Investing in Prevention or Paying for Recovery - Attitudes to Cyber Risk

Anna Cartwright, Edward Cartwright and Lian Xue

Original citation & hyperlink:
Cartwright, A., Cartwright, E., & Xue, L. (2019, October). Investing in Prevention or Paying for Recovery-Attitudes to Cyber Risk. In *International Conference on Decision and Game Theory for Security* (pp. 135-151).
https://dx.doi.org/10.1007/978-3-030-32430-8_9

Published as part of Lecture Notes in Computer Science, Volume 11836

ISSN 0302-9743
ESSN 1611-3349

Publisher: Springer

The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-030-32430-8_9

Investing in prevention or paying for recovery - attitudes to cyber risk*

Anna Cartwright[1][0000−0003−1965−842X], Edward Cartwright[2][0000−0003−0194−9368], and Lian Xue[3]

[1] School of Economics, Finance and Accounting, University of Coventry, UK
ac8373@coventry.ac.uk
[2] Department of Strategic Management and Marketing, De Montfort University
edward.cartwright@dmu.ac.uk
[3] School of Economics, Wuhan University, China.
Lian.Xue@whu.edu.cn

Abstract. Broadly speaking an individual can invest time and effort to avoid becoming victim to a cyber attack and/or they can invest resource in recovering from any attack. We introduce a new game called the prevention and recovery game to study this trade-off. We report results from the experimental lab that allow us to categorize different approaches to risk taking. We show that many individuals appear relatively risk loving in that they invest in recovery rather than prevention. We find little difference in behavior between a gain and loss framing.

Keywords: cyber-security · ransomware · insurance · recovery · risk aversion.

1 Introduction

Cyber-crime is a growing threat to society that will become increasingly important as reliance on technology grows (e.g. through the internet of things). Extensive evidence suggests, however, that individuals and organizations (both private and public) take excessive risk in cyber-space. Indeed, there are simple and low cost behaviors, such as two factor authentication and regular offline back-ups, that would dramatically decrease the likelihood and costs of a cyber-attack. Yet many individuals, employees and managers do not routinely follow such behavior [1]. An analogy would be a society in which we all rely on cars and yet leave them unlocked with the key in the ignition. A fundamental question is why we observe such risk taking?

In looking at an individual's approach to cyber-security we distinguish between prevention and recovery [2]. We view prevention as decisions enacted *before*

* This research was funded by the Engineering and Physical Sciences Research Council (EPSRC) for project EP/P011772/1 on the EconoMical, PsycHologicAl and Societal Impact of RanSomware (EMPHASIS). The authors would like to thank three anonymous reviewers for there comments on an earlier version of the paper.

an attack with the objective of reducing the likelihood and/or damage from attack. Regular software updates, anti-malware and two factor authentication are primarily aimed at preventing an attack from being 'successful'. Similarly, regular offline-back ups and insurance can prevent an attack from causing significant damage. We view recovery as decisions enacted *after* an attack. For instance, they may have to reset passwords, reformat hard drives or pay for an IT company to recover data and restore systems.

While prevention and recovery are not mutually exclusive we can delineate a strategy that focuses, consciously or not, on prevention and one that focuses on recovery.[4] As a case in point consider ransomware. Crypto-ransomware is a relatively new form of malware in which an individual's files are encrypted and a ransom is demanded for the key to decrypt the files [5–7]. If the encryption is done in a technically sound way then the files are only recoverable by paying the ransom. Crypto-ransomware provides, therefore, a viable business model for criminals and some variants of ransomware have a 'good reputation' for returning files to victims (if the ransom is paid) [8–10]. In another, older variant, of ransomware victims are held to ransom for the release of sensitive information [11].

Consider an individual who stores sensitive information on her computer and is aware of the threat of ransomware. Broadly speaking the individual has two options. She can limit the damage from attack through, say, regular back-ups or insurance against loss. Or she can pay the ransom if attacked in order to try and recover her files. Law enforcement clearly encourage individuals to take the former approach. It would seem, however, that many take the latter approach. For instance, estimates of the proportion of individuals paying the ransom are as high as 40% [12]. To focus on recovery rather than prevention would appear to be risk-taking behaviour.

Evidence from the field of behavioural economics suggests that individuals are more risk seeking in the loss domain than the gain domain [13]. That is, they are more willing to take risks to regain 'losses' than to earn 'gains'. This would appear to be relevant in a cyber context. For instance, an individual who has 'lost' files to a ransom attack may be willing to take a risk in paying the ransom. We also know that perception of loss and gain is sensitive to framing [14, 15]. A growing body of literature has explored the effectiveness of using different frames to influence behaviour [16–18]. These studies suggest that loss aversion can be a factor in shaping individual choice.

The relevance of framing for cyber-security is well acknowledged in the academic literature [19–25].[5] However, prior studies have focused, using our terminology, on either prevention or recovery. In our paper we explore prevention and recovery in tandem. This opens us interesting new avenues for exploration. In

[4] One can also delineate strategies that focus on different aspects of prevention or recovery. For instance [3, 4] compare protection versus insurance, where the former lowers the probability of attack and the latter the damage from attack.

[5] It is also, arguably, acknowledged (consciously or not) by cyber-criminals with ransomware demands threatening the permanent destruction of files etc.

particular, we can check for consistency of behaviour across the two different decision tasks. For instance, do individuals who take risks in terms of prevention also take risks in terms of recovery. Indeed, can it be optimal for an individual to spend on recovery and yet not spend on prevention?

We introduce a new game that captures investment on prevention and recovery in a cyber-security context. The game contains four stages in which individuals invest in prevention against a cyber attack, learn if they are attacked, can spend on recovery if attacked, and then learn if they have regained their files. We explore how behavior is likely to be influenced by a gain or loss frame. We show that an individual is predicted to invest more on recovery in the loss frame than gain frame. Conversely, she is predicted to invest more on prevention in a gain frame than loss frame.

We then report an experiment designed to test the hypotheses of our model. We find only limited support that framing matters. More noteworthy is the large heterogeneity of behavior. A significant proportion of subjects invest mainly in prevention, some mainly in recovery, and then some in both or neither. Moreover, we see a lot of risk taking behavior. The behavior we observe in the lab would seem relatively consistent with that in the field. We argue, therefore, that our game and experimental design can be extended to further explore the trade-off between prevention and recovery.

The rest of the paper is organized as follows. Section 2 summarizes the game, section 3 contains our theoretical results, section 4 presents our experimental results, and section 5 concludes. Supplementary material, including experiment instructions and data, is available on Figshare (https://dmu.figshare.com/).

2 The prevention and recovery game

In this section we introduce a simple game designed to capture salient aspects of the choice between preventing and recovering from cyber-attack. The game consists of four stages. In the first stage, ***the prevention stage***, the individual can spend resource to insure against attack. In the second stage Nature determines if the individual is attacked. In the third stage, ***the recovery stage***, the individual can, if attacked, spend resource on trying to recover her files. In the fourth stage nature determines if the losses are recovered. The game is carefully designed so that we can distinguish different potential influences on behavior. We now explain each stage in more detail.

The individual has computer files worth V tokens. In Stage 1 of the game the individual chooses how much to spend on *preventing loss from cyber-attack*. She can spend any amount up to $\overline{I}$ tokens, where $\overline{I}$ is exogenously given. Let $I \in [0, \overline{I}]$ denote the amount allocated to prevention.

In Stage 2 the individual may suffer a cyber-attack that means she loses the files worth V.[6] The probability of attack is given by $max\left\{\frac{100p-I}{100-I}, 0\right\}$ where p is

[6] Here we assume that all attacks are 'successful'. It would be equivalent to allow for deterrence and distinguish between successful and unsuccessful attacks.

an exogenous parameter capturing the activities of the criminal and factors in place to deter attack. In interpretation, we note that if the individual does not spend on preventing loss, $I = 0$, the probability of attack is p. If the individual spends $I = 100p$ on prevention then the probability of attack is 0. Thus, the more spent on preventing loss (in Stage 1 of the game) the lower the probability of attack.

To make the analysis sharper we assume that resources allocated to prevention are not sunk. This is consistent with compensation for spending on prevention if attacked. For instance, the individual may not need to pay a cyber-security provider if they are attacked. The payoff of the individual at the end of stage 2 is, therefore, 0 if she is attacked and $V - I$ if she is not attacked. Note that if the individual fully prevents attack her payoff is $V - 100p$. If the individual is not attacked then the game ends. If she is attacked then we proceed to stage 3.

In stage 3 the individual has the opportunity to recover her losses. Specifically she can allocate resource to recovery. She can denote any amount up to $\overline{R}$, where $\overline{R}$ is exogenously given. Let $R \in [0, \overline{R}]$ denote the amount allocated to recovery.

In Stage 4 the individual can recover her files. The probability of the individual recovering her files is given by $R/100$. So, if the individual devotes no resource to recovery she has no chance of recovering her losses. If she spends R then she has an $R\%$ chance of recovering her files. The final payoff of the individual is given by $V - R$ if the files are recovered and $-R$ if they are not. Note that money spent on recovery is sunk and so paid irrespective of whether the file is recovered. This captures the notion of paying a ransom to a criminal who may or may not honour their part of the bargain.

A strategy for the individual details the amount of resources allocated to preventing loss, I, and the amount that will be spent on recovery, R, in the event of attack. The strategy space is, therefore, $[0, \overline{I}] \times [0, \overline{R}]$.[7]

3 Theory

We begin with some preliminary definitions. A prospect $(x_1, q_1; x_2, q_2; ...; x_n, q_n)$ lists a set of n possible outcomes $x_1, ..., x_n$ and the probability of each outcome $q_1, ..., q_n$ (where $\sum_i p_i = 1$) [26]. The expected value of a prospect $(x_1, q_1; ...; x_n, q_n)$ is given by $\sum_{i=1}^{n} x_i q_i$. The expected deviation from expected value is given by $\sum_{i=1}^{n} |x_i - e| q_i$ where e is expected value. We say that a prospect is a sure thing if $n = 1$ and a risky prospect if $n > 1$.

Consider two prospects, $A = (x_1^A, q_1^A; ...; x_n^A, q_n^A)$ and $B = (x_1^B, q_1^B; ...; x_m^B, q_m^B)$. Suppose that A and B have the same expected value and B has a smaller expected deviation from expected value. Adopting standard terminology (without being constrained to a particular functional form) we say that an individual is risk averse (on domain A, B) if she prefers prospect B to A, is risk loving if she prefers A to B and is risk neutral if she is indifferent between A and B. Note that this definition is agnostic on whether risk aversion is due to curvature of

[7] If $I = 100p$ then attack is impossible and so, theoretically, there is a redundancy in choosing R in this case.

the utility function and/or loss aversion [27]. It merely says that a risk averse individual prefers more certainty.

We further distinguish between gains and losses. We say that a prospect is on the gain domain if the expected value is positive and on the loss domain if the expected value is negative. This terminology allows us to capture a reflection effect in which an individual is risk averse on the gain domain (would prefer prospect B to A if the expected value of the prospects is positive) and risk loving on the loss domain (would prefer prospect A to B if the expected value of the prospect is negative) [13].

To solve for the optimal strategy of the individual in the prevention and recovery game we proceed by backward induction. This means we start by solving the optimal strategy in the recovery stage and then (knowing what will happen in the recovery stage) solve for the optimal strategy in the prevention stage.

3.1 Recovery stage

Crucially, the prevention and recovery game is designed so that incentives and payoffs in the recovery stage, stage 3, are *independent of the choice of* I in the prevention stage, stage 1. We can, thus, analyze the recovery stage in a relatively straightforward way without taking into account I. In the recovery stage the individual has been attacked and simply has to decide how much to spend on recovery. Inspired by the evidence of loss aversion and reflection effect we hypothesize that attitudes to risk and, therefore, willingness to spend on recovery will be influenced by framing and the reference point. We contrast two possibilities.

In a *gain frame* we think of 0 as the status-quo. This implies that the individual has already internalized the loss of her files and so is now in the mindset of potentially regaining them. To choose R is to choose prospect $(V-R, r; -R, 1-r)$, where $r = R/100$. In other words there is probability r of recovering the files and having payoff $V-R$ and probability $1-r$ of non-recovery and having payoff $-R$. Our game is set up in such a way that if $V = 100$ a risk neutral individual is indifferent as to how much she spends on recovery. Specifically, setting $V = 100$, the expected value from spending R on recovery is

$$EV(R) = V \times \frac{R}{100} - R = 0. \tag{1}$$

Note that, in this case, expected value is independent of R.

To investigate the incentives of an individual who is not risk neutral let us contrast the choice of $R = 0$ and $\overline{R}$. Throughout we fix $V = 100$. If the individual chooses $R = 0$ then her final payoff is 0; so she has sure prospect $(0, 1)$. If she chooses $R = \overline{R}$ then she has $\overline{r} = \overline{R}/100\%$ chance of recovering her files and getting payoff $V - \overline{R}$ and a $(1 - \overline{r})\%$ chance of not recovering her files and getting payoff $-\overline{R}$; so she has prospect $(V - \overline{R}, \overline{r}; -\overline{R}, 1 - \overline{r})$. The individual, therefore, has a choice between a sure thing and a risky prospect (with the same expected value). So, a risk averse individual would set $R = 0$ and a risk loving individual would set $R = \overline{R}$.

In a loss frame we think of $-V$ as the status-quo. This implies that the individual has not accepted the loss of her file and so sees recovery as a way to avoid the loss. Specifically, if she spends nothing on recovery she has sure loss $(-V, 1)$. If she spends $\overline{R}$ on recovery she faces prospect $(-\overline{R}, \overline{r}; -V - \overline{R}, 1 - \overline{r})$. Again, if $V = 100$, a risk neutral individual is indifferent as to her choice of R, a risk averse individual would set $R = 0$ and a risk loving individual would set $R = \overline{R}$.

The preceding discussion leads to our first result.

Proposition 1. *If $V = 100$ an individual who is risk averse will allocate no resource to recovery while an individual who is risk loving will allocate the maximum resource to recovery.*

The reflection effect suggests that individuals will be risk averse in the gain frame and risk loving in the loss frame. Thus, there is a tendency towards $R = 0$ in the gain frame and $R = \overline{R}$ in the loss frame. We, therefore, obtain a testable hypothesis.

Hypothesis 1 *In a gain frame individuals will invest less in recovery than do individuals in a loss frame.*

3.2 Prevention stage

The optimal choice in the prevention stage, stage 1, will depend on what the individual is going to choose in the recovery stage, stage 3. From Proposition 1 we know that (unless the individual is risk neutral) the optimal strategy in the recovery stage will be to choose either $R = 0$ or $R = \overline{R}$. Using a gain and loss frame we will consider each possibility in turn.

In a gain frame the status quo is to have 0 payoff meaning that the individual has not internalized the ownership of the files. So to not be attacked would be a gain. Similarly, to recover the files would be a gain. Suppose that the individual would choose $R = 0$ in stage 3. This means that she makes no attempt to recover her files in the case of being attacked. Her expected value in stage 1, setting $V = 100$, is therefore

$$EV(I) = (V - I) \times \left(1 - \frac{100p - I}{100 - I}\right) = 100(1 - p). \tag{2}$$

Again, a risk neutral individual is indifferent as to how much to spend on prevention.

To progress further contrast the two extremes of $I = 0$ and $I = Vp$. If the individual chooses $I = 0$ then there is a p chance they are attacked and have payoff 0 and a $1 - p$ chance they have payoff V. To not allocate to prevention is, therefore, to choose a risky prospect $(0, p; V, 1 - p)$. If the individual chooses $I = Vp$ then she has final payoff of $V(1 - p)$. To fully prevent is, therefore, to

choose sure prospect $(V(1-p),1)$. Thus, if $V = 100$ a risk averse individual would set $I = Vp$ and a risk loving individual would set $I = 0$.

Next suppose that the individual would choose $R = \overline{R}$ in stage 3. You can verify that the expected value is still $V(1-p)$ and so independent of I. To set $I = Vp$ is still to choose sure prospect $(V(1-p),1)$ and so will appeal to someone who is risk averse. To set $I = 0$ is now to choose over a risky prospect with possible payoffs $-\overline{R}, V-\overline{R}$ and V. This will appeal to someone who is risk loving.

In a loss frame the status-quo is to have V meaning that the individual has internalized ownership of the file. So to be attacked would be a loss. The preceding analysis follows through independent of the frame. But we do need to reconsider the interpretation of fully preventing attack. If the individual sets $I = Vp$ then she has a sure loss of Vp relative to her status-quo. This compares to a sure gain of $V(1-p)$ in the gain frame. The reflection effect would, therefore, point to more risk loving behavior in the loss frame. This leads to our second result and hypothesis.

Proposition 2. *If $V = 100$ an individual who is risk averse will allocate maximum resource to prevention while an individual who is risk loving will allocate nothing to prevention.*

Hypothesis 2 *In the gain frame individuals will invest more on prevention than in the loss frame.*

3.3 Summary

Our two propositions and two hypotheses are summarized in Table 1. Overall we expect a risk averse individual would allocate resource to prevention rather than recovery while a risk loving individual would allocate resource to recovery rather than prevention. Moreover, we predict that in the gain frame individuals are more likely to be risk averse than in the loss frame. We now proceed to an experiment designed to test these predictions.

Table 1. Behaviour in the prevention and recovery game.

Attitudes	Prevention	Recovery	Framing
Risk averse	$I = 100p$	$R = 0$	Gain
Risk loving	$I = 0$	$R = \overline{R}$	Loss

4 Experiment

The Experiment consisted of 20 rounds and was conducted in computer rooms at the University of Kent. Participants were recruited from the general student

population and did not have experience in participating in an individual risk taking experiment. In total 77 participants were recruited, with ages ranging from 18 to 41, 49 of which were female. At the end of the experiment, 2 rounds of the 20 rounds were selected to be paid in cash. 20 tokens were converted to £1. All participants were given an additional £5 show-up fee. The average final earnings were £10.01. All tasks in the experiment were computerized using z-Tree [29].

In each round participants first performed a short real effort task in which they 'earned' a file worth 100 tokens. The task was to solve a travelling salesman problem (TSP) by finding a path between 10 points less than a pre-defined distance. The task was set up in such a way that it was easily solved. Even so, we expected that completing the task may give subjects more ownership over the 'file' and corresponding 100 tokens. An example of a completed file is shown in figure 1. A further benefit of using the (TSP) is that it gives us additional data on participants in terms of route length. This could be seen as a measure of engagement with the experiment.

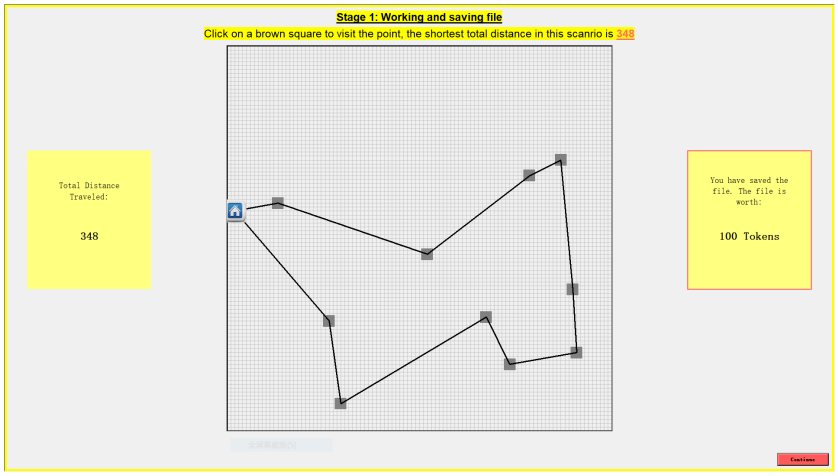

Fig. 1. An example of a completed TSP task

After completing the TSP participants played the prevention and recovery game outlined above. We set $p = 0.5$ and $\overline{R} = 50$. This choice of parameters was designed to give maximal variation in risk. In particular, a subject could choose (in both the prevention and recovery stages) between a sure thing or a prospect with a 50-50 risk profile. In interpretation, $p = 0.5$ means there was a 50% chance of attack in the event of no prevention. This is consistent with an individual who does nothing to prevent attack having a relatively high chance of being attacked. Setting $\overline{R} = 50$ means that an individual has at most a 50%

chance of recovering files after attack. This is consistent with the notion that there is no guarantee files can be recovered after an attack.

In the experiment we consider a relatively continuous choice set in that subjects could allocate any integer amount to prevention, from 0 to 50, and to recovery, also from 0 to 50. In each round participants were asked to make their recovery choice without having been informed of the outcome of the prevention stage. This gives us additional data in that we see the recovery choice of the subject in every round (even if they were not attacked). At the end of the round participants were given full feedback on the outcome in that round (whether they were attacked and whether they recovered their files) before they moved onto the next round.

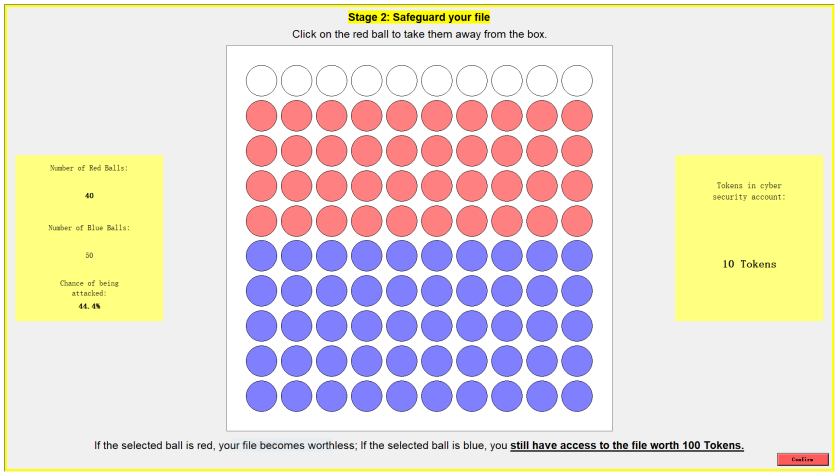

Fig. 2. An example of the prevention stage in the game (investing 10 tokens to prevent the file from attack; I = 10)

Note that in this experiment we deliberately used a cyber-security frame that explicitly talked of files, cyber-attack and recovery etc. The experimental interface was also designed in a way to make the probability of attack and recovery as transparent as possible. Specifically, in the prevention stage participants were presented with a box with 100 balls on their computer screen, 50 of them red and 50 blue. For each token a participant put in a 'cyber-security account' a red ball was removed from the box (see figure 2 for an example). Once the participant had confirmed their choice the computer randomly selected a ball from those remaining. If the selected ball is red, the file would be attacked. If the selected ball is blue, the file would not be attacked.

In the prevention stage participants were presented a box with 100 brown balls. For each token the participant put in a 'recovery account' one brown ball was replaced with a green ball (see figure 3 for an example). Once the participant

had confirmed their choice the computer randomly selected a ball from the box. If the selected ball was brown the file was not recovered and if it was green it was. Note that the visual approach just described, for both the prevention and recovery stage, matches the incentives the in the recovery and prevention game. For example, if $I = 10$ in the prevention stage then 10 red balls are removed and the probability of attack becomes $(50 - I)/(100 - I) = 4/9$. Similarly, if $R = 10$ in the recovery stage then the probability of recovery is $R/100 = 1/10$.

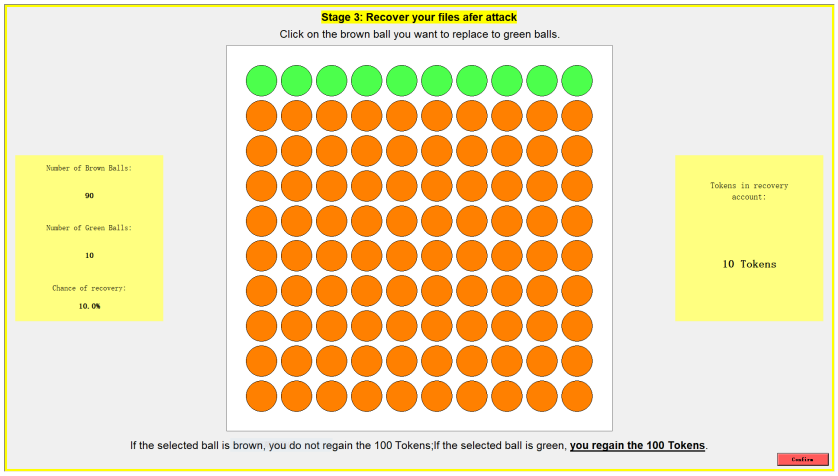

Fig. 3. An example of the recovery stage in the game

We ran two treatments corresponding to a gain and loss frame. The treatments differed only in the instructions provided to subjects. The key differences are illustrated in Table 2. The gain frame emphasizes the potential to gain 100 tokens by keeping or recovering the file. By contrast, the loss frame emphasizes the potential to lose the 100 tokens. Note that a subject was only exposed to one of the treatments - gain or loss. At the end of each treatment, we include two additional sets of questionnaires. One is a domain specific risk taking (DoSpeRT) task [28], the other includes demographic questions and a survey on attitudes towards ransomware. The two framings allows us to test Hypotheses 1 and 2 while data on risk attitudes allows us to explore Propositions 1 and 3.

4.1 Results

Let us look first at the average amount invested in prevention and recovery. Table 3 reports the mean and median amount of tokens participants invested in prevention and recovery. Figure 4 presents a box-plot of spending in prevention and recovery. The conditional R box controls for subjects who fully prevent (and so the recovery decision is irrelevant). We find that in the gain treatment

Table 2. Comparison of two framings - gain and loss.

	Prevention stage	Recovery stage
Gain	"... If you are not attacked, you will not lose access to the file and so it is **still worth 100 Tokens.**"	"... If the selected ball is green, your files are recovered. You **regain the 100 Tokens**."
Loss	"... If you are attacked, you will lose access to the file saved in stage 1 and so it becomes worthless. You therefore, **lose the 100 Tokens**."	"... If the selected ball is brown, you do not recover your file. The **100 Tokens are lost**."

investment in prevention is significantly higher than investment in recovery ($p < 0.05$, two-sided Wilcoxon matched pairs signed-rank test with individual average as unit observations). By contrast, in the loss treatment there is no significant difference ($p > 0.1$). This leads to our first experimental result.

Result 1. Participants invested more in prevention than recovery in the gain treatment. There is no significant difference between investment in prevention and recovery in the loss treatment.

Table 3. Investment in Prevention (I) and Recovery (R) by treatments. Mean investments in I and R measure the average of participants' investment in prevention and recovery. Median is derived from the median of average investments.

		Prevention (I)	Recovery (R)
Gain	Mean	29.2	22.7
	Median	(28.6)	(22.4)
Loss	Mean	28.2	26.0
	Median	(31.1)	(25.4)

We next consider Hypotheses 1 and 2. Given that the observations of prevention and recovery are not independent, to assess the gain-loss treatment effect, we take the average of participants investment in back up and recover and run a bootstrap linear regression with robust standard errors. The regression results are reported in Table 4. The effect of treatment on prevention is statistically insignificant, whereas the effect on recovery is marginally lower in the gain treatment ($p < 0.1$). This result provides some marginal support for Hypothesis 1. There is no support for Hypothesis 2.

Result 2. The amount invested in prevention is the same in the gain and loss treatments. Investment in recovery is marginally higher in the loss treatment than in the gain treatment.

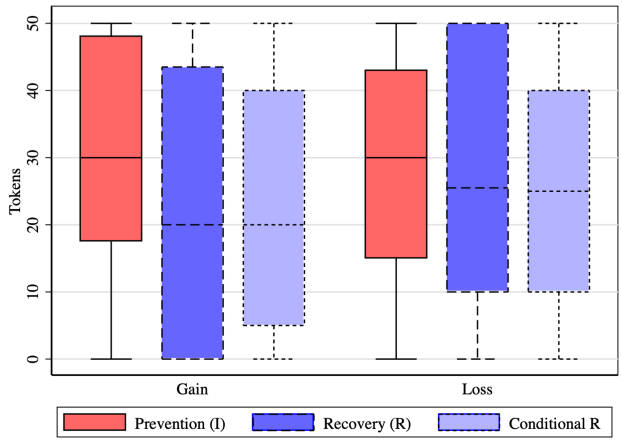

Fig. 4. Box plot of average numbers of tokens invested in prevention (I), and recovery (R and RCon).

Table 4. Bootstrap regression on back up and recovery investments by participants. The unit observation is the average investment in recovery (R) and investment (I). Independent variables include treatments framings and individual characteristics, ethical/financial risk taking attitudes, gender, age, first language English and average total distance traveled in TSP games. Robust standard errors in parentheses. *** p<0.01, ** p<0.05, * p<0.1.

	(1)	(2)
VARIABLES	Recovery	Prevention
Gain frame	-6.059*	-0.742
	(3.182)	(4.018)
Ethical-risk taking	1.036	-0.296
	(3.203)	(2.520)
Financial-risk taking	-2.758	-3.827*
	(2.403)	(2.214)
Male	-2.523	1.412
	(3.757)	(4.653)
Age	-0.120	-0.0726
	(0.688)	(0.639)
English	-4.348	-3.924
	(3.697)	(3.799)
Total Distance	0.0273	0.0235
	(0.0873)	(0.104)
Constant	28.02	33.77
	(38.13)	(42.87)
Observations	76	76
R-squared	0.071	0.057

The average data (see Table 3) suggests that spending on prevention and recovery is 'in the middle' of the permissible range. At the individual level, however, we see clustering at the extreme combinations $(I, R) = (0, 0); (0, 50); (50, 0)$ and $(50, 50)$. For instance, Around 13% of subjects invest nothing in prevention (11% in the gain treatment and 15% in the loss treatment) while 23% invest the maximum amount (24% and 22%). Around 22% of subjects invest nothing in recovery (29% and 16%) while 24% invest the maximum amount(20% and 27%).

To study individual behavior in more detail we classify behaviour into 5 categories detailed in Table 5. The categories are (1) prevention lover, who invests in prevention not recovery, (2) recovery lover, who invests in recovery not prevention, (3) payment lover, who invests in both prevention and recovery, (4) payment averse, who invests in neither prevention nor recovery, (5) intermediate, who invests 'in the middle' for both prevention and recovery.

Table 5. Classification of strategies.

	$I - R$	$I + R$
Prevention lover	$[25, 50]$	$[25, 75]$
Recovery lover	$[-50, -25]$	$[25, 75]$
Payment lover	$(-25, 25)$	$[75, 100]$
Payment averse	$(-25, 25)$	$[0, 25]$
Intermediate	$(-25, 25)$	$(25, 75)$

Figure 5 provides a scatter plot of the frequency of each combination of I and R. We can see large clusters at payment lover, $I = R = 50$ and prevention lover, $I = 50, R = 0$. There are also smaller clusters at no payment averse, $I = 0, R = 0$, and recovery lover, $I = 0, R = 50$. A lot of subjects also fit in the intermediate category. Overall, therefore, there is considerable heterogeneity in how subjects behaved in the task. One interesting thing to observe is the near symmetric split around $I = R$ meaning that a large proportion of subjects invest more in recovery than investment. This leads to our next result.

Result 3. There is large heterogeneity in individual behaviour with clustering at the extremes of full prevention, no prevention or recovery, and maximum recovery.

We finish the analysis by looking at how behaviour correlates with risk attitudes. At the end of the experiment, we used the Domain Specific Risk Taking Attitude Scale to elicit individual risk preferences. For the analysis we focus on risk attitude in the financial domain. Subjects are defined as extreme risk averse if their financial risk taking score is in the lower 25 percentile of all subjects and extreme risk seeking if the score is in the upper 25 percentile. The average investments in prevention and recovery is plotted in figure 6. There is marginal evidence that risk averse individuals invest more in prevention (see also Table 4).

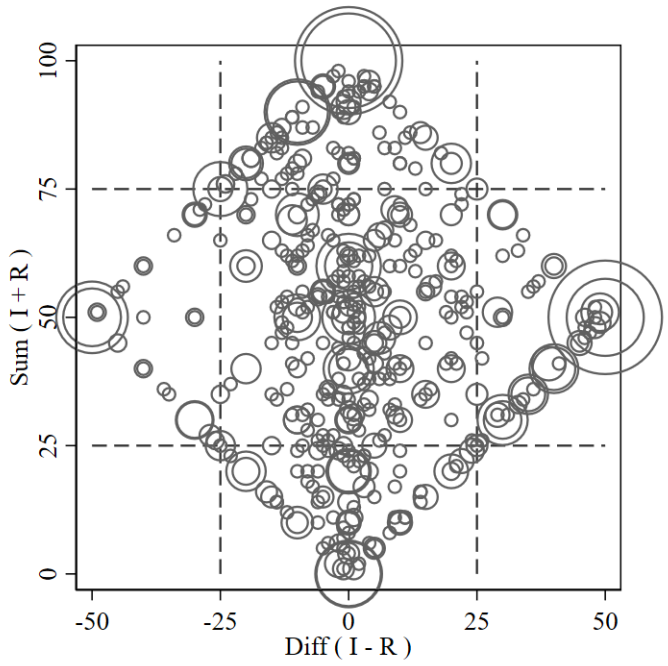

Fig. 5. Scatter plot of aggregate choice distributions by difference between spending on prevention and recovery versus total amount spent on prevention and recovery.

There is also marginal evidence that the framing effect is larger for risk averse individuals than risk seeking individuals.

Result 4. There is marginal evidence that risk averse individuals invest more in prevention and are more influenced by framing than risk seeking individuals.

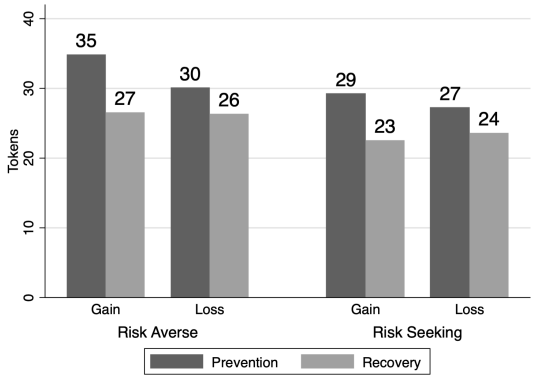

Fig. 6. Choice of back up and recovery by risk attitudes under gain and loss framing.

5 Conclusion

In this paper we have introduced a simple game to explore the strategic trade-off between prevention of a cyber-attack and recovery from a cyber-attack. This game can be useful in examining situations such as ransomware in which an individual can prevent attack (e.g. through off-line back-ups) or attempt to recover from attack (e.g. by paying the ransom). We show that the optimal strategy depends on risk attitudes. Our findings reinforce, therefore, the need to model risk attitudes in security games [30]. We show that a risk averse individual will invest in prevention while a risk loving individual will invest in recovery. We know in the field that many individuals do pay ransom demands and so it is interesting to explore the factors that influence this decision.

A particular factor we wished to explore is whether behavior is influenced by framing. This is an important issue, in practical terms, for guiding the design of cyber-awareness campaigns [31, 32]. We hypothesized that in a loss frame individuals would be more risk loving and so invest in recovery. Conversely, in a gain frame they would be more risk averse and so invest in prevention. This is consistent with a reflection effect [13]. We ran an experiment to test this prediction. While the framing effect we observed was in the predicted direction it was small in magnitude. In short, framing seemed to make relatively little

difference. This may be because the difference in our frames was 'too subtle' or it could be that framing is difficult to manipulate in a cyber-security context.

In practical terms we hoped that a gain frame could increase investment in prevention. The observed effect was marginal at best. This means that individuals were relatively risk seeking. In particular, a large proportion of subjects invested more in recovery than prevention. While this result might be disappointing from a policy perspective it is arguably a reflection of the reality on the ground. Indeed the risk seeking we observed in our experiment is above that observed in standard lab experiments with a non cyber-security frame. This may suggest individuals are more willing to take risks in cyber-space than other domains. This is something we plan to test in future work by directly comparing a cyber and neutral frame. One can also consider other settings with a prevention and recovery dichotomy such as in health care (prevention versus treatment of illness) and security (preventing theft versus recovering losses). It would also be of interest to see how risk taking in our experiment compares with standardized measures of risk taking [33]

More generally, we believe that the prevention and recovery game, and our experimental design, offer a novel approach to explore cyber behavior. One possible extension is to embed the prevention stage within a network security game in which the probability of attack depends on the actions of other users. Previous work has modelled (what we have called the prevention stage) as a weakest-link, best-shot, weakest-target and total effort games [3, 4, 34]. This adds strategic uncertainty in that an individual also needs to take account of the actions of others. Framing may have interesting influences on that strategic uncertainty in changing the focal expectation [35, 36].

References

1. Bada M, Sasse AM, Nurse JR. Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672. 2019 Jan 9.
2. Arora A, Hall D, Pinto CA, Ramsey D, Telang R. An ounce of prevention vs. a pound of cure: How can we measure the value of IT security solutions?. Lawrence Berkeley National Lab.(LBNL), Berkeley, CA (United States); 2004 Jan 12.
3. Grossklags J, Christin N, Chuang J. Predicted and Observed User Behavior in the Weakest-link Security Game. In UPSEC 2008 Apr.
4. Grossklags J, Christin N, Chuang J. Secure or insure?: a game-theoretic analysis of information security games. In Proceedings of the 17th international conference on World Wide Web; 2008 Apr 21 (pp. 209-218).
5. Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment 2015 Jul 9 (pp. 3-24). Springer, Cham.
6. Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science. 2019 Dec;8(1):2.
7. Richardson R, North MM. Ransomware: Evolution, mitigation and prevention. International Management Review. 2017;13(1):10.

8. Cartwright A, Cartwright E. Ransomware and Reputation. Games. 2019 Jun;10(2):26.
9. Laszka A, Farhang S, Grossklags J. On the economics of ransomware. InInternational Conference on Decision and Game Theory for Security 2017 Oct 23 (pp. 397-417). Springer, Cham.
10. August T, Dao D, Niculescu MF. Economics of Ransomware Attacks. Available at SSRN. 2019 Mar 12.
11. Janofsky A. HBO, Uber Incidents Shed Light on Ransoms Without Ransomware. Wall Street Journal. 2017 Dec 11.
12. Cook, S. 2017-2018 Ransomware statistics and facts. 2018 urlhttps://www.comparitech.com/antivirus/ransomware-statistics/
13. Kahneman D, Tversky A. Prospect Theory: An Analysis of Decision under Risk. Econometrica. 1979 Mar;47(2):263-92.
14. Tversky A, Kahneman D. The framing of decisions and the psychology of choice. Science. 1981 Jan 30;211(4481):453-8.
15. Tversky A, Kahneman D. Rational choice and the framing of decisions. In Multiple Criteria Decision Making and Risk Analysis Using Microcomputers 1989 (pp. 81-126). Springer, Berlin, Heidelberg.
16. Homonoff TA. Can small incentives have large effects? The impact of taxes versus bonuses on disposable bag use. American Economic Journal: Economic Policy. 2018 Nov;10(4):177-210.
17. Field E. Educational debt burden and career choice: Evidence from a financial aid experiment at NYU Law School. American Economic Journal: Applied Economics. 2009 Jan;1(1):1-21.
18. Fryer Jr RG, Levitt SD, List J, Sadoff S. Enhancing the efficacy of teacher incentives through loss aversion: A field experiment. National Bureau of Economic Research; 2012 Jul 19.
19. Hernandez-Castro J, Cartwright E, Stepanova A. Economic Analysis of Ransomware. arXiv 2017. arXiv preprint arXiv:1703.06660.
20. Pfleeger SL, Caputo DD. Leveraging behavioral science to mitigate cyber security risk. Computers & security. 2012 Jun 1;31(4):597-611.
21. Baddeley, M. (2011). Information security: Lessons from behavioural economics. Workshop on the Economics of Information Security.
22. Rosoff H, Cui J, John RS. Heuristics and biases in cyber security dilemmas. Environment Systems and Decisions. 2013 Dec 1;33(4):517-29.
23. Harrington S, Anderson C, Agarwal R. Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. ICIS 2006 Proceedings. 2006 Dec 31:93.
24. Ravindran SK, Nah FF, Cheng MX. Effect of Probable and Guaranteed Monetary Value Gains and Losses on Cybersecurity Behavior of Users. MWAIS 2018 Proceedings. 2018:1-5.
25. Smith SN, Nah FF, Cheng M, Ravindran SK. The impact of monetary value gains and losses on cybersecurity behavior. In Proceedings of the Midwest Association for Information Systems Conference, Springfield, Illinois 2017.
26. Starmer C. Developments in non-expected utility theory: The hunt for a descriptive theory of choice under risk. Journal of economic literature. 2000 Jun;38(2):332-82.
27. O'Donoghue T, Somerville J. Modeling risk aversion in economics. Journal of Economic Perspectives. 2018 May;32(2):91-114.
28. Weber EU, Blais AR, Betz NE. A domain specific risk attitude scale: Measuring risk perceptions and risk behaviors. Journal of behavioral decision making. 2002 Oct;15(4):263-90.

29. Fischbacher U. z-Tree: Zurich toolbox for ready-made economic experiments. Experimental economics. 2007 Jun 1;10(2):171-8.
30. Johnson B, Bhme R, Grossklags J. Security games with market insurance. InInternational Conference on Decision and Game Theory for Security; 2011 Nov 14 (pp. 117-130). Springer, Berlin, Heidelberg.
31. Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS quarterly. 2010 Sep 1:549-66.
32. Bada M, Sasse AM, Nurse JR. Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672. 2019 Jan 9.
33. Kharlamov A, Jaiswal A, Parry G, Pogrebna G. A cyber domainspecific risk attitudes scale to address security issues in the digital space.
34. Grossklags J, Christin N, Chuang J. Security and insurance management in networks with heterogeneous agents. Proceedings of the 9th ACM Conference on Electronic Commerce; 2008 Jul 8;8:160-9.
35. Dufwenberg M, Gchter S, Hennig-Schmidt H. The framing of games and the psychology of play. Games and Economic Behavior. 2011 Nov 1;73(2):459-78.
36. Poulsen O, Saral KJ. Coordination and focality under gainloss framing: Experimental evidence. Economics Letters. 2018 Mar 1;164:75-8.