Table of Contents

Go Back

# Choice Under Risk In IT-Environments According To Cumulative Prospect Theory

**Agata Sawicka**
**Jose J Gonzalez**
Faculty of Engineering and Science
Dept. of Information & Communication Technology
Agder University College
NO-4876 Grimstad, Norway
Phone: +47 37 25 33 58
Fax: +47 37 25 30 01
Email: agata.sawicka@hia.no

*How do people choose between action options in risky environments and why do they so often opt for not following prescribed security measures? In our research we focus on human factors in modern work environments that rely on information technology (IT). To effectively counteract noncompliance, a good understanding of its origins is indispensable. In this paper, we analyze what contributions cumulative prospect theory (CPT) – one of the currently most prominent theories of choice under risk – can make to our understanding of human behavior in IT-security systems. We present a system dynamics model of laboratory experiment to collect data on IT-security observance. Subject's actions are modeled in accordance with CPT. Using the model, we discuss the behavior patterns implied by CPT, providing some tentative policy recommendations and outlining ways in which the basic model may be extended to provide a viable tool for IT-security policy design.*

## Introduction

There is a growing consensus among IT-security experts and researchers that while security technology is dependable, people are not (Schneier 2000, Economist.com 2002, Anderson 2001). Knowledge on how to deal with the "people problem" is at large implicit and resides with experienced IT-security practitioners. Parts of the knowledge and expertise are shared as reports on practices successfully increasing people's observance of security measures (Callene 2000, Smith 2001, Tuesday 2001, Voss 2001). But comprehensive guidelines on how to elicit and sustain desired behavior patterns are still missing. To develop such guidelines a good understanding of why undesired behavior patterns occur is indispensable. In this paper, we analyze what contributions cumulative prospect theory (Tversky and Kahneman 2000, see also Kahneman and Tversky 2000) – one of the currently most prominent theories of choice under risk – can make to our understanding of human behavior in IT-security systems.

In Figure 1 we sketch a typical behavior observed in risky environments.

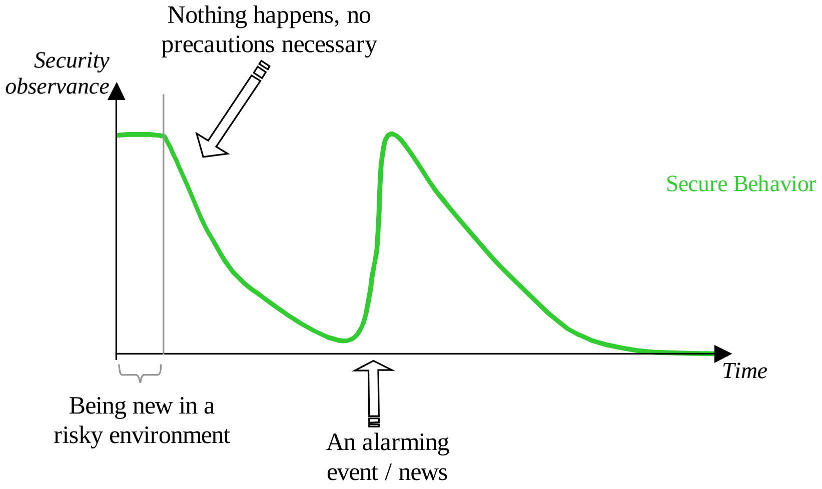

Nothing happens, no precautions necessary
Security observance
Secure Behavior
Time
Being new in a risky environment
An alarming event / news

**Figure 1 Behavior pattern typically observed in risky environments.**

Usually, two factors are indicated as the main causes of dynamic changes in security observance: (1) increasing attention to throughput goals at the expense of security objectives and (2) fading estimates of risk exposure. Sole identification of these problematic trends seems insufficient to develop policies that would effectively counteract the security observance erosion. For this, a good understanding of why the shifts in attention and risk estimates occur is indispensable. To gain such insight it is necessary to turn to relevant socio-psychological theories.

Various theories about people's perception of probabilities and risks have been cited to explain the troublesome patterns in variety of risky environments (see e.g. Kahneman and Tversky 2000, Hogarth 1987, Dörner 1996, Reason 1990, Gonzalez 1995, Hastie and Dawes 2001). Despite the urgency of the problem, analysis of security observance in IT-work environments has been however limited. With our research we want to foster the current understanding of human behavior in these environments as well as contribute to the general knowledge about mechanisms likely to drive human behavior in risky environments. System dynamics is our main research method: Drawing on psychological theories, we develop system dynamics models of human behavior in IT-based environments. Using the models we explore what behavioral patterns are implied by the various theories. Simulation results are compared with data gathered through various field studies as well as laboratory experiments we conduct. Coupling formal modeling and experimental methods enhances our ability to explore research hypotheses and to evaluate descriptive adequacy and coherence of theories under investigation.[1]

In a parallel paper, we outline several theories cited as possible explanations for the phenomenon of security observance erosion. Pointing out limitations of these theories, we discuss how instrumental conditioning may plausibly account for the phenomenon (Gonzalez and Sawicka 2003b). In this paper, we narrow our focus to examine how people choose between action options in risky environments. From the plethora of theories on the subject matter, we decided to analyze in detail cumulative prospect theory, developed by Kahneman

[1] On application of formal modeling to socio-psychological theories see Simon 1982. On different use of simulation in the study of complex decision making see Brehmer, Laplat et al. 1991.

and Tversky (Tversky and Kahneman 2000, see also Kahneman and Tversky 2000). This theory has been widely acknowledged as most robust and comprehensive among the current descriptive theories of choice under risk. Using system dynamics we explore which contributions cumulative prospect theory can make to the explanation of the behavioral dynamics in IT-based work environments.

A system dynamics model simulating subject's behavior in laboratory environment that resembles a typical IT-based work environment is presented. The simulated subject is assumed to act in accordance with cumulative prospect theory (CPT). We begin our discussion with a brief presentation of CPT – its origins and main postulates. After describing our laboratory environment, we outline the system dynamics model and discuss the behavior of the simulated subject. Next, some tentative policy recommendations are drawn. As it turns out, CPT[2] is likely to deliver quite robust description of choices in a short run, but it is not likely to account accurately for behavior patterns observed over longer time periods. At the end, we indicate how the model could be revised to improve its descriptive adequacy. In particular, our understanding of mechanisms governing the security observance may benefit from embedding the basic choice model in the more general model of people's behavior in IT-work environment that we developed based on instrumental conditioning theory (see Gonzalez 2002, Gonzalez and Sawicka 2002, and also Gonzalez and Sawicka 2003b). In that way, results of the current investigation further not only our search for mechanisms governing security observance in IT-work environments, but also deliver insights into how CPT[2] could be augmented to provide a robust description of choice under risk also in dynamic settings.

## Normative and descriptive theory of choice under risk

Decisions in risky environments may be described in terms of two attributes: the likely outcomes and the probability of their occurrence. According to the expected utility theory (EUT), each agent has a unique utility function $u(x_i)$ which assigns utility values to all possible outcomes $x_i$ for $i = 1, 2, \ldots, j$. The sum of utilities of all decision's outcomes, weighted by their respective probabilities $p_i$ for $i = 1, 2, \ldots, j$, returns the decision's expected utility. When choosing among a number of decisions, a rational agent follows by definition the principle of maximum expected utility and chooses the option of the highest expected utility. (von Neumann and Morgenstern 1944)

Many studies have, however, shown that people do not make their choices according to EUT[2] (see e.g. Kahneman and Tversky 2000, Camerer and Ho 1994, Wu and Gonzalez 1996, Bleichrodt and Pinto 2000). Several "nonexpected utility theories" were developed. The majority of these theories claim that individuals not only transform outcomes $x_i$, but also the associated probabilities $p_i$. CPT (Tversky and Kahneman 2000, see also Kahneman and Tversky 2000) is maybe the best tested among the alternative theories. CPT differs from EUT[2] in three ways:

1. First, it assumes that people do not evaluate possible outcomes as such, but rather "code" them as gains and losses relative to some reference point. It is these relative gains and losses that are transformed. To distinguish the transformation function from the utility function used in EUT, Tversky and Kahneman call the function that transforms gains and losses "value function".
2. Second, individuals are assumed to be loss averse. This means that losses loom larger than gains of corresponding absolute magnitude. Thus, the outcome transformation

[2] Appendix 1 contains a listing of acronyms used in the text.

function is no longer as smooth and concave as in EUT. Rather, it is supposed to have a kink at the reference point, being concave for gains and convex (and relatively steeper due to the loss aversion) for losses.[3]

3. Third, individuals are assumed to use the so-called capacities instead of objective probabilities in their evaluation of risky prospects. The objective probability values are internally transformed using some ω(p) function. As a result, small probabilities are overestimated, while moderate and high probabilities are underestimated.[4] The capacities are used to determine decision weights assigned to each outcome in the prospect valuation formula.

Under CPT, a prospect $P(x_n, p_n; x_{n-1}, p_{n-1}; ...; x_k, p_k; ...; x_{j-1}, p_{j-1}; x_j, p_j)$, where possible outcomes are sorted so that $x_n \geq x_{n-1} \geq ... \geq x_k \geq ... \geq x_{j-1} \geq x_j$, is evaluated as follows (Tversky and Kahneman 2000, p. 47):

$$V(P) = V(P^+) + V(P^-) \qquad (1)$$

where $V(P^+)$ and $V(P^-)$ indicate the value of gains and losses respectively and are defined as:

$$V(P^+) = \sum_{i=0}^{n} \pi_i^+ v(x_i) \text{ and } V(P^-) = \sum_{i=-m}^{0} \pi_i^- v(x_i) \qquad (2)$$

Although Tversky and Kahneman stress that CPT is a descriptive theory and most insight is delivered from qualitative analysis of data, they do propose some parametric forms for the transformation functions (Tversky and Kahneman 2000, cf. p. 59). For the value function, v(x), they suggest a two-part power function defined as (Tversky and Kahneman 2000, p. 57):

$$v(x) = \begin{cases} x^{\alpha} & \text{if } x \geq 0 \\ -\lambda(-x)^{\beta} & \text{if } x < 0 \end{cases} \qquad (3)$$

A distinct feature of the value function suggested in equation (3) is, of course, that it is defined separately for gains and losses. A power form is used both for gains and losses. The exponents α and β indicate to which degree the individual is risk-averse and risk-seeking for gains and losses respectively. The λ parameter accounts for the individual's loss aversion: As the exponents α and β have been shown to be approximately equal, it is the λ parameter that accounts for the fact that losses loom larger than gains equivalent in absolute terms.

Decision weights $\pi_i$ are defined using cumulative functionals of transformed probabilities (Tversky and Kahneman 2000, p.48):

$$\pi_n^+ = \omega^+(p_n) \text{ , } \pi_{-m}^- = \omega^-(p_{-m}),$$

$$\pi_i^+ = \omega^+(p_i + ... + p_n) - \omega^+(p_{i+1} + ... + p_n), \quad 0 \leq i \leq n-1 \qquad (4)$$

$$\pi_j^- = \omega^-(p_{-m} + ... + p_j) - \omega^-(p_{-m} + ... + p_{j-1}), \quad 1-m \geq j \geq 0 \qquad (5)$$

[3] See Figure 3.1 in Appendix 2: Transformation of outcomes: Value function.

[4] See Figure 3.2 in Appendix 2: Transformation of probabilities: Decision weight function.

Tversky and Kahneman (2000, p. 58) suggest the following formula for the probability transformation function ω(p) function:

$$\omega^{+}(p)=\frac{p^{\gamma}}{(p^{\gamma}+(1-p)^{\gamma})^{1/\gamma}} \text{ for probabilities associated with gains} \qquad (6)$$

$$\omega^{-}(p)=\frac{p^{\delta}}{(p^{\delta}+(1-p)^{\delta})^{1/\delta}} \text{ for probabilities associated with losses.} \qquad (7)$$

The parametrical form given in equations (6) and (7) for the transformation of probabilities ω(p) produces an inverse S-shape function. The convex and concave regions of the function describe well with the empirical findings indicating that people under- and overestimate probabilities. The rationale behind the decision weights for gains $\pi^{+}$ is that each gain outcome is weighted by a difference between the capacity of obtaining at least this outcome and the capacity of obtaining a strictly better outcome. Similarly, each loss outcome is weighted by $\pi^{-}$: a difference between the capacity of obtaining this outcome or worse and the capacity of obtaining a strictly worse outcome (Tversky and Kahneman 2000, cf. p. 48).

As with the expected utility model, the cumulative prospect model has been mainly tested in the economical domain. Fitting the parametric forms into experimental data, Tversky and Kahneman (2000) obtain the following estimates for parameters: α=β=0.88, λ=2.25, γ=0.61, δ=0.69. Many researchers confirmed that human preferences are in agreement with the CPT's postulates (Camerer and Ho 1994,Wu and Gonzalez 1996, Prelec 2000) and that similar parameter estimates are derived from various data sets. Recently, the model has also been shown to hold in the context of health decision-making (Bleichrodt and Pinto 2000, Abdellaoui 2000).

The growing body of evidence increases confidence that the cumulative prospect model indeed provides an appropriate description of how people choose among risky prospects. It should, however, be noted that thus far the model has been tested predominantly for static settings. Subjects were asked to indicate their preferences for a number of explicitly stated risky prospects. The choices made typically did not impact each other in any particular way. This type of problems imitates well discrete decision making such as one-time purchase of insurance policy, but fails to approximate continuous and implicit choices under risk such as applying security measures in everyday work. Indeed, the bulk of risky choices is recurrent and often not implicit. For CPT to be accepted as truly general descriptive model of human choice under risk, the theory needs to be also tested in such settings. Before analyzing the behavior patterns that CPT implies in dynamic settings, we first describe briefly the assumed IT-based work environment and outline the model structure.

## Testing cumulative prospect theory in a dynamic environment

As indicated in the introductory section, our approach couples a formal modeling method of system dynamics with experimental methods (see *Introduction*). By developing simulation models of laboratory environment and modeling subject's actions according to specific psychological theories we are able to examine what behavior patterns the theories imply. Our focus in this paper is on CPT and what security observance patterns this theory implies in context of simple IT-based work environments.

### Experimental study of security observance in IT-based work environment

To investigate security observance patterns in the IT-work environments we deploy a simple application resembling a typical IT-database system. During experimental sessions subjects use the mock-up application to enter data into the database. The stipulated goal is to enter as much records as possible. To distract subjects' attention from security issues we state that our goal is to assess overall productivity of the database application. A performance-based gratification system is implemented to enhance the production focus. Simultaneously, subjects are informed about the risk of data loss due to possible system crash or IT-attack during the experimental session. A backup mechanism that transfers entered data into a 100% secure location is available at the subjects' discretion. Although, the backup protects completely all work against loss, it also limits potential gains: During data backup, the system is disabled and the subjects are not able to enter new records. The ultimate profit depends on how securely subjects work: The more frequently data are backed up, the less data will be entered, but also the smaller potential losses. And vice-versa: The less frequently subjects back up their work, the more data they are able to enter, but also the greater their risk exposure.

Our mock-up environment, stores not only data the subjects enter, but also all their actions. The logs indicate when subjects prefer particular action alternative. When data backup is performed a subject prefers a safer option. Choice of data entry indicates preference of the riskier prospect. Structure of the choice problem is similar to choice questions typically used in elicitation of preferences between risky prospects (see, for example, references to experimental research on CPT given in the *Normative and descriptive theory of choice under risk* section). As it was presented in the literature, each choice situation may be framed in a number of ways (see, for example, Kahneman and Tversky 2000 or Hastie and Dawes 2001). There are many ways in which the choice may be framed in the case of our experimental tasks. Analysis of all possibilities is beyond the scope of this paper. Here, we assume that subjects frame the action alternatives in terms of losses as follows:

Frame 1: *Assuming,* p *probability of data loss event occurring in the next time unit, which do you prefer:*

*(a) Certain time loss to back up currently unprotected data*

*(b)* p *chance of time loss to reenter currently unprotected data*

Most of the subjects participating in recently conducted experiments perceived the problem in this way.[5] Assuming that average subject follows CPT and frames the problem according to *Frame 1*, what sort of compliance pattern we would expect to observe? To explore the

[5] Initial experiments have been carried out in October-November 2002 and March 2003 at Agder University College, Norway. Analyses of gathered data are currently under way; preliminary results were presented at the 5th International Conference on Cognitive Modeling (Sawicka 2003a).

question we develop a system dynamics model of a subject acting in the described IT-work environment in accordance with CPT.

## System dynamics model of CPT-subject in IT-environment

Figure 2 contains a conceptual outline of the system dynamics model of a CPT-subject working in an assigned IT-environment. What is important to keep in mind is that in the model we deal with two types of variables: independent and dependent variables. Independent variables are properties that characterize the IT-environment used in experiments. Backup initialization time, record backup time, risk estimates, test session duration and data loss event (number and time of occurrence) are independent variables in our case. These variables are controlled by the experimenter. Various configurations may be defined to test hypotheses about impact the independent variables may have on human behavior.[6]

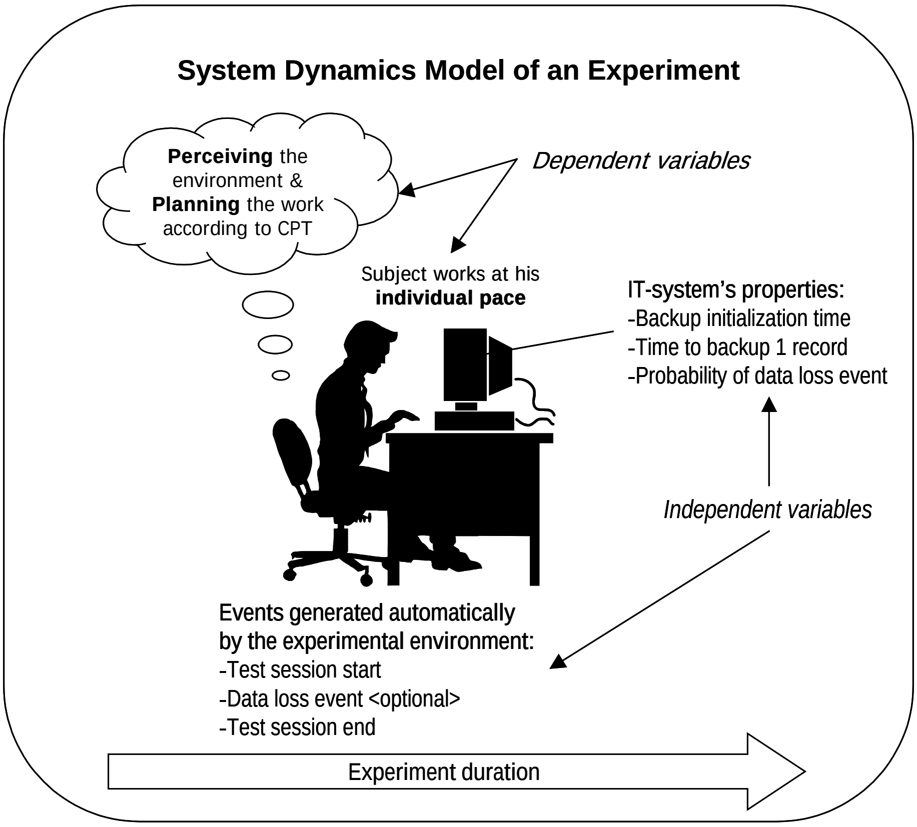

System Dynamics Model of an Experiment
Perceiving the environment & Planning the work according to CPT
Dependent variables
Subject works at his individual pace
IT-system's properties:
-Backup initialization time
-Time to backup 1 record
-Probability of data loss event
Independent variables
Events generated automatically by the experimental environment:
-Test session start
-Data loss event <optional>
-Test session end
Experiment duration

**Figure 2 Simulating subject actions during experimental sessions: A conceptual outline of the system dynamics model**

Dependent variables are beyond experimenter's control. They represent subject-specific parameters, defining subject's abilities, perceptions and decision rules. Here, we assume that the simulated subject acts in accordance with CPT (see the *Normative and descriptive theory of choice under risk* section).

When presenting the system dynamics model we will indicate and discuss all the independent and dependent variables. In our model snapshots, we will mark in blue all the dependent

[6] See the *Subject's behavior according to cumulative prospect theory* section.

variables, and in red all the independent variables. All other variables will be marked in black.

We begin review of the system dynamics model[7] by outlining the structure responsible for simulating the basic course of events during experimental session. The experimental task structure is presented in Figure 3: Entered records are accumulated in *Working database*. All data stored in this database may be lost in case of a data loss event. *Secure database* contains backed up, protected data. At the outset, both levels contain 0 records. Three rates – *Record Entry Rate*, *Backup Rate* and *Data Loss Rate* – define all possible data flows. Data are entered at constant *Record Entry Rate*:

*Record entry rate = IF (Data loss event DLE = 0, IF (Run backup, 0, Normal entry rate),0)*

Records are entered at rate *Normal Entry Rate* equal to 1 record per time step. When the subject decides to back up data, the *Run Backup* switch activates *Backup Rate* and disables *Record Entry Rate* (no data can be entered during backup). In such case, data stored in *Working Database* are transferred into a completely protected *Secure Database*:

*Backup rate = IF (Data loss event DLE=0, IF (Run backup, Working database, 0), 0)*

In case of data loss event, *Data Loss Event* switch disables both *Record entry rate* and *Backup rate* (see the rates equations above) and activates *Data Loss Rate*, which deletes all data currently stored in *Working Database*:

*Data loss rate = IF (Data loss event DLE=0,0,Working database/TIMESTEP)*

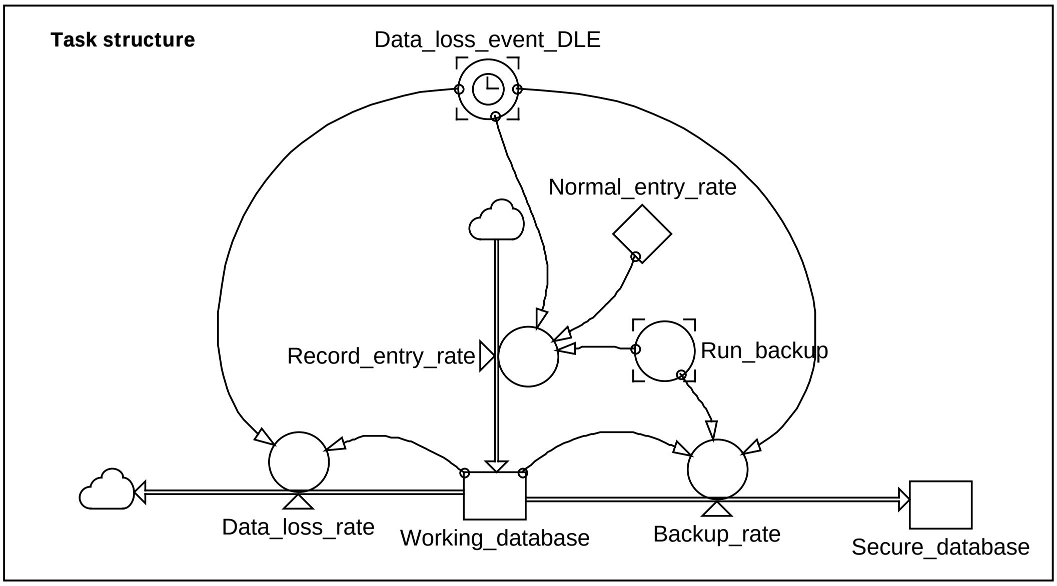


**Figure 3 Structure of the simple IT-based work environment**

As shown in Figure 3, no independent or dependent variables are directly part of the basic task structure. In that way, we obtain a laboratory environment that can facilitate various experimental setups (defined by a set of dependent variables) and remains similar for different subjects (characterized by independent variables). Although the basic task structure is independent of particular experimental setup or individual, of course, both independent and dependent variables impact the way the task is performed.

[7] In supplemental materials, the reader will find a complete listing of model equations as well as the fully documented simulation model.

Figure 4 presents the first group of independent and dependent variables. To describe how the variables impact the stream of events, we examine their impact on *Data loss rate* and *Backup rate* (see Figure 3).

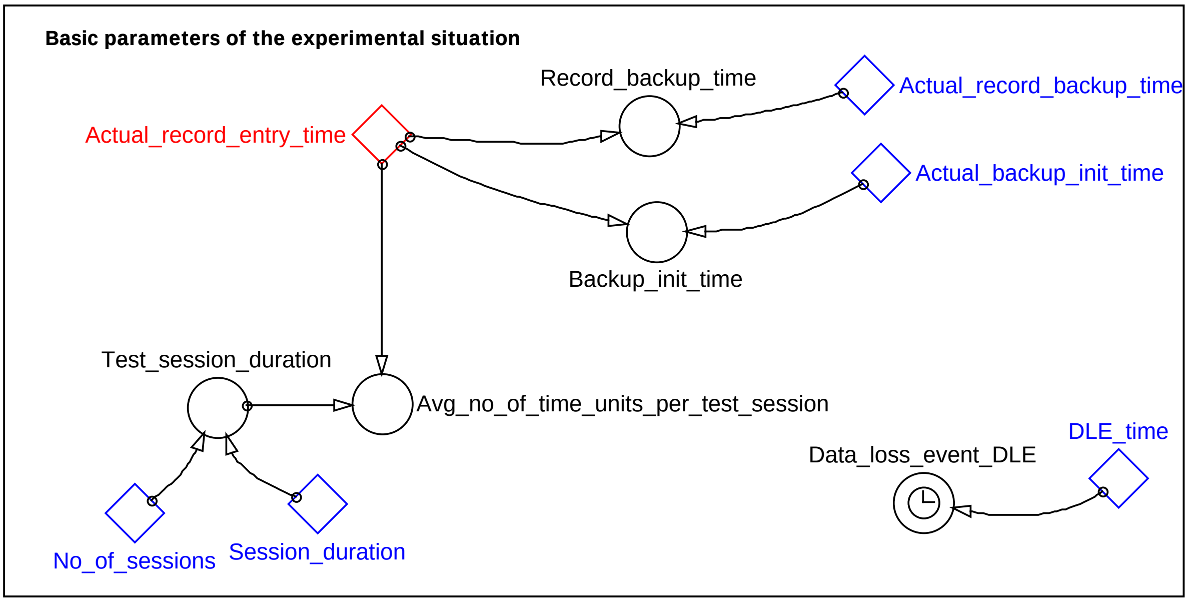


**Figure 4 Basic parameters defining the experimental situation.**

*Data loss rate* is triggered only if *Data loss event (DLE)* switch is set to TRUE. This happens when the simulation time equals *DLE time* – time of data loss event occurrence specified by the experimenter (see Figure 4):

*Data loss event DLE = IF (TIME=DLE time,1,0)*

Formulation of the data loss trigger as a simple IF condition is sufficient for our current purpose: Here, we consider only experiments with one data loss event. The model may be easily extended to account for a more general case of *n* number of data loss events during the experimental session, for example, by implementing the *Data loss event DLE* parameter as an array.

Now, let's inspect *Backup rate* (see Figure 3): Backup duration depends not only on how many records are transferred to *Secure database,* but also on how long it takes to backup one record and what is the backup initialization time.[8] The record and initialization backup times used in the actual experiment are given by *Actual record backup time* and *Actual backup init time* as fractions of minute (see Figure 4). Remember that *Normal entry rate* is assumed to be always 1 record per simulation time unit. Thus, the only case in which we could use directly the actual values of the backup parameters is when *Actual record entry rate per minute* would equal 1 record per minute. This would severely limit range of work patterns we could investigate with the model: Indeed, we could only investigate behavior of subjects who work at the specific pace, i.e. 1 record per minute. To ensure that the model gives us a desired degree of flexibility, the actual backup parameters need to be converted into fractions of the simulation time unit (*Actual record entry time,* in our case). This is done as follows:

*Record backup time = Actual record backup time / Actual record entry time*
*Backup init time = Actual backup init time / Actual record entry time*

[8] See the *Experimental study of security observance in IT-based work environment* section.

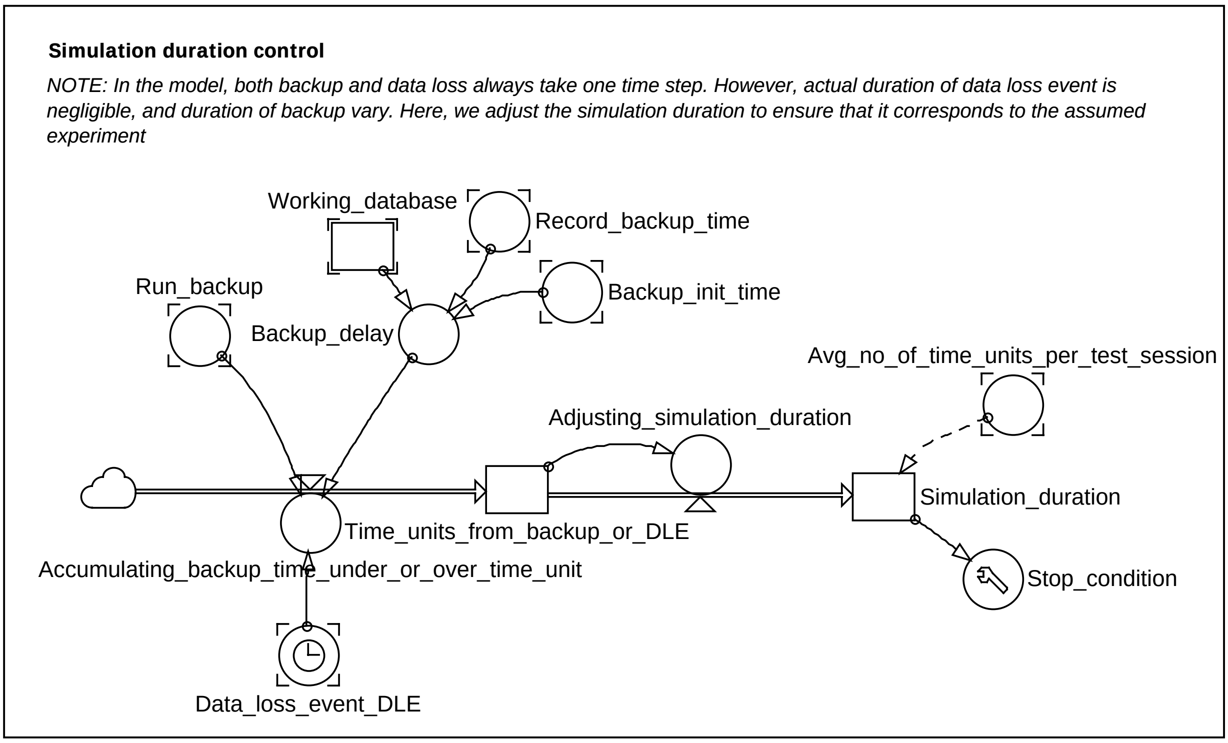
Because of the assumption that 1 record is entered during 1 time unit, we also need to derive for each simulation run the simulation duration that would correspond to the duration of the actual experiment. Two independent variables, *No. of sessions* and *Session duration*, define actual duration of the experiment (Figure 4):

*Test session duration = No of sessions*Session duration*

In the current paper we consider a 100-minute long experiment composed of four 25-minutes long work sessions. The approximate duration of the simulation is given by:

*Avg. no. of time units per test session = Test session duration / Actual record entry time*

In that way we allow for customization of the simulation to various data entry rates. One additional control mechanism is necessary to ensure that the model indeed simulates the 100-minute long experimental session: The simulation duration needs to be adjusted by the time lost or gained as a result of backup or data loss event. Both *Backup rate* and *Data loss rate* empty the *Working database* stock (see Figure 3) during one simulation time step, equal to one time unit in our case. As discussed above, the actual backup time, however, varies. The actual data loss event time, on the other hand, is negligibly small. In Figure 5, we present the control mechanism which adjusts the simulation duration so it corresponds to the 100-minute long experiment.



**Simulation duration control**

*NOTE: In the model, both backup and data loss always take one time step. However, actual duration of data loss event is negligible, and duration of backup vary. Here, we adjust the simulation duration to ensure that it corresponds to the assumed experiment*

Working_database
Record_backup_time
Backup_init_time
Run_backup
Backup_delay
Avg_no_of_time_units_per_test_session
Adjusting_simulation_duration
Simulation_duration
Time_units_from_backup_or_DLE
Accumulating_backup_time_under_or_over_time_unit
Stop_condition
Data_loss_event_DLE

**Figure 5 Mechanism controlling duration of simulation runs**

At the outset the *Time units from backup or DLE* stock is empty and *Simulation duration* corresponds to *Avg no of time units per test session*. Time units gained or lost due to backups or data loss events are accumulated at rate *Accumulating backup time under or over time unit*:

*Accumulating backup time under or over time unit = IF (Run backup, 1-Backup delay, 0) AND IF (Data loss event DLE, -1,0)*

When the *Time units from backup or DLE* stock exceeds 1 (or –1) time unit, *Simulation duration* is increased (or reduced) appropriately through the *Adjusting simulation duration* rate:

*Adjusting simulation duration = IF (Time units from backup>=1, 1,*
*IF (Time units from backup<=-1, -1, 0))*

The control variable *Stop condition* ensures that the simulation is stopped when the current simulation time reaches *Simulation duration*. When the two equal, the simulation is terminated:

*Stop condition = STOPIF (TIME>=Simulation duration)*

Figure 6 presents a mechanism generating the actual probability that a data loss event occurs at a specific point in time. Subjects participating in the experiments are given risk estimates as average number of data loss events occurring during one test session (*Avg no of DLEs per test session*). According to the continuous probability theory (see, for example, Snell 1989), *Probability of immediate loss* is described by an exponential decay function of *Time elapsed* since the last *Data loss event* or *Run backup* and the average number of data loss events per time under consideration (in our case, *Avg no. of DLEs per time unit*):

*Probability of immediate loss* =exp*(-Avg. no. of DLEs per time unit*(Time elapsed))*

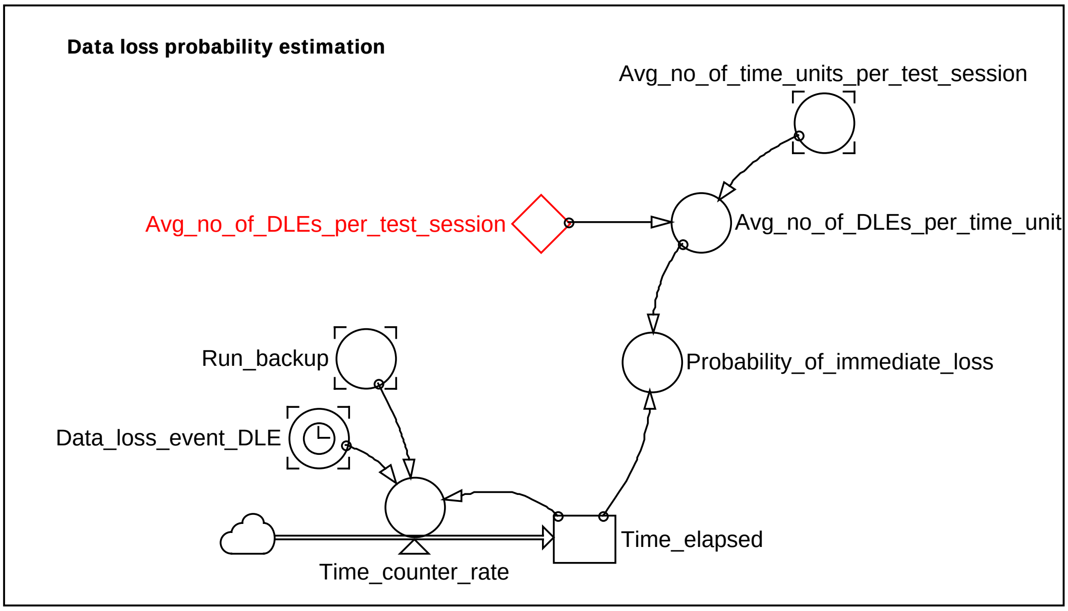

Data loss probability estimation
Avg_no_of_time_units_per_test_session
Avg_no_of_DLEs_per_test_session
Avg_no_of_DLEs_per_time_unit
Run_backup
Probability_of_immediate_loss
Data_loss_event_DLE
Time_elapsed
Time_counter_rate

**Figure 6 Structure of the decision-making mechanism.**

*Probability of immediate loss* enters the decision-making mechanism as *Perceived probability of immediate loss*. In Figure 7 we present how the probability perception is formulated.

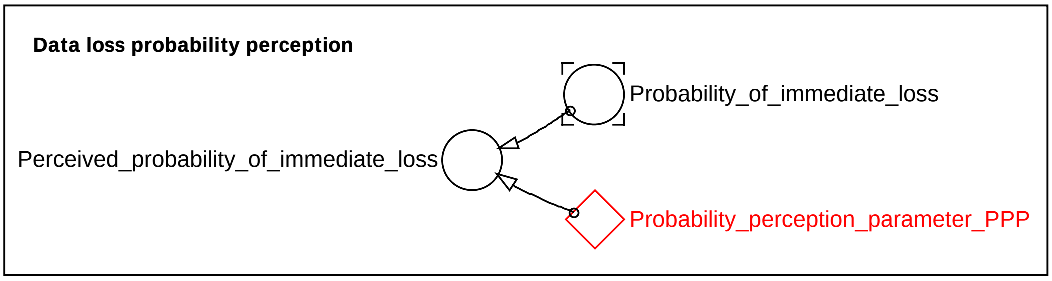

Data loss probability perception
Probability_of_immediate_loss
Perceived_probability_of_immediate_loss
Probability_perception_parameter_PPP

**Figure 7 Perceiving data loss probability.**

Following CPT, we assume that probabilities are misperceived and small probabilities are overestimated, while moderate and high probabilities are underestimated. The probability transformation function we model after Prelec (2000, p. 81): [9]

$$\omega^{+}(p) = \omega^{-}(p) = \exp\left\{-(-\ln(p))^{\eta}\right\} \tag{8}$$

Tversky and Kahneman stress that CPT is intended to provide a descriptive model of choice under risk (2000, cf. p. 59). The parametrical forms for the transformation functions they suggest should be treated as possible approximations, rather than ultimate formulas. We use Prelec's probability transformation function, since it has a simpler form and captures all main qualitative features of probability transformation postulated by CPT.[10] We set η – corresponding to *Probability Perception Parameter* in our model[11] – at 0.65, a value matching the estimate obtained by Prelec (2000) and express the perceived probability as follows:[12]

*Perceived probability of immediate loss =*
*EXP (- (-LN (Probability of  imidiate loss)^Probability perception parameter PPP ) )*

The backup batch size is estimated through a repeated comparison of values of data entry or data backup actions in the context of nearest future – the time necessary to entry one record in our case. The decision-making structure is presented in Figure 8.

[9] In his paper Prelec uses "α" to indicate the parameter (see Prelec 2000). Yet, it is common in the literature to reserve "α" for exponents of utility (or value) functions. To avoid possible confusions, we use "η" to indicate the probability transformation parameter.

[10] We refer the reader to the original paper (Prelec 2000) for a detailed argument and discussion of this issue.

[11] Throughout the analysis of the basic model behavior the Probability Transformation Parameter is assumed to be constant. We model it however as a level - reasons for this will be outlined in the final sections of the paper.

[12] In Appendix 2 we demonstrate how the formulas suggested by Prelec (2000) and Tversky and Kahneman (2000) for ω(p) transform probabilities.

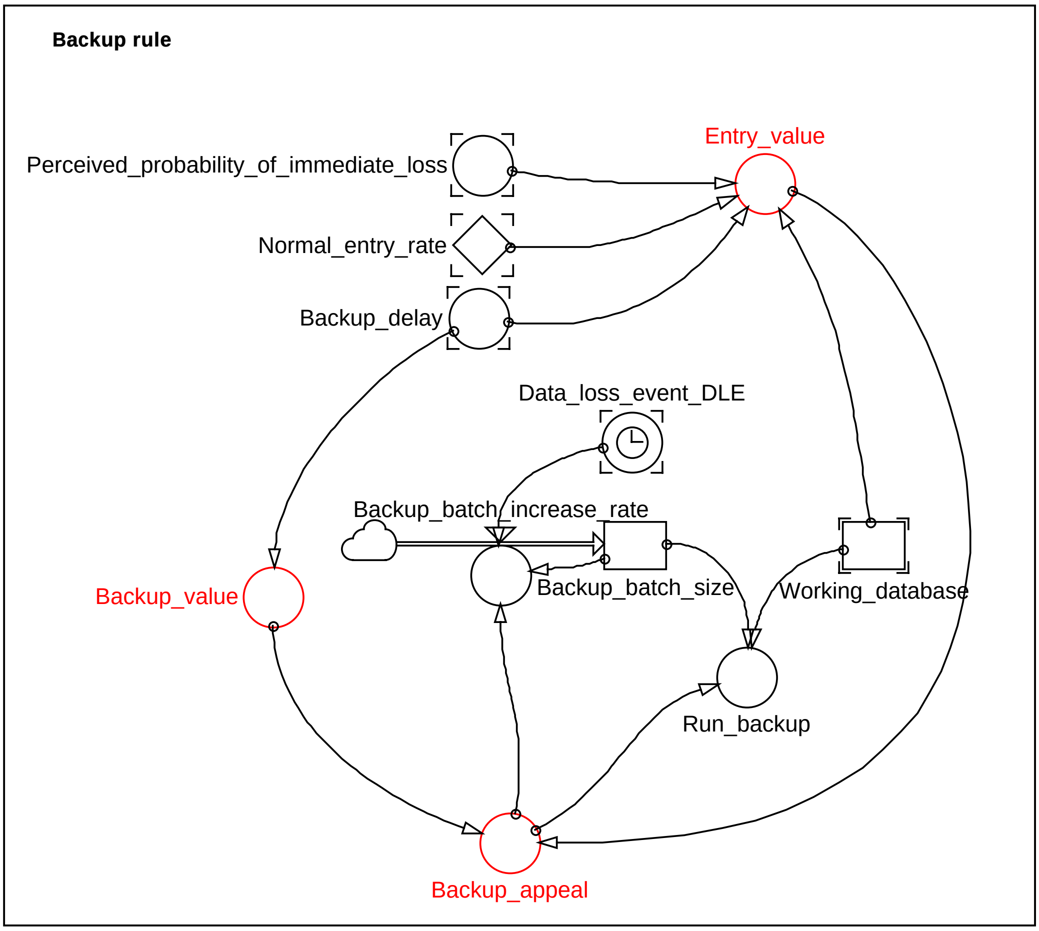


**Figure 8 Arriving at desired backup batch size.**

The way data entry and backup actions are evaluated and the decision rule for backing up data may differ among subjects. Thus, *Entry value*, *Backup value*, and *Backup appeal* are all marked as dependent variables. Here, we assume that subjects follow CPT both when evaluating the actions and when choosing between them. Accordingly, as long as the expected value of data entry action exceeds the estimated value of backup action, the subject will enter data. Once the values are equal, or the backup value exceed data entry value, the subject will back up data.

*Backup appeal = IF (Backup value>=Entry value AND Entry value<>0,1,0)*

*Backup appeal* triggers the *Run backup* switch. The structure suggests that the subject makes decision after each record input. However, its outcome, i.e. the approximate size of backup batch, should be viewed as an estimate made by the subject a priori.[13]

[13] This interpretation seems not only intuitively more plausible, but has also been confirmed by data gathered during the conducted experiments (see footnote [6]). Most subjects reported that they defined their intended backup batch size at the outset (Sawicka 2003b).

Assuming *Frame 1* (see *Experimental study of security observance in IT-based work environment*), we need only to define the value function over losses. Note, that under *Frame 1* the subject considers only the content of *Working database*; the number of records stored in *Secure database* does not impact decision about data backup. Thus, the outcome ranges the subject considers are rather narrow, accumulating over time only until backup is performed or data loss event occurs. As existing empirical work indicates that utility (or value) functions are approximately linear over narrow outcome ranges (see Wakker and Deneffe 1996), we assume a linear value function. Additionally, since both prospects under comparison are losses, the loss aversion coefficient λ from equation (4) becomes redundant. Thus, in our model we assume the following simple value function:

$$v(x) = x$$

Table 1 outlines the decision rule assumed to govern action choices of the simulated subject:

**Table 1 Evaluation of action alternatives and choice rules**

| ACTION OPTIONS: | LOSSES: |
|---|---|
| ***Data Entry*** | `- ω(p)*(R + IR*bDel)` |
| ***Data Backup*** | `- R*bDel` |

Where

**ω(*p*)** corresponds to *Perceived probability of immediate loss,*
**R** to *Working database,*
**IR** to *Normal entry rate*
**bDel** to *Backup delay*
in our model (see Figure 3, Figure 5, Figure 7)

**Decision rule** triggering *Run Backup* (see Figure 8)**:**

```
IF -ω(1-p)*(R + IR*bDel)< -R*bDel
   THEN Data Entry
   ELSE Data Backup
```

NOTE: Since the value of both prospects is expressed solely in terms of losses, the constant loss aversion coefficient λ becomes superfluous.

## Subject's behavior according to cumulative prospect theory

In this section we review basic behavior patterns implied by cumulative prospect theory. Constant simulation parameters are presented in Table 2.

**Table 2 Parameters of the basic experimental setup**

| | | Corresponding model variable[14] |
|---|---|---|
| **IT-system properties** | | |
| Backup Initialization Time | 42 sec. | *Actual backup init time* |
| Record backup time | 3 sec. | *Actual record backup time* |
| **IT-system environment** | | |
| Experiment duration | 100 min. | *Simulation duration* |
| Less risky | 1 DLE per test session | *Avg. no. of DLEs per test session* |
| More risky | 0,5 DLE per test session | *Avg. no. of DLEs per test session* |
| **Subject's working pace** | | |
| Normal working pace | 1 record/min. | *Actual record entry time* |
| Slower working pace | 0,5 record/min. | *Actual record entry time* |

Under CPT, two attributes – the value of potential outcomes and their weights derived from internal transformation of objective probabilities – impact valuation of a risky prospect (see the *Normative and descriptive theory of choice under risk* section). Thus, an average subject transforming the objective probabilities according to the assumed decision weighting function, should backup data more (less) frequently in a more (less) risky environment.

Similarly, we would expect that two subjects each working at a different pace in the same environment would back up data with various frequencies. Subjects working at a slower pace should back up data more frequently. Recall that the subject in our model values the prospects of data entry and data backup taking into account the probability of data loss in the "nearest future", i.e. the time the subject needs to input 1 record (see Table 1). Assume two subjects who work under same external risk: The subject working at slower pace would face a higher risk of data loss during each data entry and would therefore perceive the data backup action as attractive "earlier" than the subject working at substantially quicker pace.

The two basic hypotheses about backup frequency outlined above may be formulated as follows:

*H 1.1: As the external risk increases, subjects working at the same pace will backup data more frequently.*

*H 1.2: Working under the same external risks, subjects who work slower will backup data in smaller batches.*

In Figure 9 we present simulation runs for a subject working at normal pace in a more and less secure environment (see Table 2), without any data loss events.[15] We can clearly see that data backups are more frequent under the higher data loss condition (Figure 9a). This is in agreement with our H 1.1.

[14] For details, see the *System dynamics model of CPT-subject in IT-environment* section.

[15] The supplemental simulation model contains a set of GUI controls that allow for running the various simulation runs discussed throughout the paper.

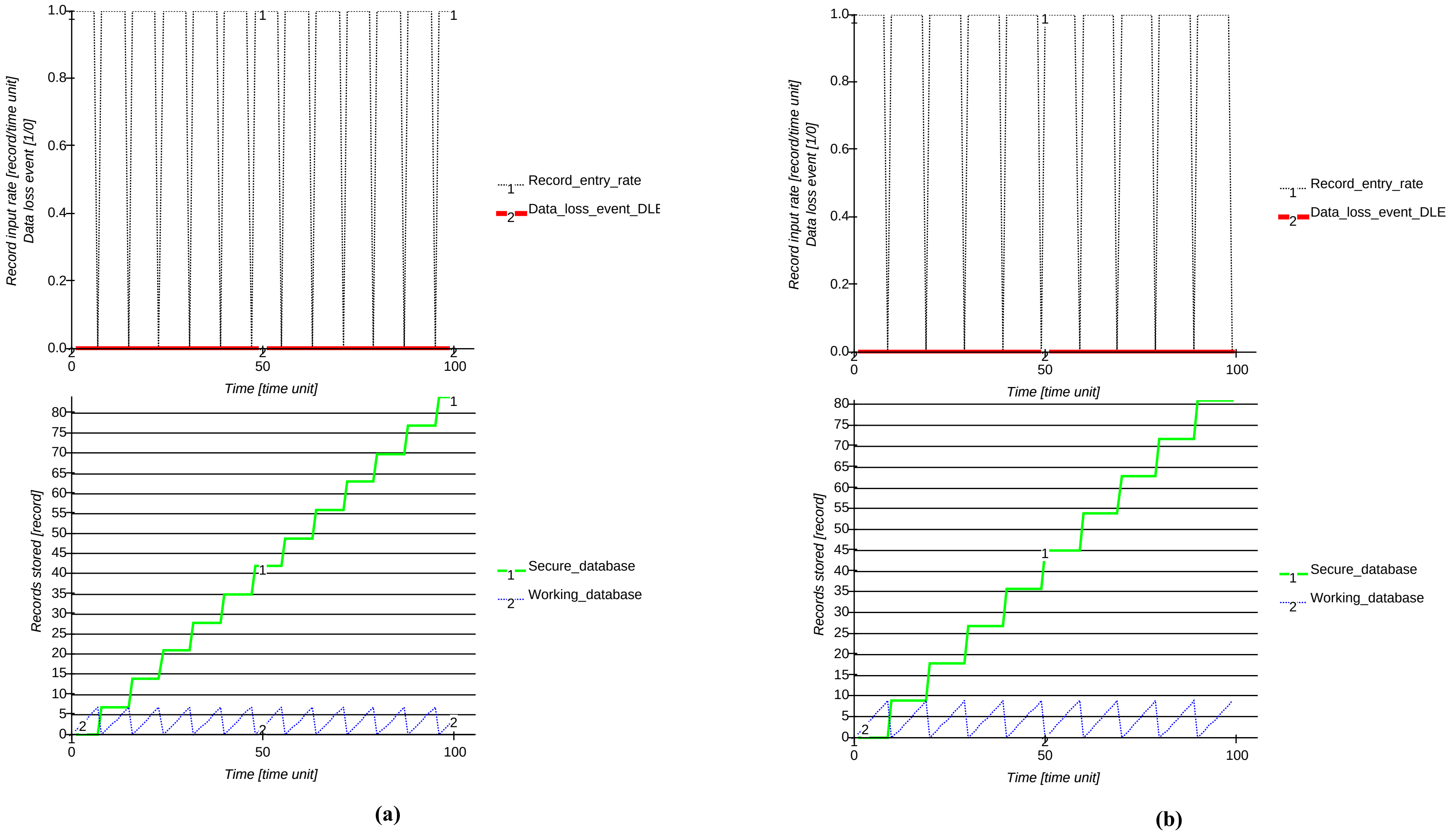


**Figure 9 Working under higher (a) and lower (b) probability of data loss (no data loss event occurs)**

Turning to our second hypothesis, we test how the backup routine would change if we assumed a subject who needs twice as much time to enter each record. The work pattern of this subject working under the low data loss condition is presented in Figure 10. Comparing the simulation results with the results presented in Figure 9b, where there was the same, low probability of data loss but records were entered at a normal rate (see Table 2), we can see that H 1.2 holds: A subject who works at the normal working pace backs up data in 9-record batches (Figure 9b); a subject working at slower working pace (see Table 2) not only enters less data during the test session, but also backs data in smaller batches of approximately 4 records (Figure 10).[16]

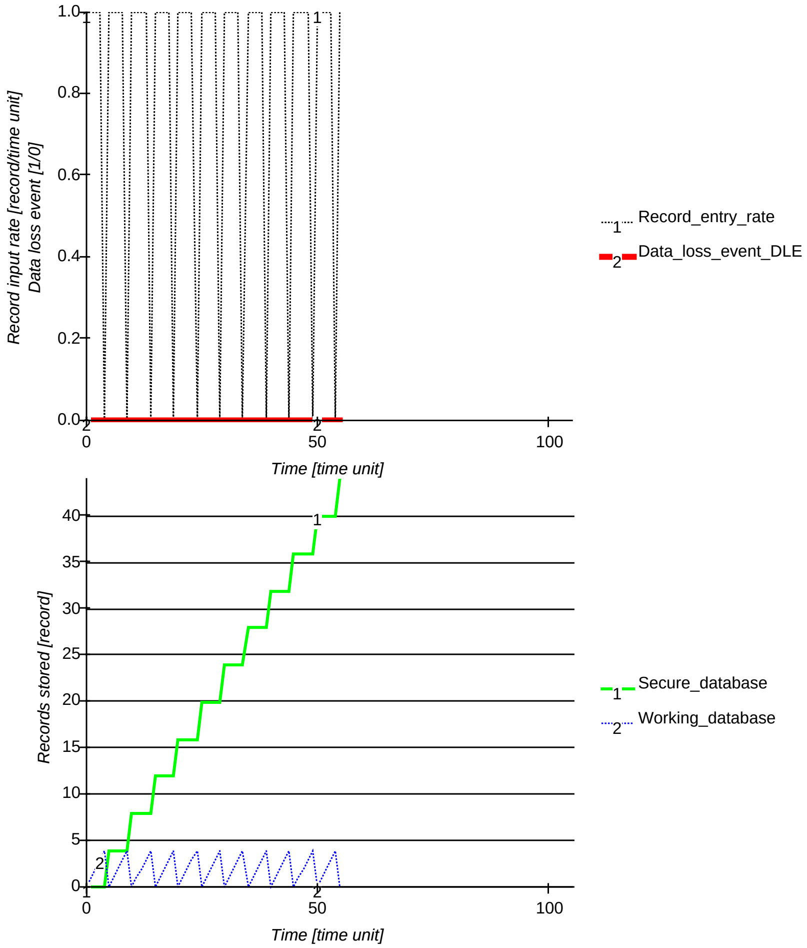


**Figure 10 Working at a slower pace under low probability of data loss**

As we indicated in the introductory part, field studies indicate that security observance is likely to be impacted by mishaps. We now turn to testing the following hypothesis:

*H 2: Data loss event will impact the backup frequency.*

[16] The reason why the simulation in Figure 8 is terminated at around the 55th time step is that the subject works at the slower pace (see Table 2) and in this case each time unit corresponds to 2 minutes, not to 1 as in case of the subject working at the normal pace. (see also discussion of the simulation duration control, pp. 9-10)

We assume a subject working at the normal pace in the low probability condition (see Figure 9b), but now we define that a data loss event occurs at 55th time unit during the simulation. As illustrated in Figure 11, the simulation results contradict our other hypothesis, H 2.

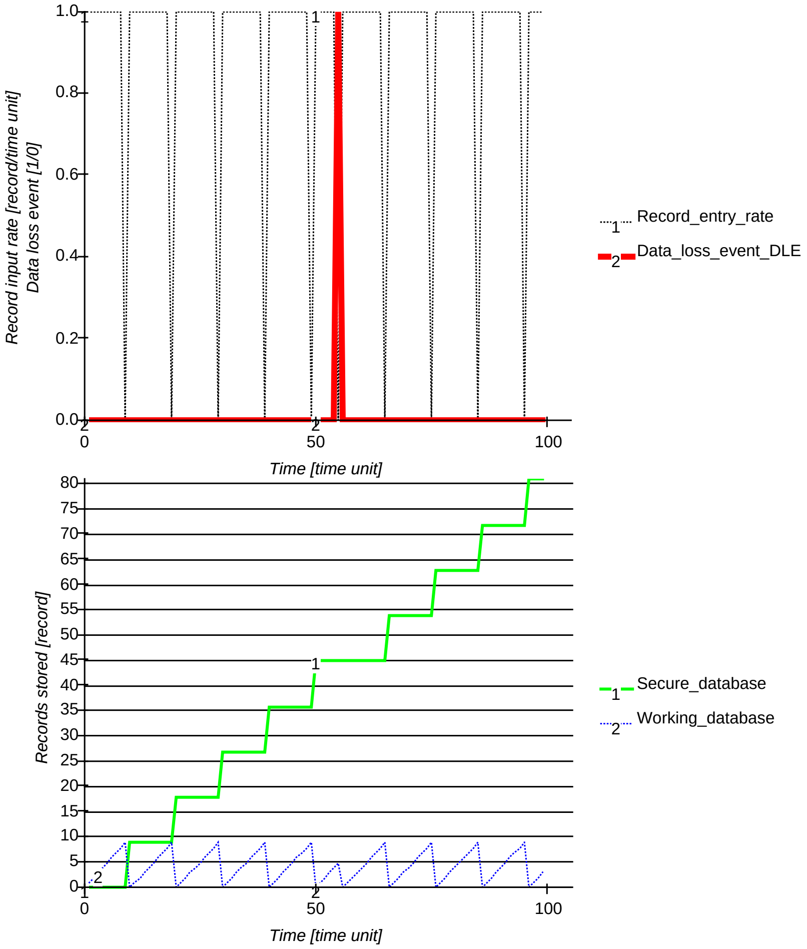


**Figure 11 Reaction to a data loss event**

Data loss event results in loss of about 5 records. After the event, the subject continues to back up data in the same batches as before. Reviewing the decision rules the subject follows (see Table 1), we see that for the backup frequency to change, either the subject's valuation of records and the time it takes to reenter them, or the subject's perception of risk should be altered as a result of the data loss event. Without such feedback relationship, the subject would always follow the initially defined backup policy. These findings are obviously in sharp contrast with observations and field studies' findings regarding human behavior over extended periods of time in risky environments. Before we discuss how the model could be modified to account also for these patterns, we want to point to some implications for security policy that may be drawn from the analysis hitherto.

## Design of IT-security policy

Intriguingly, CPT brings rather optimistic news for security policy designers: As probabilities of mishaps are usually small, under CPT people would overestimate them. Consequently, they are rather likely to act more rather than less secure. Obviously, field observations do not support such claims and reports of insufficient security observance are frequent. Experience also shows, that contrary to what the CPT-based analysis implies, people are not likely to maintain a steady security regime over time. The employed security routines are likely to evolve, being especially sensitive to occurrence, as well as absence, of mishaps.

Assuming that both an organization and an individual maintain relatively accurate estimates of mishaps' probabilities, the problematic behavior could be explained by a mismatch between their respective valuation of losses and gains. Indeed, it is not unlikely that the organization perceives some loss as much larger than an individual would do. This may be, for example, due to the fact that events such as (even minor) data loss may bring along other losses for the organization such as bad publicity. Thus, to the organization it may seem desirable and rational to employ a much higher protection level than it would seem appropriate to the individual. This situation corresponds to the organizational and personal goal mismatch described by Reason (1997). A number of policies may be designed to diminish the discrepancy; here, we outline only a couple.

First, the organization could introduce a system that would provide additional enforcement for a higher security observance. To illustrate this policy option, we implemented a system under which for each record lost the individual will have to "pay back" the equivalent of 2 records. First, recall the behavior presented in Figure 9b. In Figure 12 we present the behavior of the "same" subject who still works in the less risky environment, but under the imposed security-enforcement system. Indeed, the backup frequency increases.[17]

[17] Supplemented simulation model contains a set of GUI controls that allow for running the various simulation runs discussed throughout the paper.

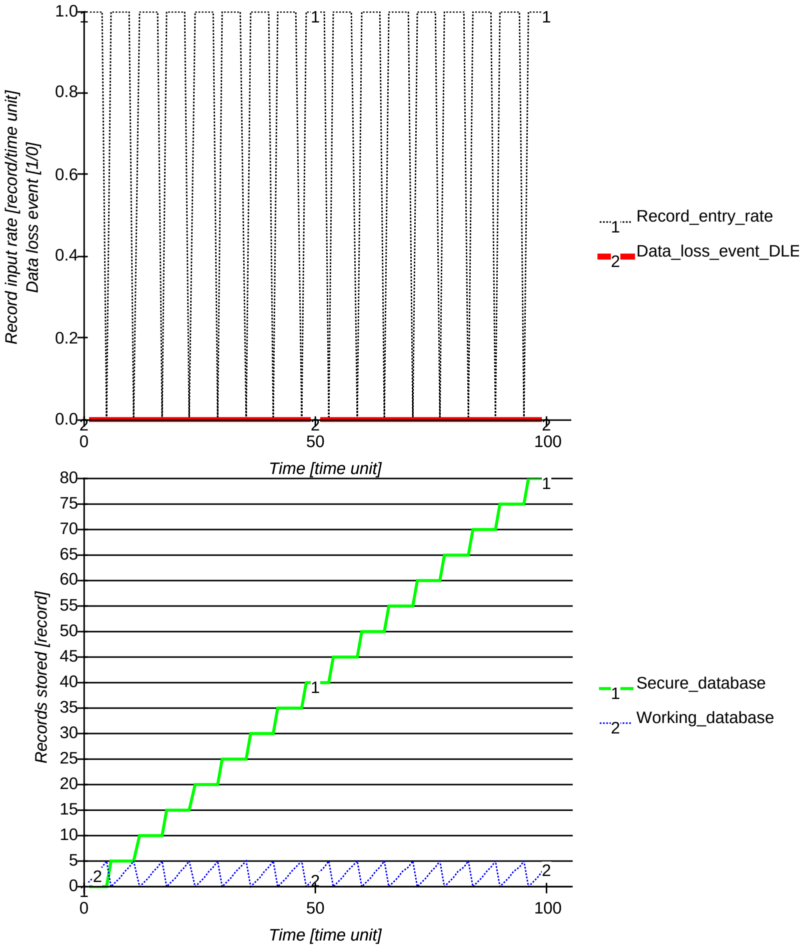
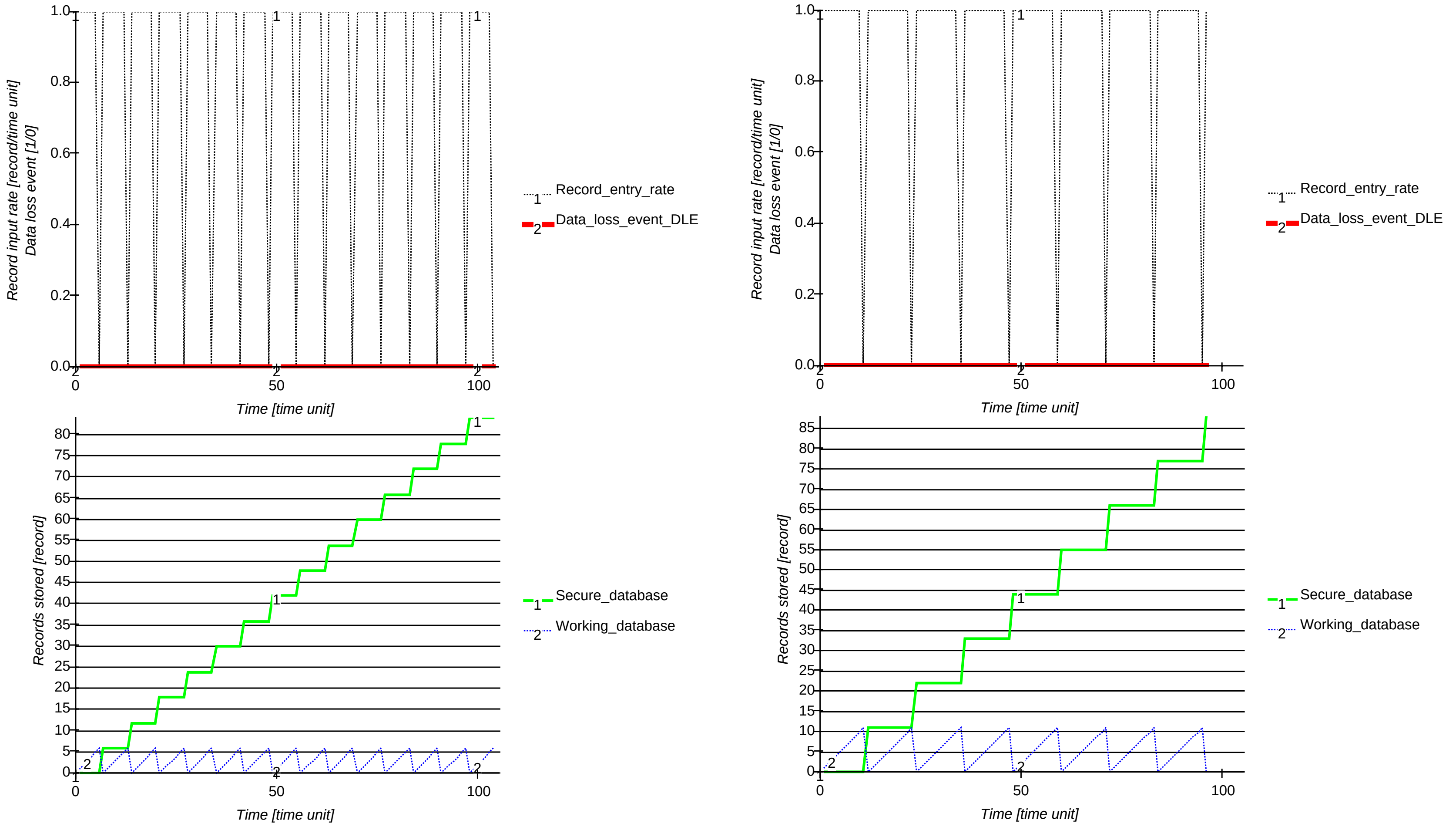


**Figure 12 Working under an enforcement system**

Alternatively to increase security observance, the organization could improve the efficiency of security mechanisms. In Figure 13a we present how the behavior of the subject working in the less risky environment at the normal pace (see Figure 9b) changes when backup initialization time is reduced by 50% (see Table 2). This illustrates how important the efficiency of security measures may be for the overall effectiveness of a security system. In Figure 13b we present the behavior of the same subject working in a system where it takes 50% more time to initialize backup. As we can see, backups are performed less frequently.



(a)

(b)

**Figure 13 Impact of efficiency of security mechanisms on security observance – shorter (a) and longer (b) backup initialization time (see Figure 9b)**

Developing appropriate motivational system supporting the actual IT-security system seems to be of key importance to elicit a sustained, more secure behavior. Indeed, cases in which eroded security observance is attributed at least in some part to an unbalanced motivational system are not rare. The Westray mine case is a good example of such situation: In his thorough analysis Cooke shows using system dynamics how the unbalanced motivational system favoring throughput and undermining security goals was instrumental in decreasing the overall security observance and creating a fertile ground for the ultimate disaster (Cooke 2003b). A similar situation occurred in case of the Omega management who were oblivious to security issues by the prevailing, omnipotent pressure to grow (see the parallel paper Melara, Sarriegi, Gonzalez, Sawicka & Cooke 2003). Both cases illustrate also the human inability to perceive accurately and promptly the deterioration of their risk exposure until it is revealed by some explicit events, like a mine accident in the Westray mine case or an attack on the company's IT-system in the Omega case.

Volatility of risk perception has been pointed out by many as one of the key factors underlying the gradual erosion of compliance (see e.g. Weick 1987, Wilde 1994, Gonzalez 1995, Gonzalez 2002). The erosion has been explained in various ways (for specific references see Gonzalez and Sawicka 2003b). In our other papers we explore how instrumental conditioning theory may explain the phenomenon (see, for example, Gonzalez and Sawicka 2003a, b). Regardless of origins, it seems indisputable however that people's perception of how risky their environment is will be significantly influenced by their past experiences.

As we indicated previously, CPT was developed using data gathered through static, one-time decisions (see *Normative and descriptive theory of choice under risk*). Thus it should not be surprising that behavior of an individual following CPT is strikingly regular over time. Indeed, once all the probability and value transformation functions' parameters are known, the pattern may be easily and accurately estimated. It is characterized by a single threshold – the size of backup-batch that we can derive from the decision rules presented in Table 1. Given that the backup is run only when (see also Figure 8):

$$-\omega(p)*(R + bDel*IR) < -R*bDel$$

where
**ω(*p*)** corresponds to *Perceived probability of immediate loss*,
**R** to *Working database*,
**IR** to *Normal entry rate*
**bDel** to *Backup delay*
in our model (see Figure 3, Figure 5, Figure 7 and also Figure 8)

and

$$bDel=R*bR + bInit$$

where
**bR** corresponds to *Record backup time*,
**bInit** to *Backup Init Time*
in our model (see Figure 5)

the threshold number of records is given by:

$$R = \frac{bInit*(1-\omega(p))}{\omega(p)*(1+bR) - bR} \tag{9}$$

The formula not only enables us to estimate the backup frequency. It also indicates some interesting relationships between factors likely to impact the backup threshold. We can clearly see that the greater the backup initialization time (*bInit*), the higher will be the threshold. Also, for any risky environment there exists some maximum record backup time (*bR*) above which backup becomes unattractive. Lastly, equation (9) indicates that the higher the perceived risk of loss the lower the threshold.

These relationships may help us understand why it is so difficult to control human factors in modern IT-systems. In most cases, protection mechanisms are highly automated and reduce substantially the end-users' risk exposure. Note that according to equation (9), as the risk exposure diminishes, or, more accurately, as the perceived risk diminishes, the higher the threshold, i.e. the less frequently the backup will be taken. To preserve the same security observance level, the reduction in risk exposure should be compensated by an appropriate increase in effectiveness of employed security mechanisms. Simulation results presented in Figure 13 illustrate how the efficiency of security mechanisms influences the backup frequency.

## Counterintuitive results

The regularity of the CPT individual's behavior pattern implies that it would be possible to design a security system in which secure behavior is sustained over time. This implication is clearly at odds with the behavior patterns commonly observed in risky environments (see Figure 1 and the accompanying discussion).

To identify possible origins of the erosion of security observance, let's assume a stable level of external threats and a constant valuation of outcomes by individuals. We need to consider two cases: First, a situation where the desired degree of security observance is elicited only under some additional enforcement system; here, it could be that security observance deteriorates due to gradual weakening of the enforcement. Second, a situation where there is no additional enforcement system (or the system does not deteriorate); in this case the gradual erosion of security observance over-time may only be explained by a decline in the individual's perception of the probability of mishaps (see also discussion at the end of the *Design of IT-security policy* section).

In both cases, the working mechanism is basically instrumental conditioning. The potential importance of conditioning mechanisms for governing the human behavior in risky environments was pointed out by Gonzalez (2002; see also Gonzalez and Sawicka 2003a, b). Both the deterioration of an enforcement system and the erosion of the perception of the probability of mishap may be interpreted as a withdrawal of enforcer in a conditioning process. The two cases differ only in the enforcer's origins: In the first case the enforcer is external to the individual, while in the second case it is internal.

In the mishaps' aftermath, it is common to try to identify those who bear responsibility. Sometimes the investigations stop short of identifying the real root causes, simply assigning the blame to actors who neglected some security measures. Yet such conclusion seems questionable if the enforcement system was malfunctioning. Assigning blame only to actors directly involved in an incident may also be questioned in cases when the enforcement system functioned properly. This is because an extensive research does show that people are poor judges of risks (Estes 1976, Kahneman and Tversky 2000, Hogarth 1987, Tversky and Kahneman 2000, Zeitlin 1994): Typically, beliefs about probabilities of events are derived from experience. Events' frequencies provide main cues for the estimates. The longer one acts in an environment and does not observe (or hear about) an event, the more likely the event's probability will be underestimated. If human nature is so, security systems should be designed in a way that would help to maintain appropriate risk perception. If they fail to do so, at least part of the responsibility for occurring mishaps should be assigned to the security systems' designers. This view coincides with the "engineering view" of origins of human error (cf. Reason 1997, pp. 224-225, see also discussion in Gonzalez and Sawicka 2003). The need to take into account human ability to perceive risk in security or safety system designs has been recently receiving more and more attention. A number of IT-security professionals point to an ongoing security training as indispensable tool for maintaining accurate security awareness (see e.g. Smith 2001, Tuesday 2001, Voss 2001). In a parallel conference paper, Cooke proposes an incident learning system to facilitate maintenance of accurate risk perception in organizations operating in risky environments (Cooke 2003a).

Psychological research has shown that the probability of events that occur frequently is likely to be overestimated. Such dynamic perception of probabilities could explain increases in security adherence just after occurrence of mishaps or release of news about such events. The overestimation of risks would then be the likely cause for an increased observance of security measures. As the reader may recall, our model failed to demonstrate such effect. According to the model, data loss has no impact on employed security routines (see Figure 11 and accompanying discussion). This counterintuitive outcome however is entirely consistent with CPT: The theory does not account for any dynamic changes in perception of probabilities or for possible changes in value functions. This narrows its applicability to situations where people choose between risky prospects in domains that they have relatively little prior experience in, and where in their choices they are forced to rely primarily on external information.

Acknowledging limitations of CPT, a number of researchers have proposed alternative theories. Prior information and experience within a problem domain and presentation of the choice problem have been often stressed as important variables impacting choices. Recently, also a number of theories providing an explicit description of choice in dynamic settings have been proposed. The applicability of these theories to our context is currently under investigation. One of the main advantages of CPT is that the theory has been extensively tested. It is therefore well known and indeed is gaining an increasing acceptance outside the psychological field. Simultaneously, our initial analyses of the competing theories indicate that many of them either fail again to account for risky choice dynamics (e.g. Einhorn and Hogarth 1985, Lopes and Oden 1999) or do not provide a fully formalized model (e.g. Slovic 2000; Slovic, Fischoff et al. 2000). Among the reviewed theories of dynamic choice under risk, we found that some deal only with particular features of dynamic choice under risk, like e.g. explanation of deliberation process in the case of decision field theory (see e.g. Townsend and Busemeyer 1995), or provide a limited explanation of psychological mechanisms underlying the choice dynamics as it is in case of token theory (Regenwetter, Falmagne et al. 1999). In the following section we suggest how CPT could be extended to account for the dynamics commonly observed in cases of repeated choice under risk, such as the case we consider here – i.e. security observance in IT-based work environments.

## Toward a dynamic prospect theory

Imagine two agents who value outcomes in a similar way and act in a risky environment where probability of loss is low. A CPT agent would act in a more cautious way than a rational agent who acts according to EUT. This is due to the CPT agent's overestimation of potential losses and simultaneous underestimation of potential gains. The CPT and the EUT agents have different focus of attention. While a CPT agent overweighs probabilities related to losses, an EUT agent assesses probabilities in a more balanced and "objective" way. As a result, the CPT agent effectuates choices that would be considered inferior under EUT. Following the attention clue, we could envisage an agent who contradicts EUT by focusing substantially more on issues related to gains. Such agent in risky environments would be likely to overestimate high and moderate probabilities of gains while underestimating low probability of losses. As a result, the agent would manifest a much less secure behavior than either the CPT or the EUT agent.

Recall the $\omega(p)$ function suggested for the probability transformation: Setting the $\eta$ parameter to 1 yields $\omega(p)=p$. This makes CPT equivalent to EUT. Elicitation of an opposite pattern of probability misperception would require $\eta>1$. Implementing a dynamically adjustable parameter $\eta$ would then yield a model in which the whole range of probability misperceptions are feasible. The $\eta$ parameter may be conceptualized as a relative attention given to small vs. moderate and high probability events.

In Figure 14 we present simulation results where the accuracy of individual's risk perception is assumed to gradually fade away, which process is modeled as an overtime increase of the probability perception parameter $\eta$.[18]

A dynamic definition of the probability perception parameter $\eta$ seems appropriate: Experience shows that people new in a risky environment are likely to focus at least as much, if not more, on potential losses as on potential gains ($\eta<=1$). Moreover, as the time passes by, throughput-oriented activities gain more and more attention. The attention given to possible losses – events that "never occur" – fades ($\eta>1$). The high level $\eta$ would be drastically reduced only by an event that brings losses into the attention of people again. The degree of $\eta$ reduction is likely to depend on the degree to which the event draws our attention to losses, i.e. the more severe the event, the greater reduction in $\eta$.

Collecting data on the phenomenon of erosion in security observance is a difficult task. It would require observations over an extended period of time, as people do not adjust instantly their perceptions. Performing experiments that would test the erosion hypothesis is rather challenging. What can however be observed in the laboratory is the impact bad news or mishaps have on security observance. Based on such data, the hypotheses about dynamic adjustment of the probability perceptions could be tested at least qualitatively. Drawing on this type of experimental results, we intend to implement more carefully a mechanism for dynamic adjustment of the $\eta$ parameter in our model. In this way, we hope to contribute to the development of a more general, descriptive theory of human behavior in risky environments. We believe the improved system dynamics models resulting from our investigations will become useful tools facilitating development of robust IT-security policies.

[18] The supplemental simulation model contains a set of GUI controls that allow for running the various simulation runs discussed throughout the paper.

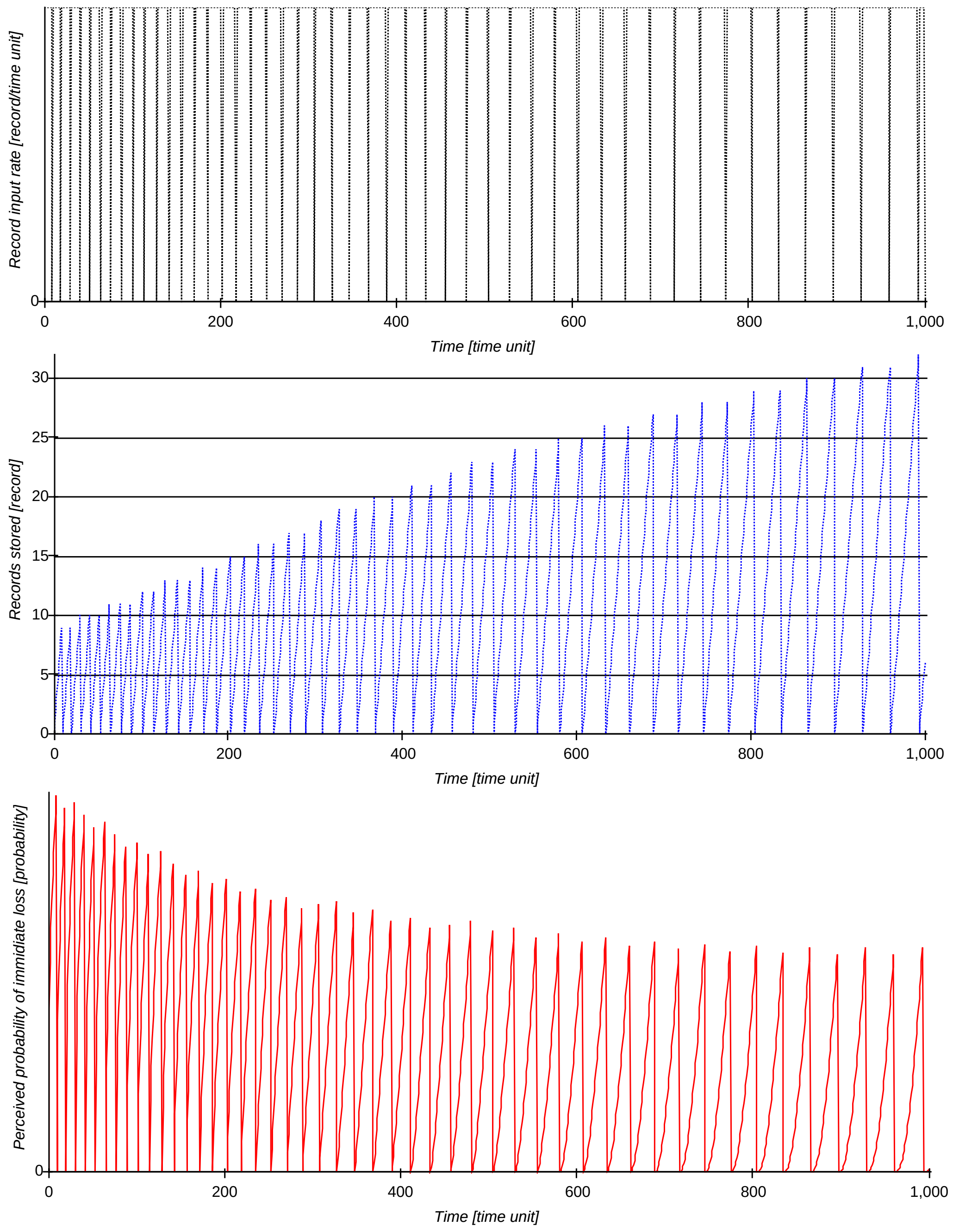


**Figure 14 Impact of change in Probability Perception Parameter**

## Acknowledgment

The contribution by Agata Sawicka has been financed with a fellowship of the City of Kristiansand, Norway.

## Appendix 1

Acronyms used in the paper:

| | |
|---|---|
| CPT | - cumulative prospect theory |
| EUT | - expected utility theory |
| IT | - information technology |

## Appendix 2

### Transformation of outcomes: Value function

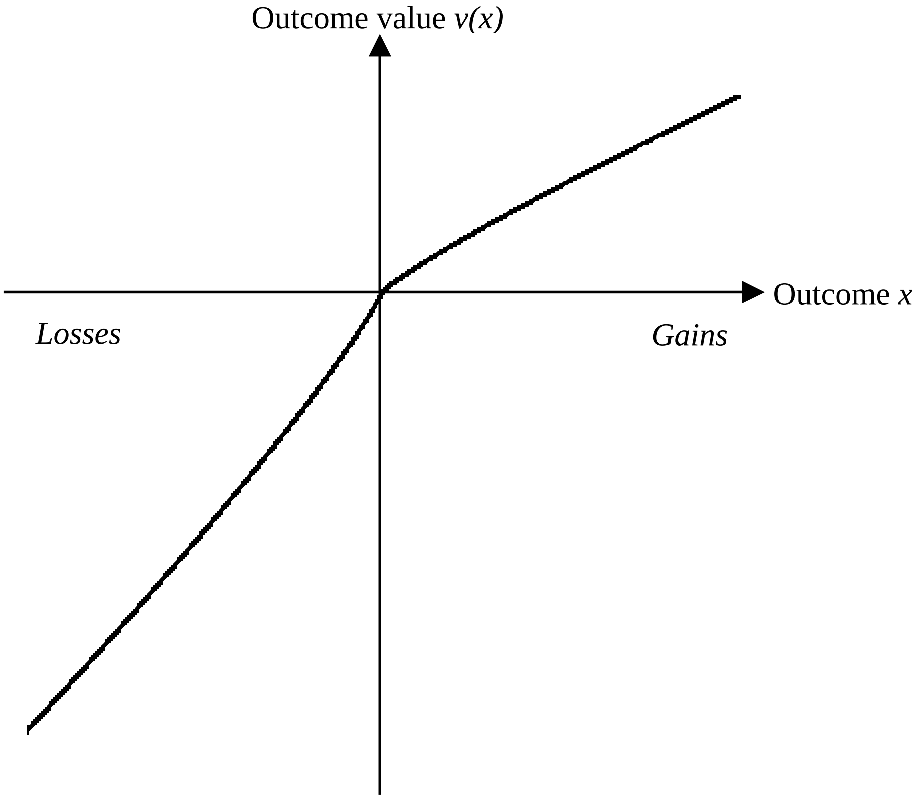


**Figure 3.1** The concave value function for gains accounts for risk aversion observed over domain of gains; the convex and steeper value function for losses illustrates risk-seeking attitudes observed in the loss domain.

## Transformation of probabilities: Decision weight function

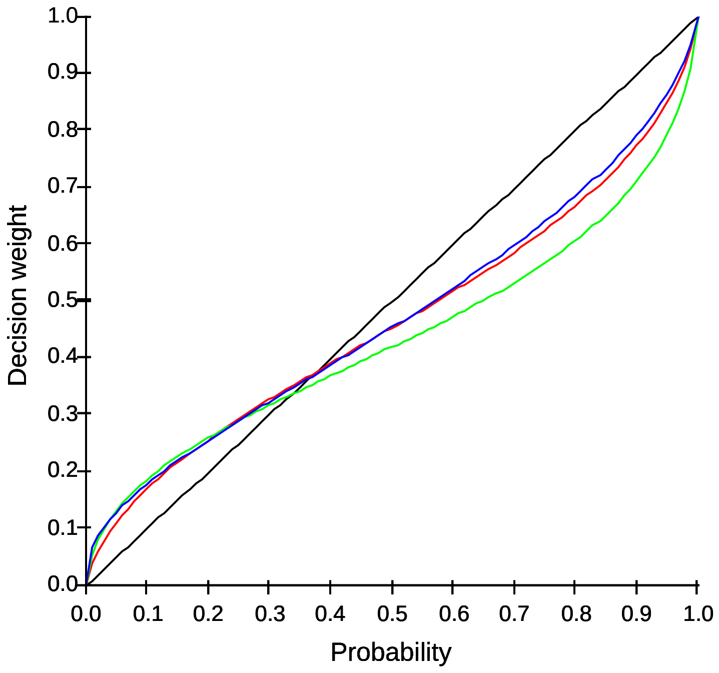


**Figure 3.2** Patterns of various decision weight functions:

| | | |
|---|---|---|
| 🟩 | $\omega^{+}(p) = \dfrac{p^{\gamma}}{(p^{\gamma} + (1-p)^{\gamma})^{1/\gamma}}$ | for probabilities associated with gains<br>where γ=0.69 (see Tversky and Kahneman 2000) |
| 🟥 | $\omega^{-}(p) = \dfrac{p^{\delta}}{(p^{\delta} + (1-p)^{\delta})^{1/\delta}}$ | for probabilities associated with losses<br>where δ=0.61 (see Tversky and Kahneman 2000) |
| 🟦 | $\omega(\mathrm{p}) = \exp\left\{-(-\ln\left(\mathrm{p}\right)^{\eta}\right\}$ | for probabilities of all outcomes<br>where η=0.65 (see Prelec 2000) |

## BIBLIOGRAPHY

Abdellaoui, M. (2000). Parameter-free elicitation of utilities and probability weighting functions. *Management Science* 46(11): 1497-1512

Anderson, R. (2001). *Security Engineering: A Comprehensive Guide to Building Dependable Distributed Systems*. John Wiley & Sons

Bleichrodt, H. and J. L. Pinto (2000). A parameter-free elicitation of the probability weighting function in medical decision analysis. *Management Science* 46(11): 1485-1496

Callene, D. R. (2000). *Managing effective information security*. SANS Institute. http://rr.sans.org/casestudies/effective_infosec.php (04.03.2002).

Camerer, C. F. and T. H. Ho (1994). Violations of the betweenness axiom and nonlinearity in probability. *Journal of Risk and Uncertainty* 8(2): 167-196

Cooke, D. L. (2003a). Learning from incidents. *Proceedings of the 21st International Conference of the System Dynamics Society, 2003 New York, USA.*

Cooke, D. L. (2003b). A system dynamics analysis of Westray mine disaster. *System Dynamics Review* 19(2)

Dörner, D. (1996). *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations*. Addison-Wesley

Economist.com (2002). The weakest link. The Economist, The Economist Newspaper and The Economist Group.**:** http://www.economist.com/surveys/displayStory.cfm?story_id=1389553.

Einhorn, H. J. and R. M. Hogarth (1985). Ambiguity and uncertainty in probabilistic inference. *Psychological Review* 92(4): 433-461

Estes, W. K. (1976). The cognitive side of probability. *Psychological Review* 83(1): 37-64

Gonzalez, J. J. (1995). Computer-assisted learning to prevent HIV-spread: Visions, delays and opportunities. *Machine-Mediated Learning* 5(1): 3-11

Gonzalez, J. J. (2002). Modeling the Erosion of Safe Sex Practices. *Proceedings of the Twentieth International Conference of the System Dynamics Society July 28 - August 1, 2002 Palermo, Italy*

Gonzalez, J. J. and A. Sawicka (2003a). Modeling Instrumental Conditioning -- The Behavioral regulation approach. *36th Hawaii International Conference on System Sciences (HICSS 36)*, Big Island, Hawaii.

Gonzalez, J. J. and A. Sawicka (2003b). The role of learning and risk perception in compliance. *Proceedings of the 21st International Conference of the System Dynamics Society, 2003 New York, USA.*

Hastie, R. and R. M. Dawes (2001). *Rational Choice in an Uncertain World: The Psychology of Judgment and Decision Making.* Sage Publications

Hogarth, R. M. (1987). *Judgment and Choice: The Psychology of Decision*. John Wiley & Sons

Kahneman, D. and A. Tversky (2000). *Choices, Values, and Frames*. Cambridge University Press

Kahneman, D. and A. Tversky (2000). Prospect theory: An analysis of decision under risk. In D. Kahneman and A. Tversky. *Choices, Values, and Frames*, Cambridge University Press. (Originally published in 1979. *Econometrica*. 47(2). 263-291.)

Lopes, L. L. and G. C. Oden (1999). The role of aspiration level in risky choice: A comparison of cumulative prospect theory and SP/A theory. *Journal of Mathematical Psychology* 43: 286-313

Melara, C., J. M. Sarriegi, J. J. Gonzalez, D. Cooke and A. Sawicka. (2003). A system dynamics model of an insider attack to information systems. *Proceedings of the 21st International Conference of the System Dynamics Society, 2003 New York, USA.*

Prelec, D. (2000). Compound invariant weighting functions in prospect theory. In D. Kahneman and A. Tversky. *Choices, Values, and Frames*. Cambridge, Cambridge University Press.

Reason, J. (1990). *Human Error*. Cambridge University Press

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate Publishing

Regenwetter, M., J.-C. Falmagne, et al. (1999). A stochastic model of preference change and its application to 1992 presidential election panel data. *Psychological Review* 106(2): 362-384

Sawicka, A. (2003). Compliance as choice under risk: Investigating cumulative prospect theory in a risky work environment. *5th International Conference on Cognitive Modeling (ICCM 2003)*, Bamberg, Germany.

Sawicka, A. (2003). *Experiments on security observance in a simple IT-based work environment: Data analysis*. Unpublished manuscript.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc.

Simon, H. A. (1982). Some strategic considerations in the construction of social science models. In H. A. Simon. *Models of Bounded Rationality*, The MIT Press. (2)**:** 209-238. (Originally published in 1954. *Mathematical Thinking in Social Sciences*, Eds. P. Lazarsfeld, pp.388-415. Glencoe, Ill. The Free Press.)

Slovic, P. (2000). Informing and educating the public about risk. In P. Slovic. *The Perception of Risk*, Earthscan. (Originally published in 1986. *Risk Analysis*. 6(4). 403-415.)

Slovic, P., B. Fischoff, et al. (2000). Preference for insuring against probable small losses: Insurance implications. In P. Slovic. *The Perception of Risk*, Earthscan. (Originally published in 1977. *Journal of Risk and Insurance*. XLIV(2). 237-257.)

Smith, K. (2001). *Security awareness: Help the users understand*. http://rr.sans.org/aware/help.php (04.03.2002).

Snell, L. J. (1989). *Introduction to Probability*. McGraw-Hill

Townsend, J. T. and J. Busemeyer (1995). Dynamic representation of decision making. In R. F. Port and T. van Gelder. *Mind as Motion: Exploration in the Dynamics of Cognition*, The MIT Press.

Tuesday, V. (2001). Human factor derails best-laid security plans. *Computerworld*

Tversky, A. and D. Kahneman (2000). Advances in prospect theory: Cumulative representation of uncertainty. In D. Kahneman and A. Tversky. *Choices, Values, and Frames*, Cambridge University Press. (Originally published in 1992. *Journal of Risk and Uncertainty*. (5). 297-323.)

von Neumann, J. and O. Morgenstern (1944). *Theory of Games and Economic Behavior*. Princeton University Press

Voss, B. D. (2001). *The ultimate defense of depth: Security awareness in your company*. SANS Institute. http://rr.sans.org/aware/ultimate.php (04.03.2001).

Wakker, P. and D. Deneffe (1996). Eliciting von Neumann-Morgenstern utilities when probabilities are distorted or unknown. *Management Science* 42(8): 1131-1150

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review* 29(2): 112-127

Wilde, G. J. S. (1994). *Target Risk*. Gerald J.S. Wilde. http://pavlov.psyc.queensu.ca/target/index.html (15.10.2001).

Wu, G. and R. Gonzalez (1996). Curvature of the probability weighting function. *Management Science* 42(12): 1676-1690

Zeitlin, L. R. (1994). Failure to follow safety instructions: Faulty communication or risky decisions? *Human Factors* 36(1): 172-181

Back to the Top