B. (2015). *Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research*.
- Toregas, C., & Zahn, N. (2014). *Insurance for Cyber Attacks: The Issue of Setting Premiums in Context*.
- Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015). Nudging towards security. In

D6.1: Concept note with the design of the economic experiments

- Proceedings of the 2015 British HCI Conference on - British HCI '15* (pp. 193–201). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2783446.2783588>
- Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, 5(4), 297–323. <https://doi.org/10.1007/bf00122574>
- UK Cyber Risk Survey Report. (2016). Retrieved from [https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/UK Cyber Risk Survey Report 2016.pdf](https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/UK%20Cyber%20Risk%20Survey%20Report%202016.pdf)
- UK HM Government 2015 Information Security Breaches Survey. (2015). <https://doi.org/10.13140/RG.2.1.4332.6324>
- Varian, H. R. (2004). System Reliability and Free Riding. In L. Camp & S. Lewis (Eds.), *Economics of Information Security (Advances in Information Security)* (Vol. 12, pp. 1–15). Kluwer Academic Publishers-Human Sciences Press. Retrieved from <http://people.ischool.berkeley.edu/~hal/Papers/2004/reliability>
- Wakker, P. P. (2010). *Prospect theory: For risk and ambiguity. Prospect Theory: For Risk and Ambiguity*. London, UK: Cambridge University Press. <https://doi.org/10.1017/CBO9780511779329>
- Young, D., Lopez Jr., J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14, 43–57. <https://doi.org/10.1016/J.IJCIP.2016.04.001>
- Zhou-Richter, T., Browne, M. J., & Gründl, H. (2009). Don't They Care? Or, Are They Just Unaware? Risk Perception and the Demand for Long-Term Care Insurance. *Journal of Risk and Insurance*, 77(4), 715–747.

D6.1: Concept note with the design of the economic experiments

5 Acronyms and Abbreviations

ISP	Information Security Protocol
DDoS	Denial of Service
SME	Small and Medium sized Enterprises
TPB	Theory of Planned Behaviour
PM	Protection Motivation Theory
GDT	General Deterrence Theory
SCT	Social Cognitive Theory
TAM	Technology Acceptance Model
WTP	Willingness to Pay

D6.1: Concept note with the design of the economic experiments

6 Appendix A

For the sake of simplicity, let us present the key concepts of the behavioural approach for a simple insurance decision. Purchasing a cyberinsurance product results in, what can be described as, a series of potential coverages $x_1 > x_2 > \dots > x_n$, where coverage x_i is obtained with the probability p_i of the insured cyberattack taking place. The key concept for the analysis of cyberinsurance purchasing behaviour is that of the 'risk attitude' of the decision-maker. Under a conventional economics approach (expected utility paradigm) risk attitude is characterised by decision-maker's utility function, which determines the psychological 'value' of each of the potential coverages of the insurance. Assuming that each decision-maker knows these probabilities, (s)he will buy the insurance only if the utility of the prime is lower than the expected utility of the outcomes of the fund. Formally, if I denotes the price of the insurance product and $U(x)$ the utility of an outcome x , the customer will buy the cyberinsurance product if and only if $U(I) < \sum_{i=1}^n p_i U(x_i)$. It is well known that, in this paradigm, a decision maker is risk-averse (respectively risk-seeking) if her or his utility function is concave (respectively convex).

Notice that, in expected utility models, the value of an outcome does not coincide with the outcome (in general $U(x) \neq x$), meanwhile the psychological value of each probability p_i is always this very same probability p_i , which is used in the valuation of the investment decision with no additional transformation. Behavioural economics proposes alternative models with a more realistic approach to the role played by probabilities in decision-making. Specifically, Prospect Theory considers the rank-dependent utility model or the equivalent cumulative prospect theory in the domain of gains (Quiggin, 1982; Tversky & Kahneman, 1992; Wakker, 2010). This model assumes that the psychological value of a probability to evaluate a fund - or *decision weight* as it is usually named - is a function of the probabilities of all potential outcomes of the investment. In this conceptual framework, a *rank* - or more intuitively a *good-news probability* - for any potential outcome x of the investment is defined as the probability of the fund yielding an outcome strictly larger than x . Formally $rank(x) = \sum_{x_i > x} prob(x_i)$. Ranks are numbers between 0 and 1, where 0 (respectively 1) is the rank associated to the best (respectively the worst) possible outcome of the fund. Let us define $x_{n+1} = -\infty$. Then, the probability of outcome x_i can be written as $p_i = rank(x_{i+1}) - rank(x_i)$ for $i = 1, \dots, n$. Before decision-making, ranks are transformed according to a non-decreasing application $w: [0,1] \rightarrow [0,1]$ named *weighting function*. Given a weighting function w , the *decision weight* of outcome x_i is defined as $\pi_i = w(rank(x_{i+1})) - w(rank(x_i))$. Notice that if the weighting function is the identity, i.e. $w(p) = p$, then the decision weights coincide with the probabilities of the outcomes ($\pi_i = p_i$). Decision weights are positive numbers lower than one, but they are not required to add up to one. Decision weights are related to the slope of the weighting function: the steeper the weighting function is, the larger the difference between $w(rank(x_{i+1}))$ and $w(rank(x_i))$ and then the larger corresponding decision weight π_i . Under rank-dependent utility, a potential customer with utility function $U(x)$ and weighting function $w(p)$ will buy a cyberinsurance product if and only if $U(I) < \sum_{i=1}^n \pi_i U(x_i)$.

D6.1: Concept note with the design of the economic experiments

Example (adapted from Wakker, 2010). Let us consider four potential insurance coverages of four potential cyberattacks $x_1 > x_2 > x_3 > x_4$ with identical probabilities $p_1 = p_2 = p_3 = p_4 = 0.25$. Let us assume that the weighting function for a potential customer is given by $w(p) = p^{0.5}$. Then, the decision weights for each outcome will be given by $\pi_1 = w(\text{rank}(x_2)) - w(\text{rank}(x_1)) = 0.25^{0.5} - 0^{0.5} = 0.50$, $\pi_2 = 0.21$, $\pi_3 = 0.16$ and $\pi_4 = 0.13$. Notice that, although the probabilities of all four outcomes are identical, the investor makes the decision of purchasing (or not) the cyberinsurance product considering that the decision weight (subjective probability) of the best outcome x_1 is $\pi_1 = 0.50 > 0.25 = p_1$ and the decision weight for the worst outcome x_4 is $\pi_4 = 0.13 < 0.25 = p_4$. *Even if the potential customer knows the actual probabilities of succeeding in the investment fund*, she or he behaves as if the probability of succeeding was higher than it actually is and if the probability of not succeeding was lower than it actually is.

Recall that ranks are good-news probabilities, i.e., a small rank means that the probability of getting a better outcome is small and the corresponding outcome is quite good. In other words, the lower the rank, the better the outcome. Figure A adapted from Wakker (2010), illustrates how two kinds of deviations from additive probabilities combine to create the probability weighting functions commonly found. Figure A(left) depicts traditional expected utility with probabilities weighted linearly; i.e. $w(p) = p$. However, empirical investigations, starting with Preston & Baratta, 1948, mostly find inverse S-shapes as in Figure A(right). The function in Figure 1a first is steep exceeding the diagonal, which suggests risk seeking. From probability 0 to 1/3, the function is over the diagonal of the square and from 1/3 to 1 is under the diagonal. The function is steeper close to 0 and close to 1. As highlighted by Wakker (2010) ‘the best-ranked outcomes receive relatively high decision weights and the worst-ranked outcomes even more. The moderate intermediate outcomes receive low decision weights. Apparently, people pay much attention to extreme and exceptional outcomes. This weighting function suggests that people are mostly risk averse, but not always, which deviates from the often-suggested universal risk aversion’.

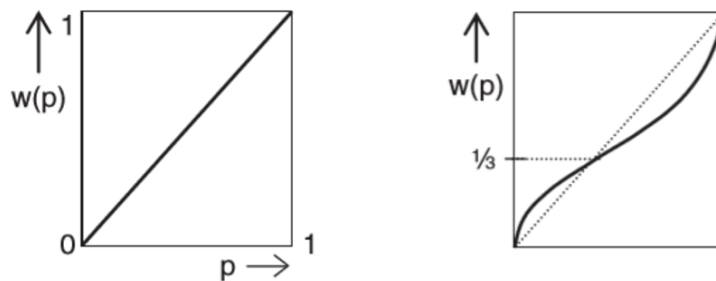


Figure A. Common weighting functions (adapted from Wakker, 2010).

CYBECO experiments will ask the participants to make decisions between investing in different protection measures and/or purchasing different insurance products. i that the expression used to quantify the subjective ‘value’ of any option of the participants (with/without

D6.1: Concept note with the design of the economic experiments

protection/insurance) is $\sum_{i=1}^n \pi_i U(x_i)$, where π_i are the decision weights that come from a transformation of the probabilities of suffering a cyberattack and $U(x_i)$ is the value function⁴. Notice that, in both the rational and behavioural models, the purchase of insurance affects to the value of the outcomes of suffering/not suffering a cyberattack and the decision of purchasing insurance is conditioned by the shape of the function $U(x_i)$. However, the framework for the analysis of the decision of purchasing protection measures is completely different in both models: in the rational (expected utility) model the purchase of protection modifies the value of the probabilities of attack p_i , that are included with no transformation in the expected utility expression $\sum_{i=1}^n p_i U(x_i)$. However, in the behavioural model, the value of the probabilities generated by the purchased protection measures need to be transformed through the weighting function into the decision weights.

⁴ In contrast to the von Neumann-Morgenstern utility function, which is computed over the monetary value of the outcome, the Prospect Theory value function is computed over the gains of losses generated by the output with respect to an initial reference point.