Risk Sciences 1 (2024) 100001

Contents lists available at ScienceDirect

Risk Sciences

journal homepage: www.keaipublishing.com/en/journals/risk-sciences/

Optimism bias and its impact on cyber risk management decisions

Martin Eling[a], Kwangmin Jung[b,*]

[a] Institute of Insurance Economics, University of St. Gallen, Switzerland
[b] Department of Industrial and Management Engineering, POSTECH, South Korea

ARTICLE INFO

Keywords:
Cyber risk
Optimism bias
Utility loss aversion
Risk management

ABSTRACT

This study explores how optimism bias influences decision-making in cyber risk management by developing a novel model that reflects utility loss aversion, a factor previously unexplored in this context. We find that decision-makers with self-protection as reference point are less likely to invest in other cyber risk management measures, providing support for optimism bias observed in the cyber-insurance market. We also show that decision-makers with higher loss aversion tend to not invest in other cyber risk management measures. Our results help to explain the lack of demand for cyber-insurance and have important implications for corporate risk management and public policy on cyber risk. They also help better understand cyber risk events which can trigger huge systemic consequences for economies and societies.

1. Introduction

Individuals, organizations and societies are heavily connected to each other, generating risks from interconnectedness. One of the most prominent risk types nowadays is cyber risk, which can make a large number of systems exposed to interconnected risk across regions and industries (Armenia et al., 2019). For instance, the "WannaCry" ransomware attack in 2017 affected more than 200,000 computers running the Microsoft Windows operating system in 150 countries within one day; the estimated total monetary loss reached almost $8 billion (Barlyn, 2017).[1] Such extreme events are less likely to occur than smaller events of daily life (Eling & Wirfs, 2019), but can trigger huge, systemic consequences to markets and societies. Systemic consequences can include, e.g., disruption in the energy, healthcare or financial industry (Welburn & Strong, 2021) and may result in a loss of support for the real economy, temporarily paralyzing operational processes and thus leading to significant business-interruption costs (European Systemic Risk Board, 2020).

Systemic cyber events with significant consequences might lead to an increase in the awareness of cyber risk among policy-makers, regulators and corporate/individual decision-makers.[2] This increasing awareness can motivate corporations to make substantial investments in risk management, including the option to buy insurance to transfer this risk. However, several surveys reveal a

* Corresponding author.
E-mail addresses: martin.eling@unisg.ch (M. Eling), kwjung@postech.ac.kr (K. Jung).

[1] Other examples are the data breaches resulting from the hacking of Yahoo in 2013 (three billion accounts) and FriendFinder in 2016 (412 million users); see Armerding (2018) for the biggest privacy data breach events in history.

[2] Practical evidence can be found in PricewaterhouseCoopers (2017) conducting a survey with 9500 decision-makers across 122 countries and documenting the increasing awareness of potential consequences by cyber events. The estimated global loss of cybercrime is in an area of $1 trillion (see, e.g., CSIS, 2020).

https://doi.org/10.1016/j.risk.2024.100001
Received 29 December 2023; Received in revised form 29 April 2024; Accepted 19 May 2024
Available online xxxx
2950-6298/© 2024 The Authors. Publishing services by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

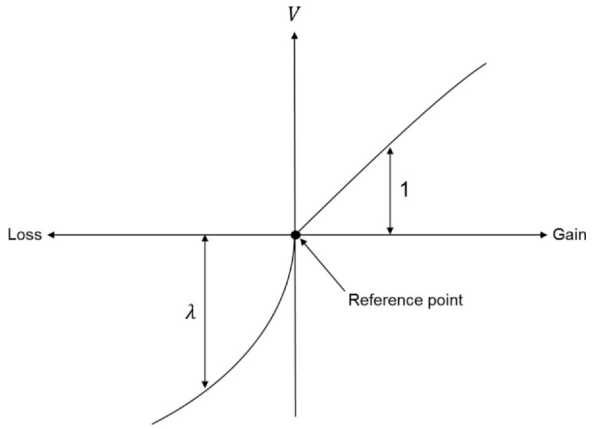

Fig. 1. The shape of the value function. The curvature of the gain state is concave, whereas that of the loss state is convex. λ is the parameter of the loss aversion, showing how convex the curvature is.

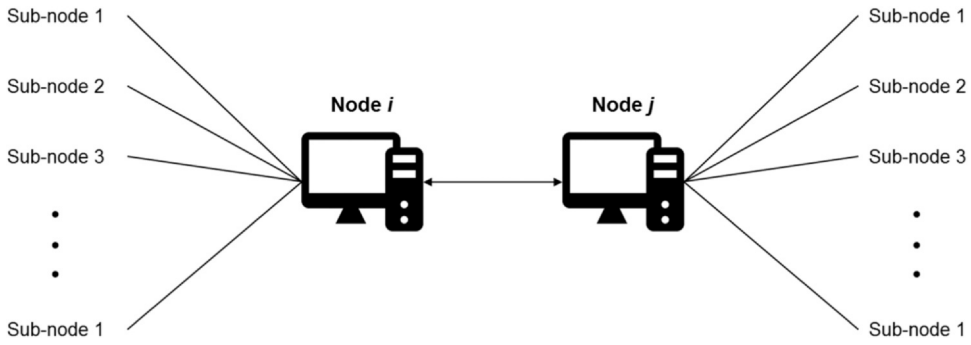

Fig. 2. Interconnected network environment between agent *i* and agent *j*. As information technology is more advanced, agents in the interconnected network environment can be more exposed to interdependent risk.

perception that decision-makers regard cyber risk events as rather unrealistic to themselves, until they finally experience a loss.[3]

Some decision-makers also exhibit optimism bias towards systemic cyber risks. Even as cyber risks become more likely, they believe that no single party can be completely secure, regardless of the cyber risk management strategy implemented and assume that they themselves will not face such risks.[4] This behavior is observable among potential participants in the cyber-insurance market who typically rely on self-protection measures, such as upgrading security software to guard against hacking, and deem insurance unnecessary. The extant literature on decision-making in the face of cyber risks has documented several findings related to self-protection and the purchase of cyber insurance.[5] However, these studies often assume that decision-makers are risk-averse, which may not accurately describe the optimism bias observed among market participants. Moreover, no study has yet investigated such a behavioral bias as optimism in the context of cyber risk.

[3] For instance, de Smidt and Botzen (2018) conducted a survey with 172 professional decision-makers in the Netherlands and call this type of perception "not-in-my-organization effect" (p. 247). Jalali et al. (2019) also argue that many organizations constantly ignore or underestimate cyber risk. This sort of perception can be called "optimism bias", as defined by Weinstein (1980), which is considered as one of the most consistent and robust biases in psychology and behavioral economics (De Bondt & Thaler, 1990; Sharot, 2011; Claus & Nguyen, 2023). These authors find evidence of unrealistic optimism—namely agents believe that it is less likely for them to experience negative events than for others. This bias has also been studied in the insurance context, where, for example, people are more likely to insure against modest risk with high probability than against extreme risk with low probability (see, e.g., Schanz, 2019, for an overview of behavioral biases in the insurance research). Zhang and Borden (2020) also find that individuals with negative emotion from cyber security threats are less likely to take risk management actions and thus are more exposed to cyber risk.

[4] Two recent surveys by the U.K. Government (DCMS, 2018) and EIOPA (2018) support this observation in the cyber risk context by showing that the most common reason not to take up cyber-insurance is that the decision-makers do not see themselves at high risk.

[5] With respect to decision-making in general see Ehrlich & Becker, 1972; Hofmann, 2007; Mürmann and Kunreuther, 2008; Alary et al., 2013; Hofmann & Rothschild, 2019. With respect to decision-making against cyber risk, the level of investment in the security system and the demand of insurance are modeled (see, e.g., Gordon & Loeb, 2002; Lelarge & Bolot, 2009; Shetty et al., 2010; Öğüt et al., 2011; Hofmann & Ramaj, 2011; Wang, 2019). Several studies analyze the impact of interdependency between network systems on loss probability (see, e.g., Lelarge & Bolot, 2009; Shetty et al., 2010; Öğüt et al., 2011; Hofmann & Ramaj, 2011). Some studies incorporate the lack of proving the loss occurrence by an insurer, which can be linked with the presence of information asymmetry (see, e.g., Lelarge & Bolot, 2009; Öğüt et al., 2011), which is not the focus of this paper.

Table 1
Model Parameters.

Notation	Explanation
$v(\cdot)$	Value function
W	Initial wealth
L	Loss amount
$p_i(s_i)$	The loss probability of agent i as a function of the self-protection level ($s_i \in [0, W]$)
$p_j(s_j)$	The loss probability of agent j as a function of the self-protection level ($s_j \in [0, W]$)
$\hat{p}_i$	The actual loss probability of agent i in the presence of interdependent risk
$\theta(s_i, s_j)$	The function of the degree of contagion
d	Deductible ($0 \leq d$)
δ	Proportional loading factor ($\delta \in [0,1]$)
β	Insurance coverage ($\beta \in [0,1]$)
I	Indemnity with deductible
π	Insurance premium
g_i	The level of self-insurance ($g_i \in [0,1]$)
$K(g_i)$	A cost function of self-insurance

To address this bias against cyber risks, we study decision-making on cyber risk management in the context of cumulative prospect theory (descriptive decision theory; Tversky & Kahneman, 1992). We assume that agents are risk seeking when dealing with losses and risk averse when dealing with gains by comparing possible outcomes with a reference point.[6] The reference points considered in this paper rely on two possible instruments: self-protection and self-insurance. Self-protection is a realistic reference point for those exposed to cyber risk, for instance, in the network environment given that most companies invest in IT security.[7] Self-protection also plays a role of a public good (Lohse et al., 2012), which can affect the loss probability of others in the interconnected environment. In contrast, self-insurance does not affect the risk of others, but rather reduces the loss amount that one can face with as a private good (Ehrlich & Becker, 1972).

We develop a conceptual model upon a partial form of cumulative prospect theory (CPT) to compare potential decisions on additional cyber risk management measures (market insurance for cyber risk transfer and self-insurance) with the reference point of self-protection against cyber risk.[8] Although our decision-making is discrete in two loss-economic states, it is a part of the truly mixed case (Wakker & Tversky, 1993) with the assessment in both gain and loss domains, not in a domain-specific scale.[9] Based on the reference points and the model framework, we find that one with the reference point of self-protection is likely to not invest in additional cyber risk management measures (market insurance and self-insurance).[10]

[6] Agents in our model can be both individuals or firms, given that cyber-insurance coverages exist at individual and firm levels. While it is widely accepted that the decision making of individuals shows some loss aversion (see, e.g., Schmidt, 2016; Gottlieb & Mitchell, 2020), recent empirical results illustrate the effect of loss aversion on decision making of firms or a group of managers, particularly in the corporate finance context, where a firm decision-making on financial investments is based on loss aversion in comparison with a reference point. For example, Baker et al. (2012) investigate the effect of loss aversion on mergers and acquisitions by setting the past 52-week peak of a stock price as the reference point and find evidence that target shareholders are more likely to accept a deal when a take-over offer is slightly higher than the reference point. Baker and Xuan (2016) find that a firm sets the equity price, at which a new CEO joined, as a reference point to decide on raising new equity. A firm decision-making upon loss aversion can also be observed in the strategic management context, where Holmes et al. (2011) review management studies using prospect theory and find 41 articles published in leading management journals looking into firm risk-taking behaviors under prospect theory. These articles commonly assume that firm-level behaviors are indications of risk-taking preferences that prospect theory predicts for individuals (Holmes et al., 2011). In the cyber risk-related context, Mersinas et al. (2016) show that IT risk managers switch their risk preferences from risk aversion to risk seeking when they experience an information system loss.

[7] Jansen et al. (2016) find from the survey results of 1622 Dutch entrepreneurs that almost all respondents have taken one or more protective measures against cybercrime. The authors also observe that a quarter of respondents have still experienced cybercrime events, which implies that more effective and additional measures should be implemented. This finding supports our reference point in the model and the motivation to study decision-making on additional cyber risk management measures.

[8] Appendix B categorizes the models for decision-making under risk into whether they consider risk control measures and utility loss aversion under the presence of interdependent risk and illustrates the positioning of our study. As shown, no study has looked at utility loss aversion under interdependent risk.

[9] Wakker and Tversky (1993) axiomatize cumulative prospect theory as well as expected utility theory with a method leading to situations allowing consistent inferences about the ordering of value differences. In particular, Theorem 6.3 of their paper describes a unique value function satisfying gain-loss consistency and sign-comonotonic tradeoff consistency, the function that is referred to as the general case allowing mixed prospects staying in both gain and loss domains (Harrison & Swarthout, 2020). Note that a domain-specific scale here refers to a situation that prospects are assessed in one specific domain, i.e., either gain or loss, allowing positive affine transformations (Harrison & Swarthout, 2020).

[10] Eckles and Volkman-Wise (2019) attempt to explain, using prospect theory-type preferences, several phenomena that cannot be explained by the expected utility theory. In particular, the phenomena studied in the paper are the preference for low deductibles, the lack of demand for catastrophe insurance and the over-demand to insure small losses. Furthermore, they find that individuals under loss aversion ($\lambda > 1$, where λ is the loss aversion parameter) tend to demand less insurance than individuals under the expected utility theory. Our finding is exactly in line with their finding that individuals with prospect theory-type preferences (loss aversion) are willing to take on more risk to avoid premium payments as certain losses.

Table 2
Model Components.

Reference point 1: Status quo with self-protection (public good)		
	Case 1: Comparison with cyber-insurance (+ self-protection)	
State	No-loss	Loss
Probability	$1-\hat{p}_i$	$\hat{p}_i$
Reference point	$W-s_i$	$W-s_i-L$
Final wealth	$W-s_i-\pi$	$W-s_i-\pi-L+I$
Gain/Loss	$-\pi$	$I-\pi$
	Case 2: Comparison with self-insurance (+ self-protection)	
State	No-loss	Loss
Probability	$1-\hat{p}_i$	$\hat{p}_i$
Reference point	$W-s_i$	$W-s_i-L$
Final wealth	$W-K(g_i)-s_i$	$W-K(g_i)-(1-g_i)\bullet L-s_i$
Gain/Loss	$-K(g_i)$	$g_i\bullet L-K(g_i)$
Reference point 2: Status quo with self-protection and self-insurance (public good + private good)		
	Case 3: Comparison with cyber-insurance (+ self-protection)	
State	No-loss	Loss
Probability	$1-\hat{p}_i$	$\hat{p}_i$
Reference point	$W-s_i-K(g_i)$	$W-s_i-K(g_i)-(1-g_i)\bullet L$
Final wealth	$W-s_i-\pi$	$W-s_i-\pi-L+I$
Gain/Loss	$K(g_i)-\pi$	$I-\pi+K(g_i)-L\bullet g_i$

This behavior (optimism bias with respect to cyber risk losses) that agents stay uninsured becomes rational in our decision model.[11] Our findings are important for better understanding a peculiar market behavior for decision-making on risk management currently observed in the cyber-insurance market. This paper does not provide empirical evidence on behavioral decision-making with risk control measures, but explores how agents facing cyber risks make a decision on the intersection of risk control measures (self-protection and self-insurance) and cyber-insurance under a descriptive decision model.

Although our study does not provide an empirical approach to validating CPT or a test of the full set of CPT as Harrison and Swarthout (2020) argue that many CPT-based studies fail to do, our study is useful as the first to examine the role of risk control measures against cyber risks using utility loss aversion, thereby providing a benchmark design to following studies. Our findings are also important for risk managers and IT professionals in firms and insurance companies that are developing cyber-insurance policies.[12] For firms, the results are important not only for decisions on internal risk management, but also for new requirements of reporting cyber incidents because the requirement emphasizes the importance of risk control measures (Eling & Wirfs, 2019).[13] The remainder of this paper is organized as follows: Theoretical background on the model is provided in Section 2. We develop the model framework by describing cyber risk, cyber-insurance and reference points in Section 3. This framework is used to show how agents make decisions on cyber-insurance and risk control measures with different reference points in Section 4. Finally, Section 5 presents the conclusion.

2. Theoretical background: prospect theory

The expected utility theory is based on the assumption that an individual makes a decision under risk by maximizing her expected utility over some final states of wealth (von Neumann & Morgenstern, 1953); the two economic states typically considered in the insurance domain are determined by a loss occurrence. A pre-defined (concave) utility function depending on the risk preferences is used to determine the utility level; however, the theory assumes dependence on the final wealth for the utility level, which largely simplifies the analysis on individual choice over risky prospects (Tversky & Kahneman, 1991).

[11] To argue that the behavior described in our decision model is rational, one might question whether utility loss aversion is rational. Tversky and Kahneman (1991) clarify it by concluding that the reference-dependent decision under loss aversion can be justified as a rational behavior when the consequences by the corresponding effect of the reference point on the decision are indeed experienced. This idea has also been employed in other contexts, such as decision-making about pension/old-age provision by Binswanger (2007), where the study evaluates normative decisions using utility loss aversion assumption (specifically, the lexicographic loss aversion model).

[12] Our findings can help to better understand the nature of cyber insurance demand and to explore potential latent cyber coverages that may be viable in the current market.

[13] In the U.S., reporting requirements for data breaches have been introduced in many states since 2002 (NCSL, 2019). In the European Union such reporting requirements will apply from 2018 (European Union, 2016). After their enforcement, more data and information will be available. This has already happened with data samples in the U.S. as the Privacy Rights Clearinghouse "Chronology of Data Breaches" (PRC, 2019).

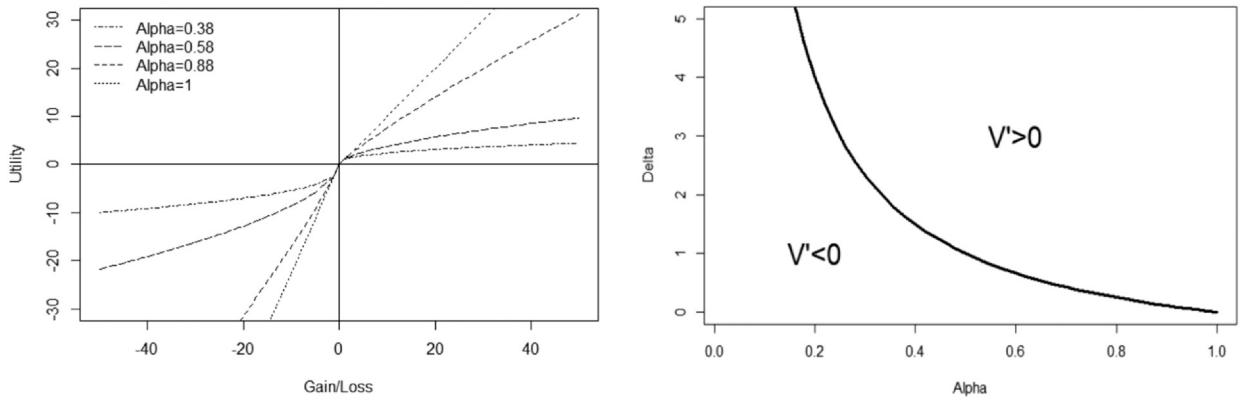

Fig. 3. The description on varying diminishing sensitivity and the marginal productivity of self-protection measure when considering cyber-insurance. The left panel displays the KT value function with different sizes of the parameter for diminishing sensitivity, and the right panel shows the sign of the marginal value with respect to the effort on security to describe the incentive for self-protection.

Prospect theory developed by Kahneman and Tversky (1979) is based on the assumption that an individual dislikes a loss more than she likes a gain of comparable size; hence, the level of utility in an economic situation is determined by the gain-loss domain. An individual makes a decision on the purchase of insurance based not on the final wealth, but on gains and losses compared to a reference point. This implies that gains and losses count the opportunity cost by comparing a potential decision with the reference point. Tversky and Kahneman (1992) complement their initial model (Kahneman & Tversky, 1979) by taking into account the cumulative functional form separately to gains and losses, thereby resolving two possible problems of the first model: lack of the explanation on stochastic dominance and lack of ability to accommodate a large number of outcomes.

We consider an individual facing two possible outcomes in an economic situation, x_1 and x_2. The individual has the loss probability, p, and makes decisions using a value function (hereafter, KT value function) and a probability weighting function (hereafter, KT weighting function). The probability weighting function is a non-linear form reflecting overweight on less likely events and underweight on more likely events. The function features rank-dependent weighting, and the violation that the sum of the subjective probability by the function is not 1. The mathematical expressions of the value function and non-linear weighting functions are (Tversky & Kahneman, 1992):

$$v(x) = \begin{cases} x^{\alpha} & if\ x \geq 0 \\ -\lambda(-x)^{\alpha} & if\ x < 0 \end{cases}, \tag{1}$$

$$\theta^{+}(p) = \frac{p^{\gamma}}{(p^{\gamma} + (1-p)^{\gamma})^{1/\gamma}}, \tag{2}$$

$$\theta^{-}(p) = \frac{p^{\xi}}{(p^{\xi} + (1-p)^{\xi})^{1/\xi}}, \tag{3}$$

where $\alpha \in [0,1]$ is a parameter to determine the diminishing sensitivity for concavity in the gain domain and for convexity in the loss domain, λ is a loss aversion parameter, and γ and ξ are probability weighting parameters differentiated depending on the gain or loss state. Tversky and Kahneman (1992) propose the values of α (= 0.88) and λ (= 2.25) with the median parameters found from their experimental study.[14] In this value function (see Fig. 1), a loss is defined by a negative value of x, whereas a gain is defined by a positive value. The diminishing sensitivity, α, indicates that an individual is risk averse in the gain state ($x \geq 0$) and risk seeking (i.e., loss averse) in the loss state ($x < 0$)—that is, $v_{-}'' > 0$, $v_{+}'' < 0$, where v_{-}'' is the second order condition in the loss domain and v_{+}'' is the second order condition in the gain domain. The reference point at the origin in Fig. 1 is not differentiable (inflection point), and the higher curvature appears in the loss state than in the gain state.

The expected value of the "prospect" (an economic situation) is determined by the combination of the value function and the weighted probability as follows:

[14] Although many studies using cumulative prospect theory follow Kahneman and Tversky (1992) parameters, they are simply the median values from the experiment and it is not an absolute rule in a general case. Erev et al. (2008) state that the parameters can vary by which reference point is used. Harrison and Swarthout (2020) point out that there also can be a case that decision weights have a gap between gains and losses, which is called probabilistic loss aversion defined by Schmidt and Zank (2008). Standing on the other side, utility loss aversion refers to a situation that an agent behaves in the same way in both gain and loss domains with regard to evaluating probabilities (Harrison & Swarthout, 2020). Estimation of utility loss aversion (i.e. estimation of λ) is not possible without allowing mixed frame choices (Bruhin et al., 2010). Our descriptive decision model is based on utility loss aversion in combination with an interdependent risk setting, which does not impose probability distortions in gain and loss domains, but plays a role of identical weighting with risk contagion.

Table 3
Criteria for Cyber-insurance in Case 1.

		α				
$\delta = 0.1$		0.1	0.3	0.5	0.7	0.88
λ	1.25	T ($\hat{p}_i \geq 0.57$)	T ($\hat{p}_i \geq 0.61$)	T ($\hat{p}_i \geq 0.69$)	F	F
	1.75	T ($\hat{p}_i \geq 0.66$)	T ($\hat{p}_i \geq 0.73$)	F	F	F
	2.25	T ($p_i \geq 0.72$)	T ($\hat{p}_i \geq 0.81$)	F	F	F
	2.75	T ($\hat{p}_i \geq 0.77$)	F	F	F	F
	3.00	T ($\hat{p}_i \geq 0.78$)	F	F	F	F
$\delta = 0.2$		0.1	0.3	0.5	0.7	0.88
λ	1.25	T ($\hat{p}_i \geq 0.58$)	T ($\hat{p}_i \geq 0.64$)	F	F	F
	1.75	T ($\hat{p}_i \geq 0.67$)	F	F	F	F
	2.25	T ($\hat{p}_i \geq 0.73$)	F	F	F	F
	2.75	T ($\hat{p}_i \geq 0.78$)	F	F	F	F
	3.00	F	F	F	F	F
$\delta = 0.3$		0.1	0.3	0.5	0.7	0.88
λ	1.25	T ($\hat{p}_i \geq 0.58$)	F	F	F	F
	1.75	T ($\hat{p}_i \geq 0.68$)	F	F	F	F
	2.25	F	F	F	F	F
	2.75	F	F	F	F	F
	3.00	F	F	F	F	F

Note: The table shows the results in three cases (δ = 10 %, 20 % and 30 %) of loading factor as an example. As the loading factor is bigger, criteria for cyber-insurance shrink further. T indicates that inequality (13) holds with the level of the loss probability in parentheses, whereas F indicates the nonsatisfaction of inequality (13). The loss probability with the validity of inequality (13) should be lower than 91 % ($=1/(1+\delta)$).

$$V = \theta^{+}(p)\bullet v(x_1) + \theta^{-}(1-p)\bullet v(x_2), \tag{4}$$

where x_1 and x_2 indicate outcomes of two states (gain and loss) and p and $1-p$ are the corresponding probabilities. The expected value of the "prospect" can be defined as subjective expected value for the decision-making, which is conceptually equivalent to the expected utility theory. The probability applied to the states is the subjective probability measure analytically calculated using the probability weighting function. According to the theory, very small probabilities are either overweighted or rounded to 0 (Kunreuther & Michel-Kerjan, 2014; Schmidt, 2016).

3. Model framework

3.1. Modeling interdependency with self-protection

Economic agents[15] nowadays operate their business in an interconnected network environment, represented in Fig. 2 with nodes as atomic elements controlled by agents (Böhme & Schwartz, 2010). If one agent were breached in an attack, there would be a high likelihood that the remaining agents in the environment would be breached as well.[16] This indirect risk to the other agents, also called interdependent risk, results in externality[17] and is of importance in the network environment, because a systemic risk by a global hacking attack or virus can take place.

For simplicity, suppose that there are two agents (i and j) in the interconnected network environment.[18] Each agent makes a

[15] Following Böhme and Schwartz (2010) in the cyber risk context, we hereafter use "agent" to describe possible economic entities facing cyber risks. Potential agents facing cyber risk include individuals, firms and governmental and non-governmental institutions.

[16] Hofmann (2007) and Mürmann and Kunreuther (2008) also parameterize both direct and indirect risks into the model to reflect the possibility of contagion risk from other sources. However, neither study considers the degree of interdependency, counting only the presence of interdependency.

[17] Zhao et al. (2013) illustrate positive externality occurring when interconnected agents have all high security risks and negative externality occurring when one agent faces high risk and the other has low risk. The authors use a concept of mutual insurance (referred as risk pooling arrangements: RPAs) to compare with cyber-insurance in evaluating a firm's investment efficiency and find that RPAs as a complement to cyber-insurance help firms induce more efficient investments in security enhancement. Their framework is in line with ours in that they see self-protection (security investments) as necessary in the presence of interdependent risk, however, our structure is differentiated by taking risk control measures as alternatives or complements to cyber-insurance.

[18] We follow Mürmann and Kunreuther (2008) in assuming that two agents are interconnected in the risk environment. In practice, many agents can be interconnected in the cyber space, where the probabilities of risk contagion from different agents may vary depending on their security levels. Our framework simplifies this by representing the average level of risk contagion with homogeneous size of efforts on risk management (i.e., cyber security).

Table 4
Critical Value of the Contagion Level (Case 1).

		α									
		$p_i = 0\%$					$p_i = 50\%$				
$\delta = 0.1$		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.568	0.606	0.688	F	F	0.136	0.212	0.376	F	F
	1.75	0.658	0.725	F	F	F	0.317	0.451	F	F	F
	2.25	0.720	0.807	F	F	F	0.440	0.614	F	F	F
	2.75	0.765	F	F	F	F	0.529	F	F	F	F
	3.00	0.783	F	F	F	F	0.565	F	F	F	F
$\delta = 0.2$		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.575	0.643	F	F	F	0.150	0.286	F	F	F
	1.75	0.668	F	F	F	F	0.336	F	F	F	F
	2.25	0.733	F	F	F	F	0.466	F	F	F	F
	2.75	0.784	F	F	F	F	0.567	F	F	F	F
	3.00	F	F	F	F	F	F	F	F	F	F
$\delta = 0.3$		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.584	F	F	F	F	0.167	F	F	F	F
	1.75	0.683	F	F	F	F	0.365	F	F	F	F
	2.25	F	F	F	F	F	F	F	F	F	F
	2.75	F	F	F	F	F	F	F	F	F	F
	3.00	F	F	F	F	F	F	F	F	F	F

Note: The table shows the results in three cases (10 %, 20 % and 30 %) of loading factor as an example. As the loading factor is bigger, the critical value of the contagion level is bigger. F stands for the nonsatisfaction of inequality (13).

monetary effort on enhancing the cyber security system denoted by s_i and s_j. These efforts represent all possible management activities by the agents to improve their cyber security levels, such as the financial investment in installing additional cyber security software and regularly updating it against cyber risk. In the insurance context, this kind of effort is called self-protection, which can reduce the loss probability (Ehrlich & Becker, 1972). The loss probability of each agent is a function of the monetary effort of self-protection defined as $p(s) \in [0,1]$.[19]

Mürmann and Kunreuther (2008) provide a theoretical background on the optimal level of self-protection and insurance in the presence of interdependent risk.[20] To model interdependent risk, we follow Hofmann (2007) and Mürmann and Kunreuther (2008), but in our case all agents invest in their security for self-protection to reflect a general behavior against cyber risk. The loss probability for agent i in this setting can be defined as

$$\hat{p}_i = p_i(s_i) + (1 - p_i(s_i)) \times p_j(s_j) \times \theta(s_i, s_j) \in [0, 1], \tag{5}$$

where $\hat{p}_i$ is the actual loss probability of agent i, $p_i(s_i)$ is the agent i's own loss probability (convex), $p_j(s_j)$ is the agent j's own loss probability (convex) and $\theta(s_i, s_j) \in [0,1]$ is a function (likelihood) of the degree of contagion relying on the size of investments on the cyber security system.[21] We assume that the contagion function, $\theta(s_i, s_j)$, is convex with respect to the cyber security investments, meaning that the more investments are made, the lower the infectiousness is, but the rate of lowering decreases.

The actual loss probability of agent i ($= \hat{p}_i$) is affected by the externality from interconnected agent j ($= p_j(s_j)$). This implies that the size of self-protection by agent j influences the loss probability of agent i. Unlike Mürmann and Kunreuther (2008), we allow for an imperfect spread of cyber risk, where risk contagion does not always occur ($\theta(s_i, s_j) \leq 1$). The degree of contagion (i.e. likelihood of risk spillover to an interconnected agent) is affected by the cyber security level, thus we explicitly include a function of the degree of contagion, relying on the size of investments on the security system.[22] Assumption 1 describes that the actual loss probability

[19] The loss probability in the cyber risk context is also called *vulnerability*, which indicates the probability that a breach attack is successful (Gordon & Loeb, 2002; Wang, 2019). We stay with the term, loss probability, meaning that the loss occurs when a system is breached.

[20] Mürmann and Kunreuther (2008) call the interdependent risk contamination between agents and consider the case of no contamination in comparative statics. However, no contamination between agents is not the case for the cyber risk context, especially in the hyper-connected world with the Internet of Things. Therefore, we do not take into account the case of no contamination in our model.

[21] The probability of risk contagion in a network environment may be influenced by several factors, such as the type of digital communication channels through which a cyber risk can occur (e.g., spam emails or web pages). The literature on cyber security games has noted that cyberattacks typically exploit weak endpoints within the network (see, e.g., Grossklags et al., 2008). Additionally, security investments are often strategic complements to the control measures for managing cyber risk contagion, as seminal studies (such as Gordon & Loeb, 2002; Kunreuther & Heal, 2003) suggest. Therefore, we follow these studies in using security investments as the key factor to control cyber risk contagion.

[22] We take into account this imperfect spread for each case in Section 4 by deriving critical values of this spread level satisfying propositions.

Table 5
Criteria for Self-insurance in Case 2.

		α				
Net margin = 10 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	0.611	0.714	0.798	0.862	0.905
	1.75	0.688	0.777	0.847	0.898	0.930
	2.25	0.739	0.818	0.877	0.919	0.945
	2.75	0.776	0.846	0.897	0.932	0.954
	3.00	0.791	0.857	0.905	0.938	0.958
Net margin = 50 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	0.573	0.606	0.639	0.670	0.697
	1.75	0.652	0.683	0.712	0.740	0.763
	2.25	0.707	0.735	0.761	0.785	0.805
	2.75	0.747	0.772	0.795	0.817	0.835
	3.00	0.763	0.787	0.809	0.830	0.847
Net margin = 100 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	0.556	0.556	0.556	0.556	0.556
	1.75	0.636	0.636	0.636	0.636	0.636
	2.25	0.692	0.692	0.692	0.692	0.692
	2.75	0.733	0.733	0.733	0.733	0.733
	3.00	0.750	0.750	0.750	0.750	0.750

Note: The table shows the critical values of the loss probability to achieve inequality (17) with varying possible values of net margin as examples (the condition holds if the loss probability is higher than the critical value for each case). The bigger the net margin is, the lower the loss probability level is in inequality (17). However, the level of the loss probability to satisfy a positive value of the decision on self-insurance is considerably high for all three cases.

function is convex and assumes positive externality; however, the risk will not disappear even if the agent spends infinite amounts for self-protection, i.e., no security measure can fully eliminate cyber risk (Assumption 1-ii).

Assumption 1.

(i) Diminishing loss probability with interdependent risk over increasing self-protection level.[23]

$$\frac{\partial \hat{p}_i}{\partial s_i} < 0. \tag{6}$$

(ii) The loss probability with interdependent risk does not disappear despite the agent's substantial capacity to invest in self-protection:

$$\lim_{s_i \to \infty} \hat{p}_i(s_i) > 0. \tag{7}$$

3.2. Cyber-insurance design and self-insurance

Market insurance in our model reflects cyber-insurance currently traded in the market by including deductibles and cost loading on pricing.[24] We denote the deductible by d and additionally consider a loading factor ($= \delta$) proportional to the loss probability to

[23] Assumption (1-i) can be derived in the following way:
$\frac{\partial \hat{p}_i}{\partial s_i} = p_i'(s_i) - p_j(s_j) \cdot p_i'(s_i) \cdot \theta(s_i, s_j) - p_j(s_j) \cdot \theta'(s_i, s_j) - p_j(s_j) \cdot p_i(s_i) \cdot \theta'(s_i, s_j)$
$= p_i'(s_i) \cdot [1 - p_j(s_j) \cdot \theta(s_i, s_j)] + p_j(s_j) \cdot \theta'(s_i, s_j) \cdot (1 - p_i(s_i))$.
Given that agents' own loss probabilities and $\theta(s_i, s_j) \in [0,1]$ are convex, we conclude
$\frac{\partial \hat{p}_i}{\partial s_i} < 0$.

[24] Romanosky et al. (2019) analyzed 100 cyber-insurance policies and documented that cyber-insurance carriers are mainly concerned about the correlated risk (interdependent risk between network systems), leading to a systemic risk but not so much the possible information asymmetry. The cyber-insurance market, particularly in the U.S. where the market is currently most developed, typically provides policies with deductibles, premiums between $10,000 and $100,000, and cover limits between $10 million and $50 million (Romanosky et al., 2019). The deductibles are, generally speaking, as low as $5000 and reach amounts between $500,000 and $1 million for insureds, whose asset values are around $1 billion or more.

account for cost in underwriting risks. Here we assume that the insurer is aware of the actual loss probability with the degree of contagion and the loss probability of an interconnected party, implying that the presence of information asymmetry possibly leading to adverse selection and moral hazard is not taken into account in this study.[25] The indemnity I and the premium π with the deductible are defined as (Zweifel & Eisen, 2012, Chapter 3)

$$I = \max[L - d, 0] \bullet \beta = (L - d)^{+} \bullet \beta, \tag{8}$$

$$\pi = (1 + \delta) \times \hat{p}_i \times I, \tag{9}$$

where L is a loss and β is the coverage of a proportional insurance with the loading factor δ.

Self-insurance does not influence loss probability (Ehrlich & Becker, 1972), meaning that loss probability in the presence of interdependent risk is not affected by the implementation of self-insurance.[26] We embed self-insurance into our model by denoting the level of self-insurance for agent i with $g_i \in [0,1]$ and a cost function of self-insurance by $K(g_i)$. We assume that the cost function of self-insurance is concave with respect to g_i ($K'(g_i) > 0$, $K''(g_i) < 0$).

3.3. Reference points

A key approach to analyze decision-making under loss aversion is to set the reference point (Tversky & Kahneman, 1991). A decision-maker uses the reference point to compare it with a potential decision, thereby framing the gain and loss of the decision.[27] For example, for insurance decision-making, the reference point is compared with an insurance plan that could be bought. We consider two possible reference points under loss aversion: status quo with self-protection and status quo with both self-protection and self-insurance.[28] The reference point based on self-protection can be cyber risk-specific in the following reasons; 1) almost all business parties are connected via computerized operations and today's network systems require regular security updates; 2) public/business policy against cyber risk may require a minimum standard for self-protection either by law or by business practice, hence agents should fulfil certain minimum requirements (i.e. investments) in terms of, e.g., enhancing IT security to start a business.

3.3.1. Status quo with self-protection as a public good

As a reference point, we assume that all agents make investments in regular security enhancement to protect against possible cyber-attacks. This self-protection effort reduces loss probability. It could also be that the government requires all economic parties to enhance their cyber security systems to a certain level. This definition of the reference point is material in that the positive externality from concurrent efforts in the interconnected network environment matters to social welfare. Therefore, this positive externality plays a role in promoting the public good.[29] We compare two scenarios with this reference point: decisions on cyber-insurance with self-protection and decisions on self-insurance with self-protection. All scenarios assume that the self-protection measure is implemented in any decision circumstance to build a realistic setting.

3.3.2. Status quo with both self-protection and self-insurance

Here the agent makes an investment in enhancing its cyber security system to protect itself and conducts a self-insurance plan simultaneously with self-protection. The self-insurance plan can reduce the magnitude of a loss, particularly for a potential extreme case, but it does not serve as a public good because it reduces the size of a loss only for those who invest in self-insurance. It can thus be regarded as a private good (Grossklags et al., 2008), which provides a benefit only for the agent implementing the plan.

[25] When it comes to cyber risk, which is a complex and business risk, a thorough, proper risk assessment procedure is required for insurers to take over a risk from potential insureds (Society of Actuaries, 2017). A survey by Swiss Re (2016) with 802 insurance executives reveals that 70 % of insurers provide cyber risk mitigation measures, e.g., in-house risk management advice and security assessments in their coverages.

[26] Self-insurance in this paper can be described by a loss reduction activity as part of the risk control plan (Hofmann & Peter, 2016). Several forms of self-insurance have been implemented in practice. For example, Ehrlich and Becker (1972) regard sprinkler systems as a self-insurance measure to reduce the size of a loss from fires. In the context of cyber risk, Grossklags et al. (2008) exemplify self-insurance activity with having good backups or conducting regular backups. This self-insurance activity can be carried out by both individual agents and corporate agents as a method of reducing a potential loss amount.

[27] The reference point in most literature about insurance demand under prospect theory is state-dependent with no insurance (Schmidt, 2016; Eeckhoudt et al., 2018; Eckles & Volkman-Wise, 2019; Gottlieb & Mitchell, 2020) or the purchase of full insurance (Schmidt, 2016; Eeckhoudt et al., 2018). Some studies in broader contexts use stochastic (dynamic), state-dependent reference points (see, e.g., Köszegi & Rabin, 2006, 2007; De Giorgi & Post, 2011).

[28] Koop and Johnson (2012) carry out experiments to investigate whether an individual considers multiple reference points (i.e., minimum requirement, status-quo and goal) in a single risky decision-making. They conclude that individuals seem to see multiple reference points important when making decisions and minimum requirement and goal references can particularly impact a decision-making behavior within a single choice context.

[29] To the best of our knowledge, there has been no literature to investigate decision-making on self-protection using utility loss aversion. However, several studies identify the equilibrium under expected utility theory that the interdependent nature of risk leads one to underinvest in self-protection when there exists a positive externality from another's self-protection measure and a limiting insurance coverage can improve individual or social welfare (Hofmann, 2007; Mürmann & Kunreuther, 2008). As a relevant literature, Hofmann and Rothschild (2019) use a simple model of the insurance and self-protection decisions with heterogeneous parameters of self-protection costs and risk spillovers to derive the finding that competitive markets and markets served by perfectly price discriminating monopolists will offer overinsurance when risk spillovers exist.

Simultaneous implementations on risk control measures might impose a significant cost to the agent, but reduce the loss probability and size. This definition of the reference point is material in that it can show interaction between cyber-insurance and both risk control measures.

In addition, a safe option with the maximum effort as the reference point is plausible for a prospective insured, which could offer a boundary value to the insured in decision-making. Schmidt (2016) defines the safe option as the purchase of insurance with full coverage; however, full insurance is not a realistic option in the current cyber-insurance market; thus, we set the safe option as the possible maximum effort on risk controls by agents.[30] We compare one possible scenario with this reference point: decisions on cyber-insurance only with self-protection. In this case, we follow Ehrlich and Becker (1972) in that market insurance is a substitute for self-insurance[31] and assume that the agent continues to maintain self-protection efforts as the basic risk management tool. Table 1 summarizes the parameters of the model. We focus on a model with two states of the world, either a loss state or a no-loss state, whose components are illustrated in Table 2.[32]

In summary, the following points reflect the features embedded in our framework, which affect the decision-making on risk management and the current cyber-insurance market:

1. *The presence of interdependent risk in the interconnected environment.*
2. *Realistic design for cyber-insurance in the current market: no available full coverage (deductible and partial coverage).*
3. *Self-protection (essential risk control measure in the interconnected environment and cyber-insurance market) as the reference point.*

4. Decision-making under loss aversion

In the expected utility theory, the utility level in any state is determined by the final wealth, which mostly provides a positive value of utility for the state. On the contrary, the value function under loss aversion consists of a positive value from the gain domain and a negative value from the loss domain in accordance with a reference point. Thus, a decision-making problem can be solved by determining the sign of the value function. In other words, if the value function turns out to be positive, a potential decision is preferred over a reference point, whereas the reference point is preferred over the decision if the value function is negative.[33]

$V > 0$	*A decision is preferred.*
$V \leq 0$	*A reference point is preferred.*

We assume that the decision-maker is a value maximizer with the KT value function to find the optimal decision on risk controls and cyber-insurance, thereby solving the following optimization problem:

$$\max_{z \in H} V(z), \tag{10}$$

where $z = (p, 1-p, x_1, x_2)$ in Eq. (4) and H is a decision space under loss aversion.

As a benchmark case, the optimal demand for cyber-insurance under the expected utility theory can be examined. Eckles and Volkman-Wise (2019) compare the expected utility theory and prospect theory by taking a power law utility function similar to CRRA utility for the former. This function is comparable with the value function in the gain domain with risk aversion (i.e., Eq. (1) when a random variable, x, is positive), and the diminishing sensitivity parameter, α, can be regarded as the risk aversion parameter in [0,1]. Following Eckles and Volkman-Wise (2019), we derive the optimal decision on cyber-insurance under the expected utility theory with our model framework. The model set-up in Eckles and Volkman-Wise (2019) takes into account the deductible with a loading factor as in this paper, but does not count a self-protection measure.

Our finding is consistent with their finding that agents with self-protection effort under the expected utility theory will purchase full insurance given if a fair premium is provided, whereas partial insurance is preferred in the presence of a loading factor.[34]

[30] As supporting evidence, Baillon et al. (2020) empirically tested with 139 participants what reference points they would choose for decision-making and found that the status quo and the maximum outcome that they can achieve are most often selected as the reference point.

[31] Ehrlich and Becker (1972) show that in equilibrium market insurance is a substitute for self-insurance, but a complement to self-protection. Courbage (2001) supports their conclusion by taking the Dual Theory by Yaari (1987) that an increasing price of insurance can lead to increasing self-insurance activity. Our cases are in line with this finding that we compare the reference point of self-protection to a decision on cyber-insurance with self-protection (complement) and the reference point of self-insurance to a decision on cyber-insurance (substitute; both with self-protection). One might argue that self-insurance could be tailored in a way that it covers exclusions of the existing insurance policies (thus, a complement to cyber-insurance). However, this argument can make sense when self-insurance refers to a self-financing (funding) method, for example, captive insurance. Note that substitutability of market insurance and self-insurance might not hold in case of non-reliable self-insurance activity (e.g., self-insurance activities disabled by a loss event; see Courbage, 2001).

[32] We apply the structure of tables in Schmidt (2016) to Table 2 for a clear overview of the model framework.

[33] Andalib et al. (2018) also use the sign of the value function to figure out the desirability of the choice. In other words, if the value function is negative, the choice (the scenario in our case) is undesirable. Finding the sign of the value function with the reference point of the average project costs, they evaluate an investment project upon the framework of the real options valuation.

Table 6
Critical Value of the Contagion Level (Case 2).

		α									
		p_i = 0%					p_i = 50%				
Net margin = 10 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.611	0.714	0.798	0.862	0.905	0.223	0.428	0.596	0.725	0.809
	1.75	0.688	0.777	0.847	0.898	0.930	0.376	0.555	0.694	0.795	0.860
	2.25	0.739	0.818	0.877	0.919	0.945	0.478	0.636	0.754	0.837	0.889
	2.75	0.776	0.846	0.897	0.932	0.954	0.552	0.692	0.794	0.865	0.909
	3.00	0.791	0.857	0.905	0.938	0.958	0.581	0.714	0.809	0.875	0.916
Net margin = 50 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.573	0.606	0.639	0.670	0.697	0.145	0.212	0.277	0.340	0.394
	1.75	0.652	0.683	0.712	0.740	0.763	0.304	0.366	0.424	0.480	0.526
	2.25	0.707	0.735	0.761	0.785	0.805	0.414	0.470	0.522	0.570	0.611
	2.75	0.747	0.772	0.795	0.817	0.835	0.493	0.544	0.591	0.634	0.670
	3.00	0.763	0.787	0.809	0.830	0.847	0.526	0.574	0.619	0.659	0.693
Net margin = 100 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.556	0.556	0.556	0.556	0.556	0.111	0.111	0.111	0.111	0.111
	1.75	0.636	0.636	0.636	0.636	0.636	0.273	0.273	0.273	0.273	0.273
	2.25	0.692	0.692	0.692	0.692	0.692	0.385	0.385	0.385	0.385	0.385
	2.75	0.733	0.733	0.733	0.733	0.733	0.467	0.467	0.467	0.467	0.467
	3.00	0.750	0.750	0.750	0.750	0.750	0.500	0.500	0.500	0.500	0.500

Note: The table shows the critical values of the contagion level to achieve inequality (17) with varying possible values of net margin as examples (the condition holds if the contagion is higher than the critical value for each case). As the net margin is bigger, the critical value of the contagion level is lower. Note that for the case of 100 % net margin ($\frac{g_i \bullet L}{K(g_i)} - 1 = 1$), the probability criteria are indifferent from the diminishing sensitivity parameter, α (see inequality (17)).

However, it provides no evidence of agents' behavioral bias toward extreme events, considering them to be unrealistic so they tend to underinvest in risk control measures. In what follows, we establish a conceptual framework under loss aversion assumption in contrast with the classical decision model by evaluating loss and gain compared to the reference point considering the current market circumstance to rationalize this market behavior.

4.1. Case 1: Decision on cyber-insurance with reference point 1

The reference point is set as the status quo with self-protection in this case; hence, positive externality works in the interconnected network environment. A public good potentially functions for all relevant parties in the network environment, and agent *i* intends to evaluate the optimal decision on self-protection and the purchase of cyber-insurance by comparing two options. In this case, agent *i* recognizes the no loss state as a loss due to the premium payment, whereas she recognizes the loss state as a gain because of the indemnity payment. With the gain and loss values in Table 2, the expected value under loss aversion is defined as

$$V = (1 - \hat{p}_i) \bullet v(-\pi) + \hat{p}_i \bullet v(I - \pi) \tag{11}$$

Clearly, the indemnity needs to be larger than the premium ($I > \pi$) to derive a gain and a loss of the decision on cyber-insurance ($I > \pi$), where the loss is bigger than the deductible level, leading to the condition $\hat{p}_i < \frac{1}{1+\delta}$.[35] If purchasing cyber-insurance is preferred, the value function must be positive. Apply the KT value function to Eq. (11), the preferred decision on cyber-insurance is defined as

$$V = -\lambda \bullet (1 - \hat{p}_i) \bullet \pi^{\alpha} + \hat{p}_i \bullet (I - \pi)^{\alpha} > 0 \tag{12}$$

Eq. (12) can be rewritten as:

$$\left[\frac{1 - (1 + \delta) \bullet \hat{p}_i}{(1 + \delta) \bullet \hat{p}_i} \right]^{\alpha} > \lambda \bullet \frac{1 - \hat{p}_i}{\hat{p}_i} \tag{13}$$

[34] See Appendix A.1 for more detail on the proof of optimal demand under expected utility theory.
[35] To recognize the loss state as a gain, the outcome of the loss state ($= I - \pi$) must be positive; thus, $I - \pi = (L - d)^{+} \bullet \beta - (1 + \delta) \bullet \hat{p}_i \bullet (L - d)^{+} \bullet \beta > 0$, leading to $1 - (1 + \delta) \bullet \hat{p}_i > 0$.

Inequality (13) holds only if the loading factor is small enough, KT parameters ($= \lambda, \alpha$) are also small enough, and the loss probability is large enough.[36] This implies that cyber-insurance with self-protection effort is only preferred for agents, who have less loss aversion (lower λ) and more diminishing sensitivity to the reference point (lower α) when a loss is more likely to occur (higher $\hat{p}$).[37] This result is in line with Schmidt's (2016) finding, where the author sets no insurance (the status quo) as the reference point. To provide a clearer idea on these conditions, we derive a numerical example with particular values of parameters, shown in Table 3. We set the loading factor δ in the range between 10 % and 30 %[38] and consider different KT parameters (α and λ) to identify the criteria to satisfy inequality (13).[39]

We find that an agent with higher loss aversion (higher λ) and less diminishing sensitivity to the reference point (higher α) tends to not make decisions on purchasing insurance. This tendency is more prominent as the loading factor is higher. Even for an agent with the opposite propensity (lower loss aversion and more diminishing sensitivity), cyber-insurance is an attractive option for cyber risk transfer only when the loss probability is high enough. This finding demonstrates a behavior that the agent is inclined to stay with self-protection against cyber risks. The agent only considers cyber-insurance unfairly priced in the current market if a loss occurrence is nearly certain with the amount above the deductible level. The following proposition summarizes this finding.

Proposition 1. Suppose an agent with the KT value function ($\alpha \in [0,1]$ and $\lambda \geq 1$) makes a decision about purchasing cyber-insurance with continuous effort on self-protection by comparing it to its status quo only with self-protection. The agent is willing to purchase cyber-insurance if both conditions are satisfied; thus, inequality (13) holds, and the loading factor is lower than $\frac{1-\alpha}{\alpha}$.

Proof. See Appendix A.2. ∎.

The finding in Table 3 poses a question about how the condition of the actual loss probability ($\hat{p}_i$) can be associated with the contagion level (θ). The conditions in Table 3 to satisfy inequality (13) are optimized solutions and if the agent *i*'s own loss probability (p_i) is larger than the critical value of a condition, she would purchase insurance regardless of the contagion level or the indirect loss probability (p_j). However, if the own loss probability is lower than the critical loss probability of a condition, the agent would take into consideration the contagion level in decision-making.

To address the association between the satisfaction of the conditions in Table 3 and the contagion level, we design scenarios with two parameters of the own loss probability (p_i): zero (the agent *i* makes massive efforts on self-protection)[40] and 50 % (arbitrary level, but much close to the critical values). For both cases, it is assumed that a loss event from an interconnected party almost surely occurs (i.e. $p_j = 1$) so that it can make the scenarios isolate the impact of the contagion level on the conditions (i.e. to see how the risk contagion can be associated with decision-making criteria).

Table 4 shows the necessary value of the contagion level (θ) to fulfil inequality (13) for each pair of KT value function parameters in two scenarios.[41] Agents with massive investments in self-protection (thus $p_i \approx 0$) purchase insurance only if the contagion level is very high. Agents with less effort on self-protection ($p_i = 50\%$) care about interdependency in risks more than those with higher self-protection and thereby are more likely to purchase insurance. Furthermore, the necessary contagion level increases with loss aversion and for higher values of λ the inequality condition (13) is still not satisfied (i.e., "F" in the table), implying a optimism bias in that they are not concerned about risk contagion.

Reconsidering Eq. (5) for $\hat{p}_i$ and the results of Table 4, we note that with increasing level of contagion $\hat{p}_i$ gets larger, thus it becomes more likely that $\hat{p}_i$ is above the critical value and agents buy insurance. However, the consequences may vary by the magnitude of interconnections. For the case that a single party is interconnected in the network environment, the impact of $\theta(s_i, s_j)$ on $\hat{p}_i$ can rather be modest. If the loss probabilities are in areas typical for insurance products, e.g., $p_i = p_j = 0.1$[42] then an increase of

[36] In addition, it is observed that although inequality (13) depends on the size of the loading factor potentially associated with the coverage level, it is indifferent from the size of deductible, implicitly derived by cancelling out the indemnity from the loss and gain of the state.

[37] The parameter for diminishing sensitivity ($= \alpha$) determines the size of curvature of the value function, where a lower level of the parameter leads to a higher curvature around the reference point in both gain and loss states (left panel of Fig. 3). The lower level of the parameter addresses more diminishing sensitivity to the reference point, meaning that the marginal increase in utility (value) is much larger nearer the reference point. Thus, a small sensitivity parameter enhances the implications of classical decision theory in the gain domain (i.e. strong risk aversion against a gain), whereas it implies in the loss domain that individuals are more sensitive to small losses (i.e. weak loss aversion) (Wakker et al., 2007). Inversely, less sensitivity with large sensitivity parameter ($\alpha \to 1$, which is nearly a linear line) accounts for the fact that individuals are almost always averse against a loss regardless of its size.

[38] Romanosky et al. (2019) observe that the safety loading is usually set between 25 % and 35 % in the U.S. cyber-insurance market, the size of loading that varies between 10 % and 30 % in other property and casualty lines as evidenced in, for example, Cummins et al. (2006) for property insurance (18 % to 26 % between 1997 and 2004) in the U.S. and Insurance Europe (2015) for motor insurance (23.2 % on average between 2005 and 2013) in Europe.

[39] Inequality (13) with no loading factor is identical to Proposition 1 in Schmidt (2016), where the value of the decision is positive if $\hat{p}_i > \lambda^{1/(1-\alpha)}/(1 + \lambda^{1/(1-\alpha)})$. As Schmidt (2016) concludes, purchasing cyber-insurance is not preferred (negative value of the decision) for most realistic cases that have low loss probability.

[40] Here, we exemplify zero own loss probability as the first case despite its convexity (thus, $p_i \approx 0$), since this example with the other of 50 % loss probability can clarify a comparison in understanding the impact of risk contagion on decision-making of an agent. Our result shows that an agent cares about risk contagion less with sufficient self-protection ($p_i \approx 0$) than insufficient amount.

[41] $p_i = 0$ with $p_j = 1$ implies $\theta(s_i, s_j) = \hat{p}_i$ and $p_i = 0.5$ with $p_j = 1$ implies $\theta(s_i, s_j) = 2\ \hat{p}_i - 1$.

[42] For example, Insurance Europe (2019) presents loss frequency for motor damage claims in European countries, showing claims probability from 11 % of Germany to 30 % of Turkey. Motor damage risks typically do not feature interdependency; hence the claims probability of this risk type might be considered as a proxy for agent's own loss probability (p_i or p_j).

Table 7
Criteria for Replacing Self-insurance by Cyber-insurance in Case 3.

Panel A: The critical values of the loss probability in the first condition of Proposition 4

		α				
Net effect = 10 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	T($\hat{p}_i \geq 0.61$)	T($\hat{p}_i \geq 0.71$)	T($\hat{p}_i \geq 0.80$)	T($\hat{p}_i \geq 0.86$)	T($\hat{p}_i \geq 0.91$)
	1.75	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.78$)	T($\hat{p}_i \geq 0.85$)	T($\hat{p}_i \geq 0.90$)	T($\hat{p}_i \geq 0.93$)
	2.25	T($\hat{p}_i \geq 0.74$)	T($\hat{p}_i \geq 0.82$)	T($\hat{p}_i \geq 0.88$)	T($\hat{p}_i \geq 0.92$)	T($\hat{p}_i \geq 0.95$)
	2.75	T($\hat{p}_i \geq 0.78$)	T($\hat{p}_i \geq 0.85$)	T($\hat{p}_i \geq 0.90$)	T($\hat{p}_i \geq 0.93$)	T($\hat{p}_i \geq 0.95$)
	3.00	T($\hat{p}_i \geq 0.79$)	T($\hat{p}_i \geq 0.86$)	T($\hat{p}_i \geq 0.91$)	T($\hat{p}_i \geq 0.94$)	T($\hat{p}_i \geq 0.96$)
Net effect = 50 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	T($\hat{p}_i \geq 0.57$)	T($\hat{p}_i \geq 0.61$)	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.67$)	T($\hat{p}_i \geq 0.70$)
	1.75	T($\hat{p}_i \geq 0.65$)	T($\hat{p}_i \geq 0.68$)	T($\hat{p}_i \geq 0.71$)	T($\hat{p}_i \geq 0.74$)	T($\hat{p}_i \geq 0.76$)
	2.25	T($\hat{p}_i \geq 0.71$)	T($\hat{p}_i \geq 0.74$)	T($\hat{p}_i \geq 0.76$)	T($\hat{p}_i \geq 0.79$)	T($\hat{p}_i \geq 0.81$)
	2.75	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.77$)	T($\hat{p}_i \geq 0.80$)	T($\hat{p}_i \geq 0.82$)	T($\hat{p}_i \geq 0.84$)
	3.00	T($\hat{p}_i \geq 0.76$)	T($\hat{p}_i \geq 0.79$)	T($\hat{p}_i \geq 0.81$)	T($\hat{p}_i \geq 0.83$)	T($\hat{p}_i \geq 0.85$)
Net effect = 100 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)
	1.75	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.64$)
	2.25	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)
	2.75	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)
	3.00	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)

Panel B: The critical values of the loss probability in the second condition of Proposition 4

		α				
Net effect = 10 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	T($\hat{p}_i \geq 0.50$)	T($\hat{p}_i \geq 0.39$)	T($\hat{p}_i \geq 0.28$)	T($\hat{p}_i \geq 0.20$)	T($\hat{p}_i \geq 0.14$)
	1.75	T($\hat{p}_i \geq 0.58$)	T($\hat{p}_i \geq 0.47$)	T($\hat{p}_i \geq 0.36$)	T($\hat{p}_i \geq 0.26$)	T($\hat{p}_i \geq 0.19$)
	2.25	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.53$)	T($\hat{p}_i \geq 0.42$)	T($\hat{p}_i \geq 0.31$)	T($\hat{p}_i \geq 0.23$)
	2.75	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.58$)	T($\hat{p}_i \geq 0.47$)	T($\hat{p}_i \geq 0.35$)	T($\hat{p}_i \geq 0.27$)
	3.00	T($\hat{p}_i \geq 0.70$)	T($\hat{p}_i \geq 0.60$)	T($\hat{p}_i \geq 0.49$)	T($\hat{p}_i \geq 0.37$)	T($\hat{p}_i \geq 0.28$)
Net effect = 50 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	T($\hat{p}_i \geq 0.54$)	T($\hat{p}_i \geq 0.50$)	T($\hat{p}_i \geq 0.47$)	T($\hat{p}_i \geq 0.44$)	T($\hat{p}_i \geq 0.40$)
	1.75	T($\hat{p}_i \geq 0.62$)	T($\hat{p}_i \geq 0.59$)	T($\hat{p}_i \geq 0.55$)	T($\hat{p}_i \geq 0.52$)	T($\hat{p}_i \geq 0.49$)
	2.25	T($\hat{p}_i \geq 0.68$)	T($\hat{p}_i \geq 0.65$)	T($\hat{p}_i \geq 0.61$)	T($\hat{p}_i \geq 0.58$)	T($\hat{p}_i \geq 0.55$)
	2.75	T($\hat{p}_i \geq 0.72$)	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.66$)	T($\hat{p}_i \geq 0.63$)	T($\hat{p}_i \geq 0.60$)
	3.00	T($\hat{p}_i \geq 0.74$)	T($\hat{p}_i \geq 0.71$)	T($\hat{p}_i \geq 0.68$)	T($\hat{p}_i \geq 0.65$)	T($\hat{p}_i \geq 0.62$)
Net effect = 100 %		0.1	0.3	0.5	0.7	0.88
λ	1.25	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)	T($\hat{p}_i \geq 0.56$)
	1.75	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.64$)	T($\hat{p}_i \geq 0.64$)	T($p_i \geq 0.64$)	T($\hat{p}_i \geq 0.64$)
	2.25	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)	T($\hat{p}_i \geq 0.69$)
	2.75	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)	T($\hat{p}_i \geq 0.73$)
	3.00	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)	T($\hat{p}_i \geq 0.75$)

Note: The table shows the criteria for the loss probability to achieve the conditions of Proposition 4 with varying possible values of net effect as examples (the conditions hold if the loss probability is higher than the critical value for each case). T indicates that two conditions of Proposition 4 in panels A and B hold with the level of the loss probability in the corresponding parentheses. The net effect in panel A indicates the effect of the transition from self-insurance to cyber-insurance, and the one in panel B accounts for the effect of staying with self-insurance.

Table 8
Critical Value of the Contagion Level (Case 3).

Panel A: The critical values of the contagion level for the first condition of Proposition 4

		α									
		$p_i = 0\%$					$p_i = 50\%$				
Net effect = 10 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.611	0.714	0.798	0.862	0.905	0.223	0.428	0.596	0.725	0.809
	1.75	0.688	0.777	0.847	0.898	0.930	0.376	0.555	0.694	0.795	0.860
	2.25	0.739	0.818	0.877	0.919	0.945	0.478	0.636	0.754	0.837	0.889
	2.75	0.776	0.846	0.897	0.932	0.954	0.552	0.692	0.794	0.865	0.909
	3.00	0.791	0.857	0.905	0.938	0.958	0.581	0.714	0.809	0.875	0.916
Net effect = 50 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.573	0.606	0.639	0.670	0.697	0.145	0.212	0.277	0.340	0.394
	1.75	0.652	0.683	0.712	0.740	0.763	0.304	0.366	0.424	0.480	0.526
	2.25	0.707	0.735	0.761	0.785	0.805	0.414	0.470	0.522	0.570	0.611
	2.75	0.747	0.772	0.795	0.817	0.835	0.493	0.544	0.591	0.634	0.670
	3.00	0.763	0.787	0.809	0.830	0.847	0.526	0.574	0.619	0.659	0.693
Net effect = 100 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.556	0.556	0.556	0.556	0.556	0.111	0.111	0.111	0.111	0.111
	1.75	0.636	0.636	0.636	0.636	0.636	0.273	0.273	0.273	0.273	0.273
	2.25	0.692	0.692	0.692	0.692	0.692	0.385	0.385	0.385	0.385	0.385
	2.75	0.733	0.733	0.733	0.733	0.733	0.467	0.467	0.467	0.467	0.467
	3.00	0.750	0.750	0.750	0.750	0.750	0.500	0.500	0.500	0.500	0.500

Panel B: The critical values of the contagion level for the second condition of Proposition 4

		α									
		$p_i = 0\%$					$p_i = 50\%$				
Net effect = 10 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.498	0.385	0.283	0.200	0.141	T	T	T	T	T
	1.75	0.582	0.467	0.356	0.259	0.187	0.163	T	T	T	T
	2.25	0.641	0.530	0.416	0.310	0.229	0.282	0.060	T	T	T
	2.75	0.686	0.580	0.465	0.354	0.266	0.372	0.159	T	T	T
	3.00	0.704	0.601	0.487	0.374	0.283	0.409	0.201	T	T	T
Net effect = 50 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.538	0.504	0.469	0.435	0.404	0.077	0.008	T	T	T
	1.75	0.620	0.587	0.553	0.519	0.487	0.240	0.174	0.106	0.037	T
	2.25	0.677	0.646	0.614	0.581	0.550	0.355	0.293	0.228	0.161	0.100
	2.75	0.720	0.691	0.660	0.629	0.599	0.439	0.382	0.321	0.257	0.198
	3.00	0.737	0.709	0.680	0.649	0.620	0.474	0.418	0.359	0.297	0.240
Net effect = 100 %		0.1	0.3	0.5	0.7	0.88	0.1	0.3	0.5	0.7	0.88
λ	1.25	0.556	0.556	0.556	0.556	0.556	0.111	0.111	0.111	0.111	0.111
	1.75	0.636	0.636	0.636	0.636	0.636	0.273	0.273	0.273	0.273	0.273
	2.25	0.692	0.692	0.692	0.692	0.692	0.385	0.385	0.385	0.385	0.385
	2.75	0.733	0.733	0.733	0.733	0.733	0.467	0.467	0.467	0.467	0.467
	3.00	0.750	0.750	0.750	0.750	0.750	0.500	0.500	0.500	0.500	0.500

Note: The table shows the criteria for the contagion level to achieve the conditions of Proposition 4 with varying possible values of net effect as examples (the conditions hold if the contagion is higher than the critical value for each case). T in panel B indicates that the second condition of Proposition 4 holds regardless of the contagion level. The net effect in panel A indicates the effect of the transition from self-insurance to cyber-insurance, and the one in panel B accounts for the effect of staying with self-insurance. As the loading factor is bigger, the critical value of the contagion level is bigger. Note that for the case of 100 % net effect (the equations in the parentheses on the left hand side of Proposition 4), the probability criteria for both panels are indifferent from the diminishing sensitivity parameter, α.

$\theta(s_i, s_j)$ from 0 to 0.5 and 1 leads to $\hat{p}_i$ only from 0.1 to 0.145 and 0.19 respectively, which is all very far from the necessary values to buy insurance.

For $p_i = p_j = 0.2$ an increase of $\theta(s_i, s_j)$ from 0 to 0.5 and 1 leads to $\hat{p}_i$ from 0.2 to 0.28 and 0.36 respectively. It thus seems that both in an environment without interconnections (see Schmidt, 2016) and with interconnections to a single party purchasing cyber-insurance is not preferred for most realistic cases with relatively low loss probability. However, if multiple parties are interconnected to the agent i, her loss probability with contagion risk, $\hat{p}_i$, would count on the aggregate loss probability of all interconnected parties with their dependent structure. In this case, the agent i's loss probability may be more likely to exceed the critical values, thus insurance can be a realistic solution to manage cyber risk.

We next investigate how the self-protection measure affects the value of the decision. The optimization problem for the agent with the value function of Eq. (11) can be resolved with respect to the level of self-protection. The following proposition reveals the decision on self-protection effort when the agent is considering an insurance option in the decision-making process.

Proposition 2. Suppose that an agent in the interconnected environment is a value maximizer with the expected value in Eq. (11). The marginal value of the agent decreases over the level of self-protection if the following condition is satisfied:

$$\frac{\alpha}{1+\alpha} < \hat{p}_i < \frac{1}{(1+\alpha)(1+\delta)} \quad , \tag{14}$$

where α indicates the parameter of diminishing sensitivity homogeneous in both gain and loss spaces, as shown by Tversky and Kahneman (1992). Conversely, increasing marginal value is observed over the level of self-protection if the following condition is satisfied:

$$\frac{1}{(1+\alpha)(1+\delta)} < \hat{p}_i < \frac{\alpha}{1+\alpha}$$

Proof. See Appendix A.3. ∎.

Proposition 2 leads to the link between the level of self-protection and insurance premium that the decreasing marginal value with the level of self-protection holds when the loading factor is smaller than $\frac{1-\alpha}{\alpha}$, whereas the increasing marginal value holds with a higher loading factor. For instance, applying the KT parameter ($\alpha = 0.88$), we identify that increasing the self-protection effort results in declining marginal value if the loading on the insurance premium is lower than 13.6 %. Intuitively, it describes a relationship that, by comparing the insurance decision with the reference point of self-protection, the agent in the KT prospect theory world is more incentivized to increase self-protection if a highly loaded premium is given. This supports the finding in Table 3 in that inequality (13) does not hold as the loading factor is higher, showing that the value of the decision on cyber-insurance becomes negative.[43]

As illustrated in the right panel of Fig. 3, the area above the line indicates a positive marginal value reflecting an incentive to increase self-protection with highly loaded insurance scenarios. Proposition 2 also holds when the first order condition is investigated with respect to the level of self-protection by interconnect agent j.[44] Thus, the self-protection measure and the insurance decision are substitutes for an agent with the reference point of self-protection, which is counter to Ehrlich and Becker (1972) under expected utility theory. In addition, positive externality from self-protection as a public good is more effective, particularly in a situation where agents cannot find affordable insurance policy in the market.

4.2. Case 2: Decision on self-insurance with reference point 1

In this case, we compare the decision for self-insurance on top of self-protection measure with the reference point. Agent i recognizes the no loss state as the occurrence of a loss due to the cost for self-insurance. The expected value of this case is defined as

$$V = (1-\hat{p}_i)\cdot v(-K(g_i)) + \hat{p}_i \cdot v(g_i \cdot L - K(g_i)) \tag{15}$$

For the self-insurance plan to be effective in this decision-making, $g_i \geq \frac{K(g_i)}{L}$ needs to hold so that the expected value is determined in both loss and gain states. In other words, this condition implies that the self-insurance coverage above a certain level is required to achieve the validity of the decision-making problem in self-insurance under loss aversion. We evaluate the necessary condition on the positive value addressing the tendency for self-insurance. The preferred decision on self-insurance is defined as

$$V = -\lambda\cdot(1-\hat{p}_i)\cdot K(g_i)^{\alpha} + \hat{p}_i \cdot (g_i \cdot L - K(g_i))^{\alpha} > 0 \tag{16}$$

We rewrite Eq. (16) as follows:

$$\hat{p}_i > \frac{1}{\left(\frac{g_i \cdot L}{K(g_i)} - 1\right)^{\alpha}/\lambda + 1} \quad , \tag{17}$$

where $\frac{g_i \cdot L}{K(g_i)}$ accounts for the ratio between the self-insurance endowment and its cost; thus, $\frac{g_i \cdot L}{K(g_i)} - 1$ can be said to be the net margin of self-insurance. Under the assumption that self-insurance is effective in this case (i.e., $g_i \geq \frac{K(g_i)}{L}$), net margin should be positive.

Net margin of self-insurance depends on the magnitude of a loss so that a larger loss results in a bigger net margin.[45] As can be observed in Table 5, a more loss averse agent (higher λ) with less diminishing sensitivity to the reference point (higher α) is more likely to not invest in self-insurance, and this propensity is stronger as the net margin of self-insurance becomes lower (i.e., the criterion on the loss probability in inequality (17) is higher). However, the criterion on the loss probability to prefer self-insurance is still high in any case (at least above 0.5). This finding is clarified in Proposition 3.

[43] In Appendix C.1, we describe how indifference curves can be derived to address the decision-making of this case in a graphical manner.

[44] The optimization problem is symmetrical between agent i and interconnected agent j, meaning that the result of the first order condition with respect to the level of self-protection by the interconnected agent is identical to that with respect to agent i's self-protection level.

[45] Let us denote the net margin function by $A(L, g_i) = \frac{g_i \cdot L}{K(g_i)} - 1$. The first order condition of net margin with respect to the loss variable is $\frac{\partial A(L, g_i)}{\partial L} = \frac{g_i}{K(g_i)} > 0$.

Proposition 3. Suppose an agent with the KT value function ($\alpha \in [0,1]$ and $\lambda \geq 1$) decides to implement self-insurance with continuous effort on self-protection by comparing it to its status quo only with self-protection. The agent is willing to implement self-insurance if both conditions are satisfied—namely, inequality (17) holds, and $g_i \geq \frac{K(g_i)}{L}$.

Proof. See Appendix A.4. ∎.

We again break down the actual loss probability to examine how the contagion level impacts the decision on self-insurance. Table 6 displays the critical values of the contagion level leading agents to make the decision of implementing self-insurance. In line with the finding in case 1, agents with massive self-protection ($p_i \approx 0$) are less concerned about risk spread from the interconnected environment and this grows for more loss averse agents from the cost of additional risk management measure. Investing in self-insurance is not preferred for relatively low loss probabilities, especially when loss aversion increases. This finding again holds irrespective of the degree of interdependence.

4.3. Case 3: Decision on cyber-insurance with reference point 2

An agent could make the maximum effort by itself, which can provide a safe option without any transfer measure. Based on this possible maximum effort, the agent evaluates decision-making outcome by switching from self-insurance to cyber-insurance when self-protection continues to be implemented as a basic management option. This evaluation is relevant under the assumption that cyber-insurance and self-insurance are substitutes for each other as shown by Ehrlich and Becker (1972); hence, the agent might take into account the difference in the cost and the value of the decision between two options. The expected value of this case is defined as

$$V = (1 - \hat{p}_i) \bullet v(K(g_i) - \pi) + \hat{p}_i \bullet v(I - g_i \bullet L + K(g_i) - \pi) \tag{18}$$

To see the indifference curve in the second quadrant, the signs of the gain and the loss should be opposite each other, which splits Eq. (18) into two cases: 1) $K(g_i) - \pi \leq 0$, $I - g_i \bullet L + K(g_i) - \pi > 0$ and 2) $K(g_i) - \pi > 0$, $I - g_i \bullet L + K(g_i) - \pi \leq 0$.[46]

The first case indicates that cyber-insurance charges a higher premium to provide higher coverage for loss than the cost of self-insurance with lower coverage.[47] The second case is the opposite instance, where self-insurance with more coverage costs higher than cyber-insurance with lower coverage does. The following proposition summarizes decision-making outcomes of two possible cases in this scenario.

Proposition 4. Suppose an agent with the KT value function ($\alpha \in [0,1]$ and $\lambda \geq 1$) decides to purchase cyber-insurance with continuous effort on self-protection by comparing it to the maximum effort (self-protection and self-insurance). The agent is willing to purchase cyber-insurance instead of self-insurance if the following conditions are satisfied:

Proof. See Appendix A.5. ∎.

For cyber-insurance	
i) Positive net effect of the transition from self-insurance to cyber-insurance:	$\left[\frac{I - g_i \bullet L}{\pi - K(g_i)} - 1\right]^{\alpha} > \lambda \bullet \frac{1 - \hat{p}_i}{\hat{p}_i}$
ii) Positive net effect of staying with self-insurance:	$\left[\frac{g_i \bullet L - I}{K(g_i) - \pi} - 1\right]^{\alpha} < \frac{1}{\lambda} \bullet \frac{\hat{p}_i}{1 - \hat{p}_i}$

The equations in the parentheses on the left hand side can explain the net effect of choosing a particular insurance type; the equation in the first condition addresses the net effect of the transition from self-insurance to cyber-insurance, whereas the one in the second condition indicates the net effect of staying with self-insurance. These net effects are all positive with the inequality assumptions from Eq. (18).[48] Table 7 shows the criteria for the loss probability that makes the conditions of Proposition 4 hold. For the first condition in panel A, the numerical results are identical to those in Table 5 (Case 2).

[46] As the size of the deductible gets closer to 0, the first case is more likely to appear, which can be shown as
1) $K(g_i) - \pi = K(g_i) - (L - d)^+ \bullet \beta \bullet (1 + \delta) \bullet \hat{p}_i \leq 0$,
2) $I - g_i \bullet L + K(g_i) - \pi = I - \pi + [K(g_i) - g_i \bullet L] = (1 - (1 + \delta) \bullet \hat{p}_i) \bullet (L - d)^+ \bullet \beta > 0$.
It can result in higher critical values of the loss probability, as in panel A of Table 7, which implies that an agent is less likely to switch its self-insurance plan to cyber-insurance when the premium level and the size of indemnity become higher, but the transition to cyber-insurance is not effective (low net margin).

[47] To prove this, the following inequality should hold
$|I - g_i \bullet L| > |K(g_i) - \pi|$,
where $I - g_i \bullet L > 0$ as $K(g_i) - \pi \leq 0$ and $I - g_i \bullet L + K(g_i) - \pi > 0$. Then, the right side of this inequality can be rewritten
$I - g_i \bullet L = (\beta - g_i) \bullet L - d \bullet \beta > 0$.
Thus, $\beta - g_i > 0$ should hold.

[48] In Appendix C.3, we also show indifference curves of this case to address the decision-making in a graphical manner.

This result implies that a more loss averse agent (higher λ) with less diminishing sensitivity to the reference point (higher α) is more likely to stay with self-insurance; this tendency is stronger as the net effect of the transition from self-insurance to cyber-insurance decreases. The results in panel B of Table 7 from the second condition are exactly in line with this finding by showing the reverse outcomes in that a more loss averse agent (higher λ) with less diminishing sensitivity to the reference point (higher α) is more likely to take up cyber-insurance instead of self-insurance; it tends to be stronger as the net effect of staying with self-insurance decreases.

Table 8 shows the critical values of the contagion level derived in the same manner as in two previous cases. The results demonstrate that more loss averse agents are less sensitive to the contagion level so that they are less likely to switch to cyber-insurance if they believe self-protection is implemented well and the net effect of switching is not high enough. If agents do not make sufficient effort on self-protection, it is overall highly likely that agents purchase cyber-insurance instead of implementing self-insurance across the size of the net effect of switching. Note that critical values in panel A of Table 8 are identical to those in Table 6 of case 2 under our simplified examples, since inequality (13) in case 2 can be identical to the first condition of Proposition 4 if the payoffs of both prospects are identical (i.e. equations in the parentheses on the right hand side of inequality (13) and the first condition of Proposition 4). The conditions of risk contagion in Table 8 can vary in how the payoff of taking cyber-insurance instead of self-insurance is determined.

5. Conclusion

We explore a conceptual framework to investigate decision-making in cyber risk management with a partial form of CPT illustrating utility loss aversion. The framework is constructed in the presence of interdependent risk as a key feature of cyber risk, against which agents typically self-protect. We consider cyber-insurance (market insurance) and risk control measures (self-protection and self-insurance) as risk management options and investigate their interaction in both loss and gain domains of our descriptive decision model distinguished from many studies that address behavioral decision-making in a domain-specific framework demonstrating all prospects defined in either loss or gain domain.

We use self-protection as a status quo reference point, given the fundamental role that self-protection (e.g., the installation of firewalls) typically has in the presence of interconnected risks, sometimes even required by law. We compare the reference point with 1) cyber-insurance and 2) self-insurance under the assumption that self-protection continues to be implemented. We also consider self-protection and self-insurance as an alternative reference point and compare it to the decision on cyber-insurance only with the self-protection measure.

In the different scenarios, we come to the consistent conclusion that one with the reference point of self-protection as a basic management tool in the interconnected environment is more likely to avoid additional cyber risk management measures (cyber-insurance and self-insurance). A more loss averse agent is more likely to maintain the status quo (self-protection). Our model also provides evidence on an expected tendency that the higher the loading on the fair price of cyber-insurance is imposed, the more likely one is to maintain the status quo.

These findings address optimism bias observed in the current cyber-insurance market that one tends to not choose any additional risk management tool, but to stay only with self-protection. We find conditions on the range of loss probability, the loading factor for cyber-insurance, and the level of coverage for self-insurance, where one is willing to decide on cyber-insurance and self-insurance. By breaking down the actual loss probability with interdependent risk, we further identify that more loss averse agents overall tend to be more inattentive to interdependency in cyber risks when they believe sufficient self-protection is implemented, thereby showing optimism bias.

Our findings are important in particular for corporate risk managers, public policy-makers and insurance companies with regard to decision-making on cyber risk management and understanding of cyber-insurance markets. As an example for corporate risk managers, the literature on cybersecurity in the business and economics domain is becoming more significant and cyber risk is one of the most important risks in the current business environment. Our findings might explain why many corporate risk managers believe that enhancing their own cyber security system via self-protection is sufficient as investment against cyber risk and thus they tend to not invest in other risk management instruments.

In addition, public policies might be demanded to build a collaborative pool against extreme cyber risks, which could reduce the price for such risks to transfer. Such a collaborative risk pool may also help cyber insurers and reinsurers to improve their risk assessment (i.e., cyber insurance underwriting) and pricing. In this context our finding shows that if the price becomes more reasonable, agents would tend to purchase more cyber insurance.

This study opens a discussion using a descriptive decision model on cyber-insurance and risk control measures in the presence of interdependent risk, but several limitations are inherent in our model that might provide motivation for future research. First, in our model the loss is not a random variable in continuous time, but a fixed amount in two economic states for a single period. The randomness of loss size requires estimating its probability distribution, which can affect the consequences for different states of wealth in our model (thus, more than two states can occur), depending on the reference point. For instance, a loss-averse individual may decide to change their reference point based on the resulting probabilities, and such changes may occur contingent on their level of loss aversion.

Furthermore, while the probability of loss occurrence in our model is influenced by the extent of self-protection measures, the size of a random loss may depend on the level of self-protection investments made by the agent herself or by interconnected parties, potentially incorporating time-dynamic features. Therefore, it could be interesting to study this set-up in a continuous time decision-making model for multiple time periods, where there could be a possibility for loss averse individuals, for instance, to adjust their reference points in the next time steps.

Second, it could be a meaningful contribution to the descriptive decision-making model to study how individual decision-making in cyber risk management under loss aversion can be associated with social welfare. This can then lead to a discussion of how the choice of a reference point for an individual should be related to social welfare and how the cyber-insurance market with purchase decisions under loss aversion can affect welfare. Furthermore, a full set of cumulative prospect theory including probability distortion is not taken into consideration in our model, where interdependency in cyber risks replaces the possibility of probability weighting.

Declaration of Competing Interest

The author Martin Eling is an Editorial Board Member for *Risk Sciences* and was not involved in the editorial review or the decision to publish this article. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Supporting information

Supplementary data associated with this article can be found in the online version at doi:10.1016/j.risk.2024.100001.

References

Alary, D., Gollier, C., & Treich, N. (2013). The effect of ambiguity aversion on insurance and self-protection. *The Economic Journal, 123*(573), 1188–1202.

Andalib, M. S., Tavakolan, M., & Gatmiri, B. (2018). Modeling managerial behavior in real options valuation for project-based environments. *International Journal of Project Management, 36*(4), 600–611.

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. M. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems Research and Behavioral Science, 36*(4), 404–423.

Armerding, T. (2018). *The 18 biggest data breaches of the 21st century.* CSO,⟨https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html⟩.

Baillon, A., Bleichrodt, H., & Spinu, V. (2020). Searching for the reference point. *Management Science, 66*(1), 93–112.

Baker, M., & Xuan, Y. (2016). Under new management: Equity issues and the attribution of past returns. *Journal of Financial Economics, 121*(1), 66–78.

Baker, M., Pan, X., & Wurgler, J. (2012). The effect of reference point prices on mergers and acquisitions. *Journal of Financial Economics, 106*(1), 49–71.

Binswanger, J. (2007). Risk management of pensions from the perspective of loss aversion. *Journal of Public Economics, 91*(3-4), 641–667.

Böhme, R., & Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. *Workshop on the Economics and Insurance Security ((WEIS))*.

Bruhin, A., Fehr-Duda, H., & Epper, T. (2010). Risk and rationality: Uncovering heterogeneity in probability distortion. *Econometrica, 78*(4), 1375–1412.

CSIS. (2020). *The hidden costs of cybercrime.* Washington D.C.: Center for Strategic & International Studies.

Claus, E., & Nguyen, V. H. (2023). Biased expectations. *European Economic Review, 154*, Article 104424.

Courbage, C. (2001). Self-insurance, self-protection and market insurance within the dual theory of choice. *The Geneva Papers on Risk and Insurance Theory, 26*(1), 43–56.

Cummins, J., Lin, Y., and Phillips, R. (2006). Capital allocation and the pricing of financially intermediated risks: An empirical investigation. Working paper.

De Bondt, W. F., & Thaler, R. H. (1990). Do security analysts overreact? *American Economic Review, 80*(2), 52–57.

De Giorgi, E. G., & Post, T. (2011). Loss aversion with a state-dependent reference point. *Management Science, 57*(6), 1094–1110.

de Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice, 43*(2), 239–274.

Department for Digital,Culture, Media & Sport (DCMS). (2018). Cyber security breaches survey2018. London: U.K. Government 2018.

Eckles, D., and Volkman-Wise, J. (2019). Loss aversion, probability weighting, and the demand for insurance. Working paper.

Eeckhoudt, L., Fiori, A. M., & Rosazza Gianin, E. (2018). Risk aversion, loss aversion, and the demand for insurance. *Risks, 6*(2), 60.

Ehrlich, I., & Becker, G. (1972). Market insurance, self-insurance, and self-protection. *Journal of Political Economy, 80*(4), 623–648.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109–1119.

Erev, I., Ert, E., & Yechiam, E. (2008). Loss aversion, diminishing sensitivity, and the effect of experience on repeated decisions. *Journal of Behavioral Decision Making, 21*(5), 575–597.

European Insurance and Occupational Pensions Authority (EIOPA). (2018). Understanding cyber insurance—A structured dialogue with insurance companies. Frankfurt: EIOPA.

European Systemic Risk Board. (2020). Systemic cyber risk. Frankfurt: European System of Financial Supervision.

European Union. (2016). The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Regulation (EU) 2016/679 of the European Parliament and of the Council.

Gordon, L., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security ((TISSEC)), 5*(4), 438–457.

Gottlieb, D., & Mitchell, O. S. (2020). Narrow framing and long-term care insurance. *Journal of Risk and Insurance, 87*(4), 861–893.

Grossklags, J., Christin, N., & Chuang, J. (2008). *Secure or insure?: a game-theoretic analysis of information security games. Proceedings of the 17th international conference on World Wide Web.* ACM,209–218.

Harrison, G. W., & Swarthout, T. J. (2020). Cumulative Prospect Thoery in the laboratory: A reconsideration. In Forthcoming, G. W. Harrison, & D. Ross (Eds.). *Models of Risk Preferences: Descriptive and Normative Challenges*.

Hofmann, A. (2007). Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. *The Geneva Risk and Insurance Review, 32*(1), 91–111.

Hofmann, A., & Peter, R. (2016). Self-insurance, self-protection, and saving: On consumption smoothing and risk management. *Journal of Risk and Insurance, 83*(3), 719–734.

Hofmann, A., & Ramaj, H. (2011). Interdependent risk networks: the threat of cyber attack. *International Journal of Management and Decision Making, 11*(5-6), 312–323.

Hofmann, A., & Rothschild, C. (2019). On the efficiency of self-protection with spillovers in risk. *The Geneva Risk and Insurance Review, 44*(2), 207–221.

Holmes, R. M., Bromiley, P., Devers, C. E., Holcomb, T. R., & McGuire, J. B. (2011). Management theory applications of prospect theory: Accomplishments, challenges, and opportunities. *Journal of Management, 37*(4), 1069–1107.

Insurance Europe (2015). *European motor insurance markets.* Brussels: Insurance Europe,.

Jalali, M., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems, 28*(1), 66–82.

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: why entrepreneurs take protective measures. *Behaviour & Information Technology, 35*(5), 368–379.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decisions under risk. *Econometrica, 47*(2), 263–292.

Koop, G. J., & Johnson, J. G. (2012). The use of multiple reference points in risky decision making. *Journal of Behavioral Decision Making, 25*(1), 49–62.

Köszegi, B., & Rabin, M. (2006). A model of reference-dependent preferences. *Quarterly Journal of Economics, 121*(4), 1133–1165.

Köszegi, B., & Rabin, M. (2007). Reference-dependent risk attitudes. *American Economic Review, 97*(4), 1047–1073.
Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty, 26*(2/3), 231–249.
Kunreuther, H., & Michel-Kerjan, E. (2014). *Economics of natural catastrophe risk insurance. In Handbook of the Economics of Risk and Uncertainty*, *Vol. 1*, Amsterdam: North-Holland,651–699.
Lelarge, M., & Bolot, J. (2009). *Economic incentives to increase security in the internet: The case for insurance. INFOCOM 2009*. IEEE,1494–1502.
Lohse, T., Robledo, J., & Schmidt, U. (2012). Self-insurance and self-protection as public goods. *Journal of Risk and Insurance, 79*(1), 57–76.
Mersinas, K., Hartig, B., Martin, K., & Seltzer, A. (2016). Are information security professionals expected value maximizers?: An experiment and survey-based test. *Journal of Cybersecurity, 2*(1), 57–70.
Mürmann, A., & Kunreuther, H. (2008). Self-protection and insurance with interdependencies. *Journal of Risk and Uncertainty, 36*(2), 103–123.
NCSL). (2019). Security breach notifications laws. Retrieved May 7, 2021 from 〈http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx〉.
Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss and observability of self protection. *Risk Analysis, 31*(3), 497–512.
PricewaterhouseCoopers (PwC). (2017). Strengthening digital society against cyber shocks: Key findings from the Global State of Information Security Survey 2018. PricewaterhouseCoopers.
PRC). (2019). Data breaches. Retrieved February 5, 2019 from 〈https://www.privacyrights.org/data-breaches〉.
Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity, 5*(1), 1–19.
Schanz, K. (2019). *Underinsurance in mature economies: Reasons and remedies.* Zurich: The Geneva Association,.
Schmidt, U. (2016). Insurance demand under prospect theory: A graphical analysis. *Journal of Risk and Insurance, 83*(1), 77–89.
Schmidt, U., & Zank, H. (2008). Risk aversion in cumulative prospect theory. *Management Science, 54*(1), 208–216.
Sharot, T. (2011). The optimism bias. *Current biology, 21*(23), R941–R945.
Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2010). *Competitive cyber-insurance and internet security. In Economics of information security and privacy*. New York, NY: Springer,229–247.
Society of Actuaries (2017). *Cybersecurity: Impact on insurance business and operations.* Society of Actuaries (SOA),.
Swiss Re (2016). *Cyber: in search of resilience in an interconnected world.* Zurich: Swiss Re,.
Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference-dependent model. *Quarterly Journal of Economics, 106*(4), 1039–1061.
Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty, 5*(4), 297–323.
von Neumann, J., & Morgenstern, O. (1953). *Theory of games and economic behavior.* Princeton, NJ: Princeton University Press,.
Wakker, P. P., & Tversky, A. (1993). An axiomatization of cumulative prospect theory. *Journal of Risk and Uncertainty, 7*(2), 147–175.
Wakker, P. P., Köbberling, V., & Schwieren, C. (2007). Prospect-theory's diminishing sensitivity versus economics' intrinsic utility of money: How the introduction of the euro can be used to disentangle the two empirically. *Theory and Decision, 63*(3), 205–231.
Wang, S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal, 57*, Article 101173.
Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology, 39*(5), 806–820.
Welburn, J. W., & Strong, A. M. (2021). Systemic cyber risk and aggregate impacts. *Risk Analysis, forthcoming*.
Yaari, M. E. (1987). The dual theory of choice under risk. *Econometrica, 55*(1), 95–115.
Zhang, X. A., & Borden, J. (2020). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research, 23*(10), 1336–1352.
Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Inforamation Systems, 30*(1), 123–152.
Zweifel, P., & Eisen, R. (2012). *Insurance economics.* Berlin Heidelberg: Springer-Verlag,.