Supporting Material is available for this work. For more information, follow the link from the Table of Contents to "Accessing Supporting Material".

The Role of Learning and Risk Perception in Compliance

By
Jose J Gonzalez
Agata Sawicka
Faculty of Engineering and Science
Dept. of Information & Communication Technology
Agder University College
Groosveien 36
NO-4876 Grimstad, Norway
Phone: +47 37 25 32 40
Fax: +47 37 25 31 91
Email: Jose.J.Gonzalez@hia.no URL: http://ikt.hia.no/josejg/

Abstract

Human factors are implicated in most security (and safety) problems, a ubiquitous aspect being erosion of compliance.
We discuss several theories of the role of human factors and present system dynamic models based on the theoretical paradigm of instrumental conditioning (the behavioral regulation theory). The proposed mechanism involves learning – both adequate and inadequate, 'superstitious' learning – and it conforms to basic facts of human character (propensity to misperceive risk, biological roots of instrumental conditioning).
Our generic models are able to render generic reference behavior. Also, they suggest possible reasons for why technological advances paradoxically may worsen human compliance. The concept of the behavioral bliss point – immanent to the behavioral regulation theory – makes the learning aspect an inseparable companion to different mechanisms promoting erosion of compliance (such as throughput/security priority conflicts, mismatch between organizational and personal goal, etc).
To counteract erosion of compliance we suggest policies involving educational and social interventions.

Introduction

The purpose of this paper is to model erosion of human compliance in regard to security and safety systems. There are strong reasons for this. Human factors are implicated in 80-90% of security and safety problems and erosion of compliance is a ubiquitous feature. Whether security or safety, we will argue that erosion of compliance is largely shaped by the same determinants. Feedback is central to the issue. Accordingly, system dynamics ought to be a promising approach to safety and security problems.

Merriam-Webster Online defines “security” and “safety” in the sense of «the quality or state of being secure: as a freedom from danger» as synonyms.[1] In another sense, viz. «something that secures: measures taken to guard against espionage or sabotage, crime, attack, or escape», “security” and “protection” are considered synonyms. As field of study, safety is concerned with the aspect of prevention of disease, hurt, injury, or loss, mainly in the frame of risks from organizational accidents. Security in the sense of property or information security has in mind measures to guard against espionage, sabotage and crime, the issues at stake being property damage or loss, or confidentiality, integrity and availability of information. One talks also of security in relation with e.g. airport security, where the main issue is protecting people against terrorist attacks. Note, however, that some authors, notably Anderson, do not use the term safety but employ security in relation to prevent “malice, error or mischance.” (Anderson 2001, p. 3)

For the purpose of studying the role of human factors in the erosion of compliance, the usual distinction between safety and security is not crucial in a *first approximation*. In the case of safety issues, fortuitous events triggered by (mostly) unintended human actions and conditions (e.g., air traffic) may or may not lead to an organizational accident – the probability for such an accident depending on the *actual risk level*. For security issues, the fortuitous events are triggered by intended human actions (malicious attacks) and conditions (e.g., network traffic.) – the probability for such a malicious attack to succeed depending again on the *actual risk level*. The actual risk level toward accidents or attacks will always depend on the degree to which human agents comply with the prescribed protection measures. The general causal mechanisms underlying human factors may be described in both cases by abstract variables such as tasks, procedures, actual and perceived risk levels, stream of triggering events, etc.

In an authoritative treatise on managing the risks of organizational accidents Reason stresses the ubiquitous nature of human factors (Reason 1997). E.g. “the natural human tendency to produce errors and violations” (p. 17); “the trading of protective gains for productive advantage and the gradual deteriorations of defenses” (p. 19); “one of the enduring findings of work psychology us that people will be tempted to take short-cuts whenever such opportunities present themselves” (p. 48); “new and improved defenses are used for furthering productive, rather than protective, goals. In other words, organizations become accustomed to their apparently safe state and allow themselves to drift – like the “unrocked boat”[2] – into regions of greater vulnerability” (p. 112). The fashionable claim that ‘human error’ is implicated in 80-90% of major accidents is endorsed by Reason, but he cautions: “this statement adds very little to our understanding of how and why organizational accidents happen.” (Reason 1997, p. 61) Referring to Deborah Lucas, Reason discusses three different views on the origins of human error (cf. Reason 1997, pp. 224-225). According to the “person model” an actor involved in an accident or security breach has the primary responsibility for the event. The model assumes that the actor is always

[1] *Merriam-Webster OnLine: Collegiate Dictionary*. 2003. http://www.merriam-webster.com/dictionary.htm (24.03.2003).
[2] Reason (1997) gives Constance Perin credit for coining the suggestive metaphor of the “unrocked boat” (opus cit., p. 20, note 4).

capable of choosing between compliant and non-compliant, safe and unsafe behaviors. The "engineering model", on the contrary, argues that actors directly involved in a security breach situation should be excused most of the times. The decisive role of the environment in the accident causation is emphasized. Safety should be "engineered into" the system, and any subsequent human failures should be viewed as failures of the system designers rather than individual actors. The "organizational model" extends the engineering model. Here, human errors are seen as mere materializations of latent error conditions existing in the organization. Origins of the latent conditions may usually be traced to a much higher levels of organization than the level at which the security breach occurred.
Reason points out that the three models should not be treated as mutually exclusive but rather as complementary (cf. Reason 1997, p. 226). Indeed, they create a powerful framework for comprehensive assessment of risk levels involved in hazardous systems. The framework suggests a feedback nature of the security systems; accidents (or security breaches) attributed to human factors can no longer be seen as instances of "pure" human failures. They must be recognized as consequences of a complex interplay between individuals and their environment. Feedback and change over time are essential in this context.

Beyond the "first approximation" mentioned above (p. 2) the role of human factors as a main cause of security problems get additional flavors through the interplay between the attacker – malicious agent – and target of the attack (see e.g. Schneier 2000; Mitnick and Simon 2002). Concerning *information* security Schneier is outspoken about people being its Achilles heel. He revokes his former claim that cryptography be "The Answer™" (Schneier 2000, p. xii; see Schneier 1994 for the, later revoked, claims concerning cryptography). He makes it clear that the vulnerability is not in the cryptography: "…I found that the weak points had nothing to do with mathematics [i.e. cryptography]. They were in the hardware, the software, the networks and the people" (Schneier 2000, p. xii). He emphasizes that technology is not enough: "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" (Schneier 2000, p. xiii). He describes the "people problem" extensively and states bluntly: "Now I tell prospective clients that the mathematics are impeccable, the computers are vincible, the networks are lousy, and the people are abysmal. I've learned a lot about the problems of securing computers and networks, but none that really helps solve the people problem… People don't understand computers. People don't understand risks." He goes on to describe six aspects of the human problem: 1) How people perceive risks. 2) How people deal with things that happen very rarely. 3) The problem of trusting computers, and why that can be so dangerous. 4) The futility of asking people to make intelligent security decisions. 5) The dangers of malicious insiders. 6) Social engineering, and why it is so easy for an attacker to simply ask for secret information. (Schneier 2000, p. 255-6)

The last point – why it is so easy for an attacker to con people using social engineering – is extensively dealt with by legendary hacker Mitnick, now a highly successful security consultant (Mitnick and Simon 2002).

Despite the artfulness of external attackers, malicious insiders and cons, experts agree that people as targets of the attacks time and again are caught off-guard, and that erosion of compliance is a key aspect of such vulnerability.

We leave aside the aspect of modeling attacks (see our parallel paper Melara, Sarriegui, Gonzalez, Sawicka, and Cooke 2003 for a model of insider attacks) and concentrate on erosion of compliance in a generic setting that applies both to safety (accidents) and security (external threats). I.e., in the sense of the "first approximation" (p. 2) we describe mishaps as solely dependent on the actual risk level. To avoid the clumsy use of "safety and security" we imply with "security" prevention of malice, error or mischance and drop the term "safety". And we concentrate on the key questions: Why does compliance with security measures erode? What policies might counteract erosion of compliance?

Many factors can affect compliance with security measures, e.g. conflicting goals (throughput pressure vs security), cost-benefit factors, incl. perception of personal gains and losses, conflicts between personal and organizational goals, risk perception and risk acceptance, etc. The literature discusses extensively those factors and others, but little has been done in terms of tracking their causative influences over time in the sense of system dynamics. The interplay of users, organizational aspects, technology, tasks and environment in security work systems[3] is necessarily a system characterized by feedback, temporal change (nonlinear dynamics), time delays, soft factors, and interdisciplinary aspects. Clearly, the ultimate practical reason for studying such systems is to achieve desired goals and to prevent undesired performance. In other words, security systems need to be managed. All the above strongly suggests that system dynamics is a promising methodology to study security systems, including their human aspect.

Quite detailed cases describing organizational accidents are readily available and have been used as points of departure for successful system dynamics modeling (see e.g. modeling the Westray mine disaster in Cooke 2003b, 2003a). The same does not apply for security problems involving malicious acts: Here, corporations tend to be very secretive by fear of bad publicity. As a consequence, studies of malicious attacks are much less detailed than case studies of organizational accidents (for a system dynamics model of an insider attack see Melara et al. 2003).

Despite the quality of the Westray mine model the available data does not permit an in depth study of all (or even most) human factors that might be relevant for the etiology of organizational accidents. Having in mind that case studies of security attacks are even less detailed, this implies that available data does not yet allow to construct system dynamics models incorporating several (potentially) competing causative mechanisms to the effect of discriminating their relative contribution. As of today, modeling of security case studies only allow to test whether one or two hypothetical causative mechanisms are consistent with case data (in the sense of BOT of models being able to render the reference behavior modes). For example, in Cooke's model of the Westray mine disaster the dynamic hypothesis is the conflict

[3] The characterization of the (security) work system as consisting of users, organizational aspects, technology, tasks and environment is borrowed from (Carayon and Kraemer 2002).

throughput-security (Cooke 2003b). In Melara et al.'s model of the Omega insider attack the dynamic hypothesis is that pressure to grow made Omega's management overly concerned with disruptions of workplace climate caused by a problematic individual in charge of the company's information system: Further, management was correspondingly oblivious to the security threat implied in his disgruntlement and revealed in precursor security incidents (Melara et al. 2003).

Not being able to assess the relative contribution of the proposed mechanisms (because of the absence of sufficiently complete case descriptions) one way of proceeding is a constructivist approach of taking the policy implications of the various approaches seriously as part of the measures to counteract erosion of compliance. Given that human factors are implicated in 80-90% of security and safety problems, policies derived from theories that make common sense (here, that they are theoretically sound and their BOT is in agreement with observed behavior) should be given a chance in practice: Apart from thus being able to test our confidence in particular theories of human factors in security settings, such policy-driven approach would have two advantages: 1) They are likely be cheaper than further advances in protective technology at nearly any cost. 2) They might have high leverage, given that human failure is a ubiquitous aspect of security problems. 3) If they work they would strengthen our confidence in the theory of human factors behind the approach.

Among the main reasons for the erosion of compliance we propose learning – or rather 'superstitious' learning (Hogarth 1987; Sterman 1997). The driving mechanism for 'superstitious' learning and, hence, for the erosion of compliance is risk misperception. The phenomenon tying risk misperception and 'superstitious' learning is instrumental (a.k.a. operant) conditioning. This paper presents system dynamics models of the basics of instrumental conditioning and of risk-modulated erosion of compliance through an instrumental conditioning mechanism. The behavior reference mode is the "unrocked boat" pattern (see *Introduction* section), i.e. a homeostatic process of erosion of compliance: Organizations become accustomed to their apparently safe state, thus misperceiving risk and allowing themselves to drift into regions of greater vulnerability, until (near) accidents temporarily induce greater risk awareness. The resulting pattern is irregular oscillations, often leading to disaster. Figure 1 illustrates the (simplified) reference behavior mode.

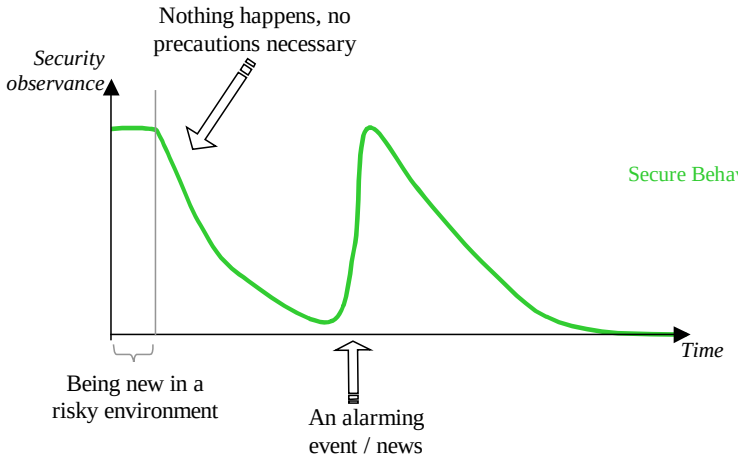


Figure 1 The "unrocked boat" pattern as reference behavior mode.

We will show below that our theory of risk-modulated erosion of compliance through an instrumental conditioning mechanism is able to render the reference behavior mode of Figure 1 – but so are other approaches, at least qualitatively. A very interesting issue is to what degree our proposed mechanism of risk-modulated erosion of compliance through instrumental *learning*[4] is a competing mechanism to erosion of compliance induced by, say, a throughput/security priority conflict. We come back to this issue in the *Discussion and conclusion* section.

Before embarking on our modeling task we discuss several popular explanations for erosion of compliance and discuss their strengths and limitations.

Human factors and throughput pressure

In the context of various organizations issues of erosion of protection measures are often linked with those of productivity and profit generation (see e.g. Reason 1997). Typically, an organization would have some throughput and protection objectives. If the objectives are not well attuned, they will have to compete for the same resources – manpower, money, time, etc. In goal-conflict situations, throughput goals usually prevail: Fulfillment of throughput goals delivers relatively instant and tangible results both to employees and organizations, while pursuit of protection goals most often results in *non-events* (i.e. people comply with the prescribed protection measures, yet *nothing* happens). The *non-event outcome* of compliant behavior is far less attention catching than the tangible and well-defined results of throughput-oriented actions. Thus, throughput objectives by and large keep the upper hand in security and safety systems (see e.g. Reason 1997; Weick 1987).

A simple causal loop model (Figure 2) illustrates the mechanism: Assuming an unbalanced definition of throughput and protection goals, maximum compliance will result in the compliance level (*Compliance*) matching *Compliance Goal* and *Throughput* never matching *Throughput Goal*. The only way to close *Throughput Gap* is to reduce *Compliance* and in that way increase resources available for throughput generation (*Currently Available Resources*). The balancing loop operates until *Throughput* reaches *Desired Throughput*. At this point, *Pressure to prioritize throughput goals* is eased and

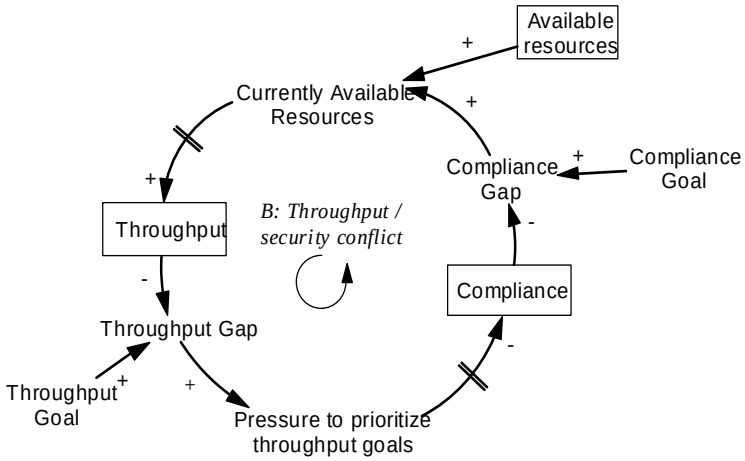


Figure 2 Feedback structure governing the throughput/security goal-conflict situation

[4] Note the emphasis on learning – conditioning is a form of learning.

compliant behavior is re-invoked through the same negative loop. The cycle is iterated resulting in a checkered pattern of compliant and non-compliant behaviors accompanied by lower and higher productivity, respectively.

The simple model assumes that in absence of the strong competing throughput objective, the individual compliance level will be constant over time. The assumption is highly unrealistic. Even if not burdened with throughput goals, people often do not comply with protection measures or change their compliance level regardless of variations in the experienced throughput pressure. The behavioral economics and risk homeostasis theories – discussed in turn – address the issue.

The behavioral economics approach

According to behavioral economics human action is guided by an internal need for minimization of endured costs and maximization of expected benefits (see e.g. McKenzie and Tullock 1975; Navon and Gopher 1979). Thus, in a risky environment a subjective judgment of perceived costs and benefits of compliant action against the costs and benefits of non-compliant behaviors would determine the degree of compliance (see also Battmann and Klumb 1993). The postulated mechanism is illustrated with a simple (linear, i.e. no feedback) causal diagram in Figure 3.

Observance of protection measures is usually more resource-demanding than risky behavior. An individual would be inclined to "invest" extra resources into protective measures only if the benefits expected from compliance exceeded the inferred costs sufficiently; i.e. the cost:benefit ratio associated with compliant behavior is greater that any other associated with non-compliant behavior. Indeed, it has been observed that the higher the cost of compliance with protection measures, the more likely is risky behavior (see e.g. Zeitlin 1994).

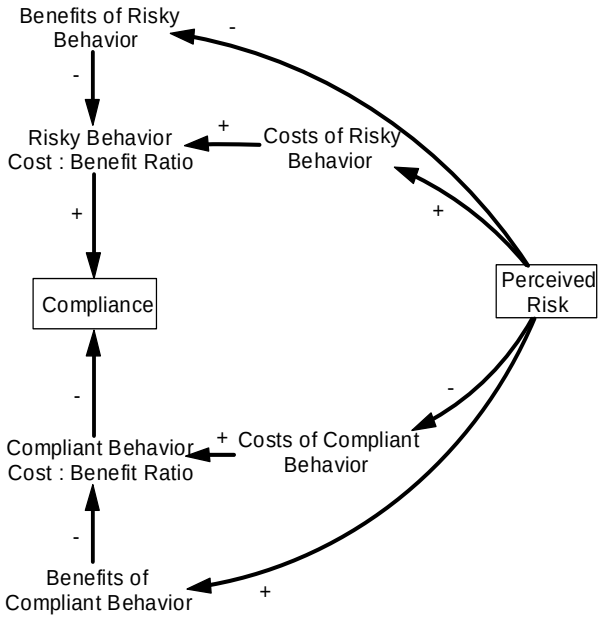


Figure 3 Calculating the optimal action in risky environment according to behavioral economics

While the costs of compliant behavior may usually be estimated quite accurately, the assessment task is much more difficult for the estimation of benefits of compliant behavior or costs and benefits of noncompliant behaviors. The difficulty originates from the impaired human ability to analyze and perceive complex and risky situations. People are poor judges of risk. Research initiated with the formulation of Tversky's and Kahneman's prospect theory shows that people in the face of very unlikely events either overestimate the probability of their occurrence or neglect it at

all (Kahneman and Tversky 2000a, 2000b). This introduces a dangerous bias in people's perception and interpretation of risky situations, where probabilities of disastrous events are usually very low. Underestimation or negligence of risk is likely to result in noncompliant behavior. Research conducted by Estes documents further the problems people have concerning the accurate perception of probabilities. Apparently, people seem to 'derive' probabilities from relative frequencies of events rather than from the actual probabilities with which the event occurred (Estes 1976). Thus they may easily become comfortable with non-compliant behaviors, reasoning that accidents "never" happen. Acquisition of such erroneous beliefs based on personal observations and experience is referred to as superstitious learning (see e.g. Hogarth 1987, p. 230).

Behavioral economics asserts that people are bound to take the path yielding the highest benefit:cost ratio (Battmann and Klumb 1993; see also Hogarth 1987). In this context, accurate assessment of costs and benefits of various action alternatives is decisive. Since most compliant behaviors would have an asymmetrical cost-benefit structure, requiring substantial investments in the short-term run and delivering benefits only in the longer-term, it is crucial that the cost-benefit analysis is conducted using the long-term perspective. The human ability to conduct such analysis is highly questionable: People have great difficulties with correctly inferring results of actions – especially, their long-term results – in complex systems (see e.g. Dörner 1975; Dörner and Reither 1978; Dörner 1980, 1989, 1996; Brehmer and Allard 1991; Sterman 1989).

Behavioral economics explains breaches of protection measures as results of the attractiveness of noncompliant behaviors. In the light of various human cognition limitations, instances of noncompliant behavior should not be expected to be rare events. Noncompliant behavior entails a much greater risk, which apparently is not taken into account when the action choice is made. Behavioral economics provides a plausible framework to explain the variety of instant action choices made by actors in risky situations. However, the framework fails to explicitly discuss mechanisms that could explain the changes over time in compliance level, so prominent in various security and safety systems (see Reason 1997; see also Sawicka and Gonzalez 2003). The risk homeostasis theory may be considered as an extension of the behavioral economics approach in this respect. Note also that this version of the behavioral economics approach assumes instantaneous adjustment to equilibrium, a shortcoming that the dynamic perspective of the risk homeostasis and the instrumental conditioning approach overcome.

The risk homeostasis theory

The risk homeostasis theory was developed in the context of automobile safety (Wilde 1994). This theory considers human behavior as dynamic, governed by a homeostatic adjustment mechanism. Figure 4 reproduces the causal model given as illustration of the suggested adjustment mechanism.

Target Risk is a key variable in the model. The "target risk" is not assumed to be constant: It expresses the currently "preferred, desired, accepted, tolerated and subjectively optimal" level of risk, which varies according to *Perceived costs and*

benefits of action alternatives. The more *Target Risk* exceeds *Perceived Risk*, the riskier the human behavior and, accordingly, the higher *Resulting Accident Loss*. I.e., the environment is perceived as more risky (*Perceived Risk*). Once the environment is perceived as too risky (i.e. *Perceived Risk* > *Target Risk*), an opposite adjustment process is initiated producing a more compliant human behavior.

The suggested behavior regulation mechanism depends on the individual's ability to perceive the actual risk accurately (*Perceptual skills*) and to make a good decision about what sort of adjustment is necessary (*Decision-making skills*). The individual's *Vehicle-handling skills* determine the ultimate effectiveness with which the desired adjustments are carried out.

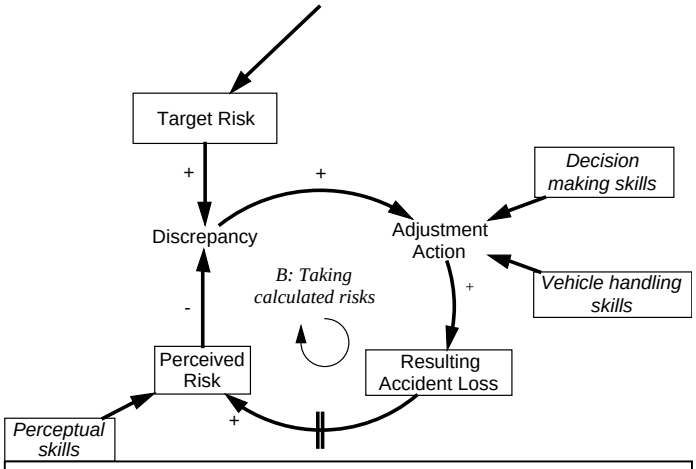


Figure 4 Feedback structure underlying human behavior in risky situations as postulated by the risk homeostasis theory

The model may be easily coupled with the behavioral economics framework through *Perceived costs and benefits of action alternatives* and in that way provide a more comprehensive feedback structure describing the human behavior adjustment mechanism.[5]

The "homeostasis risk theory" points clearly toward a dynamic nature of human behavior in security systems. Although the model offers a plausible causal framework for general analysis of human factors, it fails to explore more detailed issues. E.g. it is unclear whether there is any difference in pace at which compliant or noncompliant behaviors are obtained.[6]

An insight into this question may be gained by referring to theories of conditioning. Drawing on these theories we develop in the following section an alternative model of human behavior in security systems.

Erosion of compliance as risk-modulated instrumental conditioning

Learning is frequently based on noting that events occur closely together – for example, in time. An example is the ability of children to learn the rules of grammar: By observation and experiment on noting co-occurrences, children acquire schemes capable of generating quite complex behavior. But cues-to-causality such as co-variation to infer, and 'learn' causal relations in the environment, may be erroneous in

[5] See Ch. 4.1 in Wilde (1994) for discussion of how the "target risk" is assessed.
[6] Indeed, it is even suggested that the compliance acquisition and attrition rates would be symmetrical. (see Figure 2.2 in Wilde 1994)

particular instances and lead to the acquisition of superstitious beliefs, with potential for severe human error – learning of falsehoods, "superstitious learning" (Hogarth 1987, p. 229-30).

Skinner (1948) showed in his famous paper "'Superstition' in the pigeon" that coincidences would condition pigeons to exhibit any kind of strange behavior as a consequence of being fed automatically by a timer, completely independent of the pigeon's actions. "Every fifteen seconds, food would appear. Although the most efficient strategy might be to perch in front of the feeder and wait patiently for it to turn on, Skinner's pigeons were very active. After a few minutes in the [experimental] chamber, each bird developed a distinctive ritual. One walked in circles, making two or three revolutions between reinforcements [e.g. food appearing]; another rapidly thrust its head into one of the upper corners of the apparatus. Still others bobbed their heads up and down, as if trying to keep an invisible soccer ball aloft. These peculiar behaviors were created by simple temporal contiguity… the accidental pairing of some random act of the pigeon with the presentation of food was enough to reinforce these idiosyncratic behaviors" (Vyse 1997, p. 70-1).

Many scientists were skeptical of Skinner's claim that human superstitious behavior could be equated to idiosyncratic behavior by pigeons, cats (Guthrie and Horton 1946) or other animals. As alternative explanation for such strange behavior of Skinner's pigeons it was argued that the birds filled the time between feeding with not learned behavior, i.e. that Skinner had mistaken instinct with conditioning. Others could not accept that complex human superstition could be explained by simple conditioning (reported in Vyse 1997, p. 71-2). Today the issue seems settled after startling experiments with children (Wagner and Morris 1987; see also Vyse 1997, p. 72-3) and adults (Ono 1987; see also Vyse 1997, p. 73-4) in which people develop idiosyncratic, superstitious behavior by pure coincidences as if their behavior would influence a completely automatic and independent mechanism.

Reporting about Ono's results (Ono 1987), Vyse concludes: "Not all of Ono's university students developed superstitious behavior but *most* [our emphasis] did" (Vyse 1997, p. 74). All the above illustrates the power of coincidence – contiguity in time and space of different events – to shape human behavior. As Vyse states (1997, p. 60): "That human beings are extremely sensitive to coincidence is both an often overlooked psychological truth and a monumental understatement. When important events happen together, they can change our behavior, alter our thought processes, and lift or dash our spirits."

A security culture requires that people be aware of threats, whether due by malice, error or mischance. Risk perception influences people behavior even in its absence – by seemingly "proving" that careless behavior is appropriate. In fact, risk perception is highly volatile and its influence on behavior is conspicuous. Everybody has read numerous newspaper reports on change of risk-related behavior following alarming stories – followed by rapid return to business as usual. A pattern repeatedly observed in European countries has been consumer's shunning of beef ensuing reports on "mad cow disease" with subsequent return to normal beef consume when new topics

catch media attention – although the objective risk has not declined in the meantime. Accordingly, it should make sense to study how volatile risk perception shapes human compliance. In fact, we claim that while other potential influences (e.g. throughput pressure) may or may not be present in a particular setting, the high volatility of risk perception makes this parameter indispensable for theories of human compliance with security regulations.

Several authors have argued that the erosion of compliance is driven by a reinforcement mechanism (see e.g. Battmann and Klumb 1993; Dörner 1989, 1996; Gonzalez 1995). Dörner (1996, p. 31) expresses this mechanism (in connection with the disaster at the nuclear reactor in Chernobyl) so: "Another likely reason for this violation of the safety rules was that operators had frequently violated them before. But as learning theory tells us, breaking safety rules is usually reinforced, which is to say, it pays off. Its immediate consequence is only that the violator is rid of the encumbrance the rules impose and can act more freely. Safety rules are usually devised in such a way that a violator will not be instantly blown sky high, injured or harmed in any other way but will instantly find that his life is made easier."

Reinforcement of security breaches as mechanism behind the erosion of compliance is intuitively appealing, but the accepted paradigm for instrumental conditioning, the behavior regulation theory, leads to an interpretation differing from the above explanation in subtle ways (cf. the *Discussion and conclusion* section).

The behavioral regulation approach

In the proposed model of human behavior in relation to security we couple the behavioral regulation approach to instrumental conditioning (Allison 1989; Timberlake 1980, 1984) with the dynamics of risk perception (see discussion in *The behavioral economics approach* section). Our work is related to erosion of protection measures toward HIV-infection conducted by Gonzalez (Gonzalez 1995, 2002b) and it represents an extension of previous work on instrumental conditioning based on the behavioral regulation approach (Gonzalez and Sawicka 2003b) to compliance with security procedures (see also Gonzalez 2002a; Gonzalez and Sawicka 2002, 2003a).

Instrumental conditioning is learning through consequences: Behavior yielding positive results (high "instrumental response") is reinforced, and that producing negative effects (low "instrumental response") is weakened. For conditioning to occur, these requirements must be satisfied: (1) A contingency between a highly desirable event ("reinforcer") and one perceived by the subject as less desirable ("instrumental response"). (2) Contiguity between instrumental response and reinforcer (Domjan 2000).

The terminology of psychological conditioning is somewhat confusing. First, the term "reinforcer", traditionally defined as "a stimulus whose delivery shortly following a response increases the future probability of that response" (see glossary, p. 209, in Domjan 2000) is an old term that can be misleading. Among other issues, *responses*, not just stimuli, can serve as "reinforcers" (Domjan 2000, p. 125ff), implying that a wide range of pairings between different psychological events can

result in learning by instrumental conditioning. In fact, in many cases fondness for a particular hypothesis seems to be sufficient to get sensitized and conditioned by more or less fortuitous events "confirming" the hypothesis. Second, the term reinforcer contradicts the usual logic of system dynamics in that – as we will see below – the effect of the reinforcer is to drive a *negative* feedback loop leading to increase of instrumental response toward a goal.

To eliminate misunderstandings we use a dual terminology, pairing the abstract concepts reinforcer (R) and instrumental response (IR) with concrete psychological responses (viz. time devoted to music listening and school work) in a specific example.

According to the behavior regulation theory of instrumental conditioning (Allison 1989; Timberlake 1980) each individual has a preferred distribution of activities – the "behavioral bliss point." The behavioral regulation approach borrows ideas from physiology (the concept of homeostasis), behavioral instigation (response choice), control theory and behavioral economics. Behavioral homeostasis is analogous to physiological homeostasis in that both involve defending the optimal or preferred level of a system. Physiological homeostasis means keeping physiological parameters (blood levels of oxygen and glucose, e.g.) close to an optimal or ideal level. The homeostatic level is "defended" in the sense that deviations from the target levels trigger compensatory physiological mechanisms that return the system to their respective homeostatic levels. In behavioral regulation, what is defended is the organism's preferred distribution of activities, its *behavioral bliss point*. Behavioral bliss point is a term borrowed from behavioral economics. In the framework of response choice, the behavioral bliss point corresponds to so-called baseline levels. In control theory one would speak of set points. In system dynamics, the behavioral bliss point would encompass the "desired values" or goals of the negative feedback loops describing the response of the individual in a constrained situation.

In a classroom example of instrumental conditioning – Kim's case (Domjan 2000, Ch. 8) – a teenager ("Kim") has two activities after school. She spends ½ hour a day for school work whereas she devotes 3 hours a day listening to music: Kim's behavioral bliss point is the point {½ hr, 3 hr} in activity space. To increase the amount of time Kim spends doing school work her parents introduce an instrumental condition-

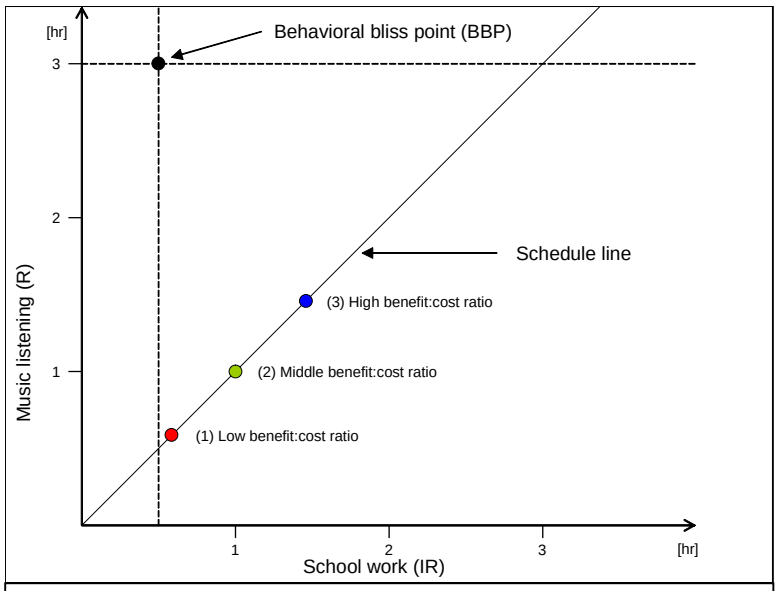


Figure 5 Behavioral bliss point, schedule line and conditioning results depending on benefits:cost ratios.

ing procedure: They enforce that Kim spends a given amount of time on school work before her being allowed to spend an equal amount of time listening to music. Knowing that successful conditioning requires contiguity they make sure that the reinforcer – music listening – follows immediately after the instrumental response – school work.

The 1:1 "planned activity ratio" is a constraint on Kim's preferences for the available response alternatives. In the absence of other response options Kim will opt for doing a total of X hours of school work, "earning" her X hours of music listening. The behavioral regulation theory predicts that Kim's choice will be on the "schedule line" (here a 1:1 distribution of the two activities) but the precise conditioning result (i.e. the actual value of X) will be dependent on the cost and benefits of the various options (Figure 5).

Model of Kim's case

We give a description of basic system dynamics models of instrumental conditioning, referring to Gonzalez and Sawicka (2003b) for more details (see Gonzalez 2002a; 2002b for preliminary versions).[7]

As a first step we define basic parameters of the model, viz. '*Behavioral Bliss Point*', '*Instrumental Response at BBP*', '*Reinforcer at BBP*', '*Activity ratio at BBP*' and '*Free daily time*':

'*Behavioral Bliss Point*' (a constant array) describes Kim's preferred distribution of activities in her free time (0.5 hr school work and 3 hr music listening per day):

'*Behavioral Bliss Point*'= {0.5,3.0} <<hr>>

'*Instrumental Response at BBP*' and '*Reinforcer at BBP*' are the two components in the constant array and '*Activity ratio at BBP*' is the ratio of these components:

'Instrumental Response at BBP' = 'Behavioral Bliss Point'['School Work']

'Reinforcer at BBP'= 'Behavioral Bliss Point'['Music Listening']

'Activity ratio at BBP' = 'Instrumental Response at BBP'/'Reinforcer at BBP'

Finally, '*Free daily time*' is the total daily number of hours left after sleeping, eating and time at school:

'Free daily time' = 'Reinforcer at BBP'+'Instrumental Response at BBP'

'*Planned activity ratio*' – in previous versions called "instrumental contingency" – is the 1:1 constraint enforced by the instrumental procedure:

'*Planned activity ratio*'= 1 // Imposed ratio IR:R, i.e. "school work" : "music listening"

[7] This said, note that the present version of the models – though equal in content – manifestly express the role of the reinforcer as driving force of the instrumental conditioning in the stock and flow diagram.

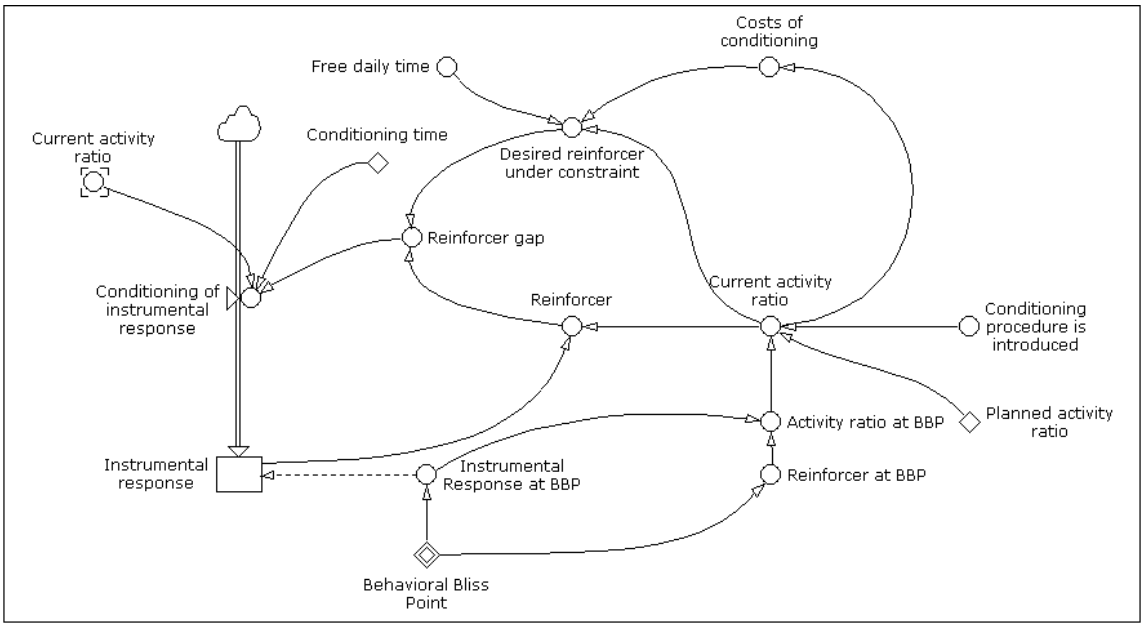


Figure 6 Basic model of instrumental conditioning.

Figure 6 shows a basic model of Kim's case. It has just a balancing loop, involving the variables '*Instrumental response*', *Reinforcer*, '*Reinforcer gap*' and '*Conditioning of instrumental response*'. The goal of the loop is determined by '*Desired reinforcer under constraint*' (i.e. the goal for '*Instrumental response*' follows from it, see below).

We give the definition of the main variables of the Powersim Studio model:

'*Instrumental Response*' = *'Instrumental Response at BBP*' + dt·' *Conditioning of instrumental response*'
'*Reinforcer*' = *'Instrumental response'/'Current activity ratio'*

where '*Current activity ratio*' equals '*Activity ratio at BBP*' before and '*Planned activity ratio*' after the conditioning procedure is introduced (defined by '*Conditioning procedure is introduced*').

'*Desired reinforcer under constraint* ' = *'Free daily time'/(1 + 'Current activity ratio')/'Costs of conditioning''*

where '*Cost of conditioning*' expresses how much Kim resents having to spend more time on school work rather than pursuing her favorite leisure time occupation (music listening).[8]

'Reinforcer gap' = 'Desired reinforcer under constraint' – Reinforcer
'Conditioning of instrumental response' = ('Reinforcer gap''Current activity ratio')/'Conditioning time'*

[8] We refer the reader to (Gonzalez and Sawicka 2003a) for more details.

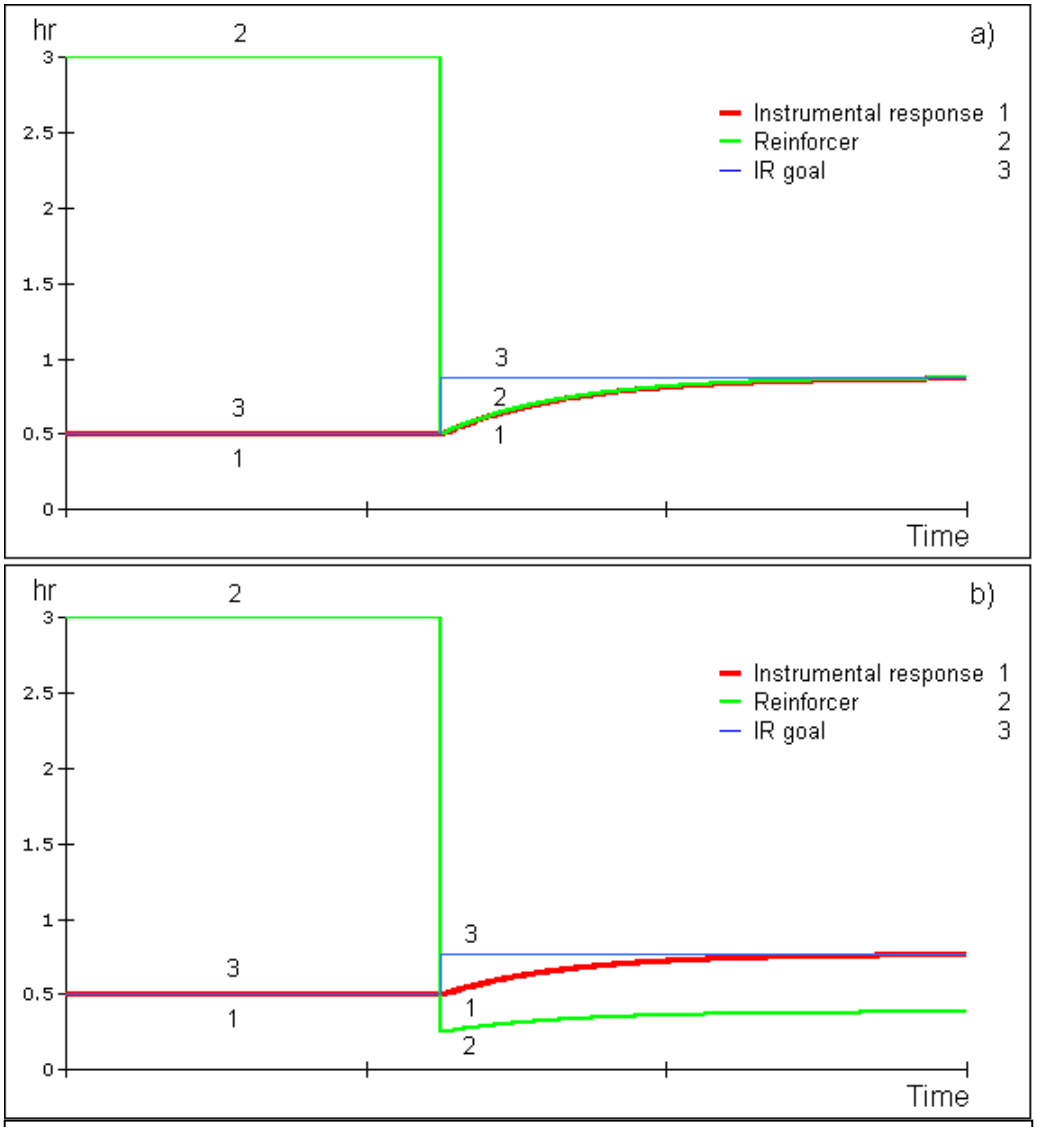


Figure 7 Behavior over time of the basic model. Planned activity ratio: a) 1:1; b) 2:1. Notice that higher costs for case b) actually *reduce* the outcome (lower IR than in case a).

Figure 7 displays the behavior over time for two choices of the planned activity ratio, a) 1 (1:1 relation between instrumental contingency and reinforcer) and b) 2 (2:1 relation between instrumental contingency and reinforcer). Notice how the value of the reinforcer (music listening) initially drops and then follows the value of the instrumental response (school work) in the relation enforced by the instrumental contingency, until Kim is fully conditioned ('*Instrumental response*' approaches its limit asymptotically).

We now extend the basic model to describe extinction of conditioned behavior. Ignorant of the subtleties of instrumental conditioning, and because sustenance of the instrumental contingency incurs costs (time, effort, possibly money), Kim's parents will lift the instrumental contingency when they perceive their daughter as fully conditioned. Extinction of the conditioned behavior sets on, implying that Kim's behavior approaches her behavioral bliss point. On noticing this, Kim's parents

reinstall the instrumental conditioning procedure and the story repeats itself. Accordingly, one would expect "homeostatic" oscillations in the level of instrumental response.

We approach this issue in two steps: First, by explaining the sector of the extended model dealing with both aspects of instrumental conditioning, viz. LEARNING AND EXTINCTION OF CONDITIONED BEHAVIOR. Second, by describing the PERCEPTION sector, i.e. the sector dealing how Kim and her parents perceive the situation and act according to their perception.

The sector LEARNING AND EXTINCTION OF CONDITIONED BEHAVIOR is shown below (Figure 8). Comparing with Figure 6 one sees that the main differences from the simple model of instrumental conditioning are 1) the outflow '*Extinction of instrumental response*' with its associated parameters ('*IR Extinction goal*'[9], '*Extinction time*' and the '*Extinction switch*') that determines if conditioned behavior is being extinguished; 2) the new '*Reinforcing switch*', which determines if instrumental conditioning is occurring; and 3) the PERCEPTION sector, which will be described in detail in Figure 10.

'*Reinforcing switch*' is unity and '*Extinction switch*' zero when Kim's parents enforce the instrumental conditioning procedure and the converse ('*Reinforcing switch*' = 0 and '*Extinction switch*' = 1) when Kim's parents – misled by their faulty perception that Kim's higher dedication to school work is entrenched – do not monitor Kim's actual compliance and Kim notices her parents' lack of attention.

The actual definitions of these parameters are:

'Extinction switch' = IF('Instrumental Response'-'IR Extinction goal'>0 <<hr>>,1,0)

'Reinforcing switch' = 1-'Extinction switch'

'IR Extinction goal' = ('Current activity ratio'/(1+'Current activity ratio'))'Free daily time'/'Costs of conditioning'*

where the expression ('*Current activity ratio*'/(*1+'Current activity ratio*'))*'*Free daily time*' is derived from the definition '*Time to activity A*' / '*Time to activity B*' = '*Current activity ratio*'. Of course, A stands for school work (IR) and B for music listening (R).

We assume that extinction (forgetting) takes much longer time, on average 50 hours, than learning (instrumental conditioning), 10 hours. Empirical evidence does indeed show that conditioned responses can last for very long time (indeed, even for years). For more details about model equations, see the enclosed, fully documented Powersim Studio model or the text model file at http://ikt.hia.no/josejg.

[9] Remember that IR stands for Instrumental Response.

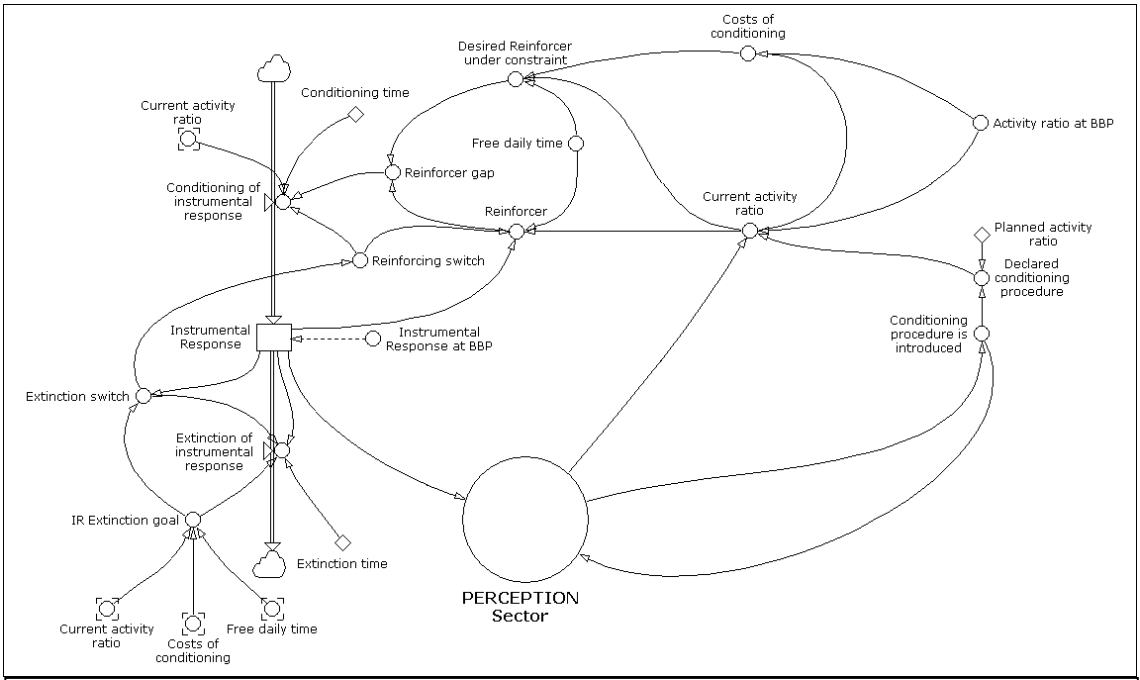


Figure 8 The sector LEARNING AND EXTINCTION OF CONDITIONED BEHAVIOR.

Forgetting for a moment about the interaction between the sectors LEARNING AND EXTINCTION OF CONDITIONED BEHAVIOR and PERCEPTION, the basic behavior of learning with subsequent extinction of conditioned behavior would be as shown in Figure 9.

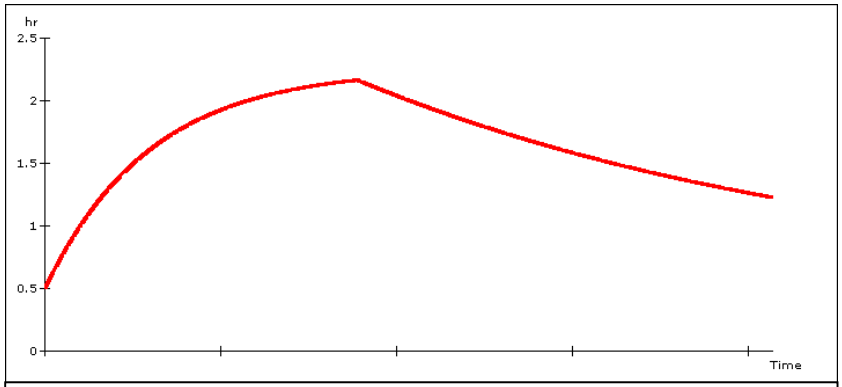


Figure 9 Learning and extinction of instrumentally conditioned behavior.

We turn now our attention to the PERCEPTION sector (Figure 10). Kim's parents perceive the conditioning success with a delay, modeled as a first order information delay ('smoothing'):

'Perception delay' = 10 <<hr>>

'Perceived success of conditioning' = DELAYINF('Success of conditioning','Perception delay',1)

'Success of conditioning' = 'Instrumental Response' DIVZ0 'Min planned IR'

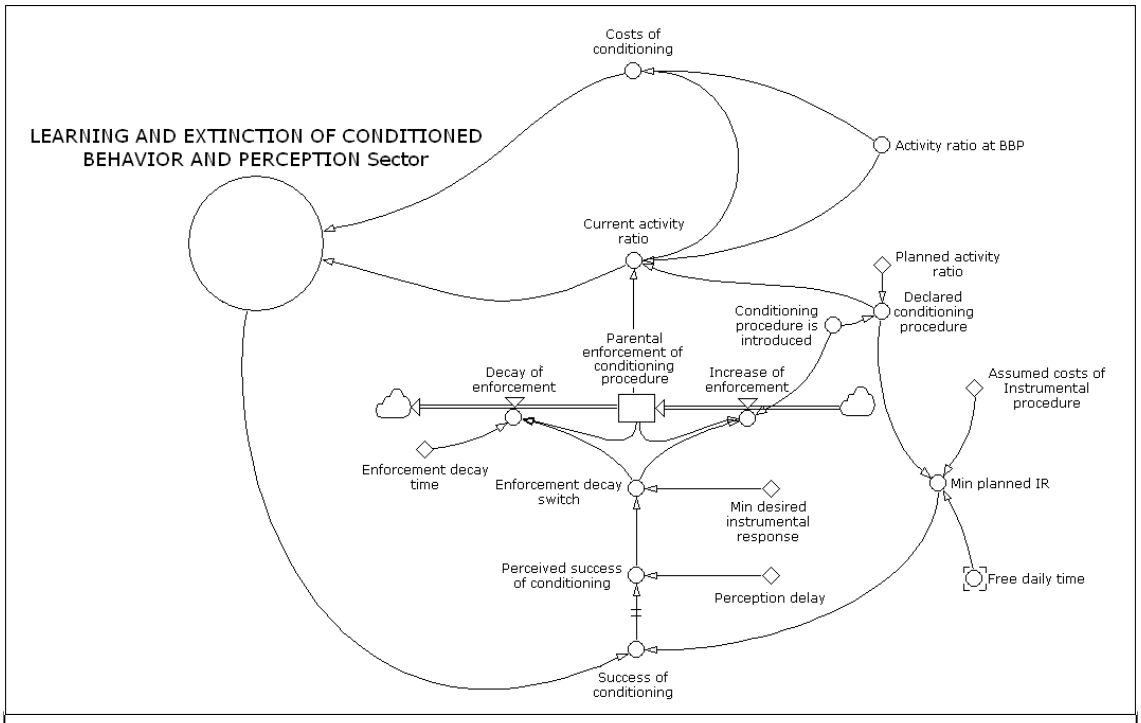


Figure 10 The PERCEPTION sector.

Note that '*Success of conditioning*' is a dimensionless number between zero and unity and that the *DIVZ0* ensures the correct result if the divisor were zero. '*Min planned IR*' indicates what Kim's parents estimate as minimum level of instrumental response (IR) as result of the instrumental conditioning process (depending on their estimate of the "costs" for Kim of the instrumental procedure).

When '*Perceived success of conditioning*' exceeds '*Min desired instrumental response*' (here defined as 0.9) Kim's parents stop monitoring Kim – expressed in the model in that the stock '*Parental enforcement of conditioning procedure*' depletes through the outflow '*Decay of enforcement*' with time constant '*Enforcement decay time*', here 10 hours. As Kim's instrumental response decays, so does her compliance with the imposed instrumental procedure. When her parents discover Kim's breach of compliance – again with the mentioned perception delay – they enforce the instrumental conditioning procedure again and Kim complains again (the inflow '*Increase of enforcement*' restores the maximum enforcement, viz. unity, instantaneously). Again, we refer for details to the enclosed, fully documented Powersim Studio model or the text model file at http://ikt.hia.no/josejg.

Not surprisingly Kim's dedication to school work (instrumental response) and her music listening (acting as reinforcer) oscillate. The origin of such homeostatic oscillations is the volatility of the enforcement of the instrumental procedure tied to the delayed reaction of Kim's parents her breaches of compliance. A similar homeostatic behavior we will see for the behavior of compliance. The reason will again be that the strength of the instrumental procedure fluctuates.

For a more detailed discussion of the behavior over time, including an explanation of the details in the shape of the reinforcer (time devoted to music listening) cf. Gonzalez & Sawicka (2003b). Note, however, that in this version of the model Kim's

parents do not start with the instrumental conditioning procedure at once, but rather 30 hours into the time horizon considered.

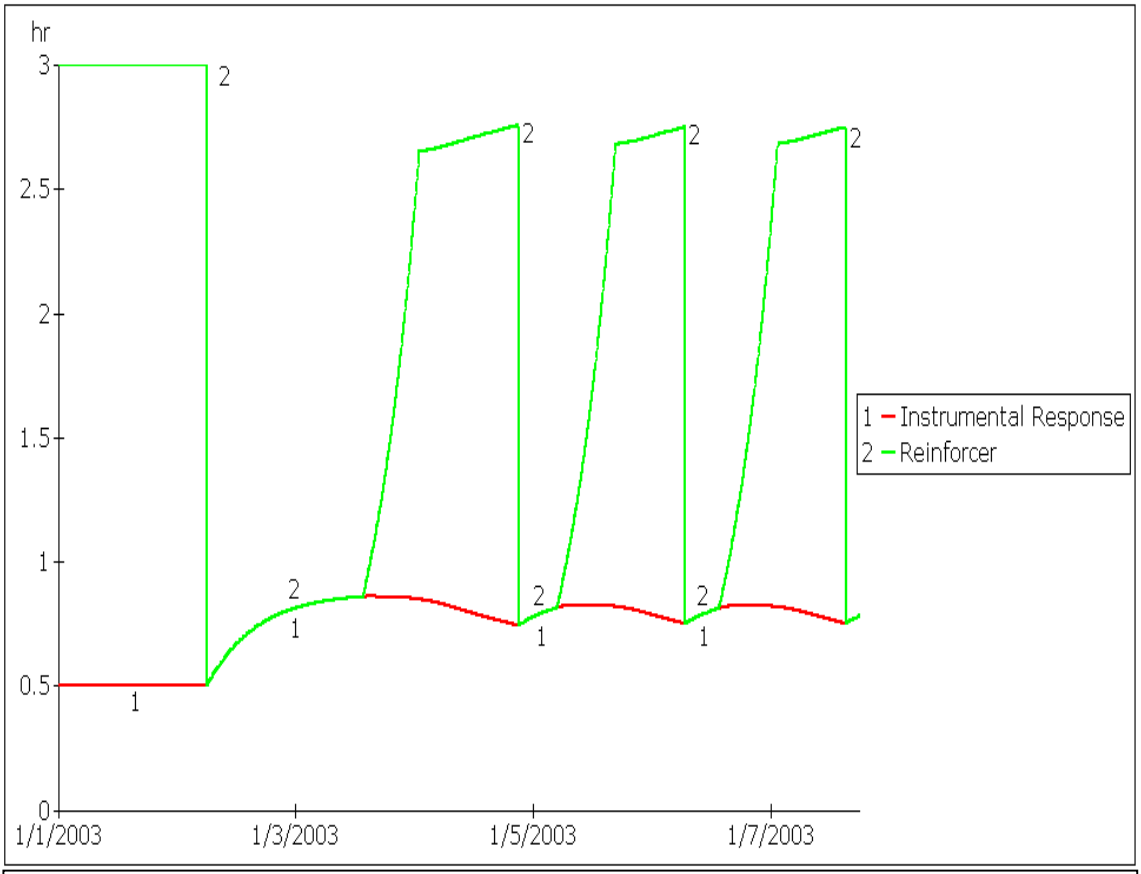


Figure 11 Homeostatic oscillations in Kim's model with learning and extinction of conditioned behavior. Note that Kim's instrumental response – dedication to school work – is a measure of her compliance.

Compliance with security as instrumental conditioning phenomenon

To be specific we consider an environment concerned with information security. Assume now that Kim has become adult and she works in a university. Kim has become accustomed to a low level of risk and her behavioral bliss point is to dedicate most of her time to interesting tasks and spend only a time slot every 14 days to security-related issues (virus scanning, updates, patches, etc.). We call this security-related activity a "task." But since July 1, 2002, Kim's university has become a popular target for hackers. More stringent security procedures are introduced and Kim complies – in the beginning – with the prescribed security measures of executing one security-related task a day (we called this the "prescribed compliance level"). Such measures prevent security breakdown (security failures will not happen if security measures stay above a certain threshold, implying keeping the risk below the "security failure zone").

In the current context, compliant behavior can be interpreted as instrumental response. Assuming that the perceived level of risk guides the individual's choice of

compliance level, risk perception may be understood as a natural instrumental conditioning procedure modulating compliance. Indeed, the feeling of risk causes anxiety, and the feeling of being protected relieves anxiety. Accordingly, it is natural to assume that the "reinforcer" is the well-being associated with feeling protected from external risks. Note that in the model describing Kim's compliance with parental demands (previous section) the parents' enforcement of the conditioning procedure plays an analogous role as risk in the present model for compliance with security measures.

The time horizon we consider is relatively short. Instrumental conditioning is low level learning and it is not likely to be the sole mechanism at work. It might dominate for a while, but the "unrocked boat" experience (Figure 1) will hopefully induce higher order learning, implying a gradual change in the behavioral bliss point. E.g., Kim as a teenager might get good grades because of her doing more school work. That might increase her liking of school subjects, boost her motivation and self-confidence, and change her preferred distribution of activities. As an adult, the chronic problems associated with the "unrocked boat pattern" might over time lead to reflection, insight and sustainable changes in Kim's attitudes toward security procedures, again changing her behavioral bliss point.

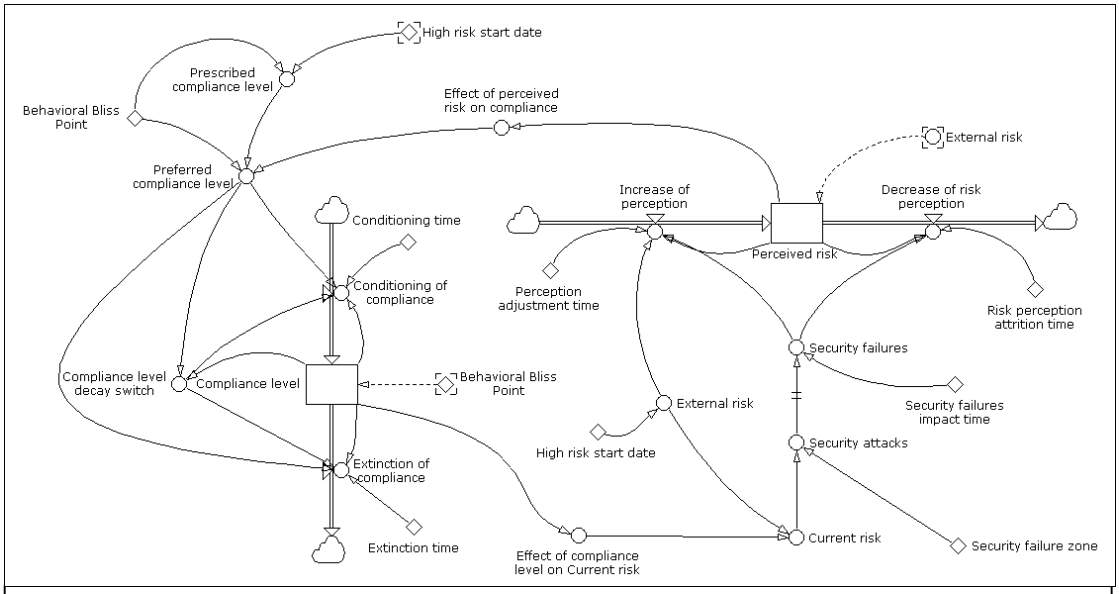


Figure 12 Model of risk-modulated compliance with security prescriptions.

The model is shown in Figure 12. The variables of main interest are the two stocks '*Compliance level*' and Kim's risk-perception ('*Perceived risk*'). The former is a measure of security – the more compliant Kim is, the higher the security level. The second influences Kim's behavior in the sense of an instrumental conditioning procedure, tying her perception of risk and her instrumental response (her dedication to security). The model does not explicitly show the reinforcer – sense of feeling safe from risks – but the variable '*Effect of perceived risk on compliance*' encapsulates its effect by mediating between risk perception (acting as instrumental conditioning

procedure) and the compliance level (instrumental response), measured in terms of how many security-related tasks Kim executes per day.

'*External risk*' is an external parameter describing low risk before July 1, 2002, and high risk afterward:

'External risk' = IF(TIME < 'High risk start date', 0 <<rsk>>, 1 <<rsk>>)
'High risk start date' = STARTTIME + 1 <<yr>>
STARTTIME = 7/1/2001

Notice that risk is defined in terms of arbitrary risk units *<<rsk>>* on a scale between 0 (no risk) and 1 (maximum risk).

'*Prescribed compliance level*' is affected by '*External risk*': Before July 1, 2002 we assume that '*Prescribed compliance level*' corresponds to Kim's behavioral bliss point (1 security-related task per 14 days); afterward it becomes 1 task/day.

'Prescribed compliance level' = IF(TIME < 'High risk start date', 'Behavioral Bliss Point', 1 <<tsk/da>>)

'*External risk*' and '*Compliance level*' jointly determine '*Current risk*'. For a given external risk, the lower the compliance level (defined as the actual number of security-related tasks executed per day), the higher the probability that a security failure occurs. (In this connection, a security failure means a major security breakdown as result of an attack.)

*'Current risk' = 'External risk' * 'Effect of compliance level on Current risk'*

'*Perceived risk*' is a stock describing Kim's perception of risk that is changed by two flows, one increasing risk perception when security failures happen and another decreasing risk perception during the periods when security failures do not happen. Both processes take time and their time constants are likely to be different.

*'External risk' + dt * 'Increase of perception' - dt * 'Decrease of risk perception'*

'*Perceived risk*' affects Kim's '*Preferred compliance level*' through '*Effect of perceived risk on compliance*'. Provided that '*Preferred compliance level*' is above the current value of the stock '*Compliance level*', the value of the stock is increased by an inflow describing the instrumental conditioning effect from sufficiently high risk perception.

'Effect of perceived risk on compliance' = GRAPH('Perceived risk',0 <<rsk>>,0.1 <<rsk>>,{0,0.01,0.03,0.1,0.3,0.5,0.7,0.9,0.97,0.99,1//Min:-0.1;Max:1.1//})

*'Preferred compliance level' = 'Behavioral Bliss Point' + ('Prescribed compliance level' - 'Behavioral Bliss Point') * 'Effect of perceived risk on compliance'*

where:

'Behavioral Bliss Point' = 1 <<tsk/da>>/14

As '*Perceived risk*' declines, so does the strength of the instrumental conditioning procedure. When '*Preferred compliance level*' drops below the value of '*Compliance level*', the stock is depleted by an outflow describing the extinction of conditioned behavior (i.e. return to the behavioral bliss point). We assume that extinction (forgetting) takes much longer time, on average 1 year, than learning (instrumental conditioning), 1 week (see remark on empirical evidence in the previous section).

*'Compliance level' = 'Behavioral Bliss Point' + dt * 'Conditioning of compliance' – dt * 'Extinction of compliance'*

The value of '*Compliance level decay switch*' determines whether extinction or conditioning of compliance occurs:

'Compliance level decay switch' = IF('Preferred compliance level'<'Compliance level',1,0)

*'Conditioning of compliance' = (1- Compliance level decay switch') * ('Preferred compliance level'- 'Compliance level')/'Conditioning time'*

'Extinction of compliance' = 'Compliance level decay switch'('Compliance level'-'Preferred compliance level')/'Extinction time'*

For the definition of the remaining variables we refer to the enclosed, fully documented Powersim Studio model or the text model file found at http://ikt.hia.no/josejg.

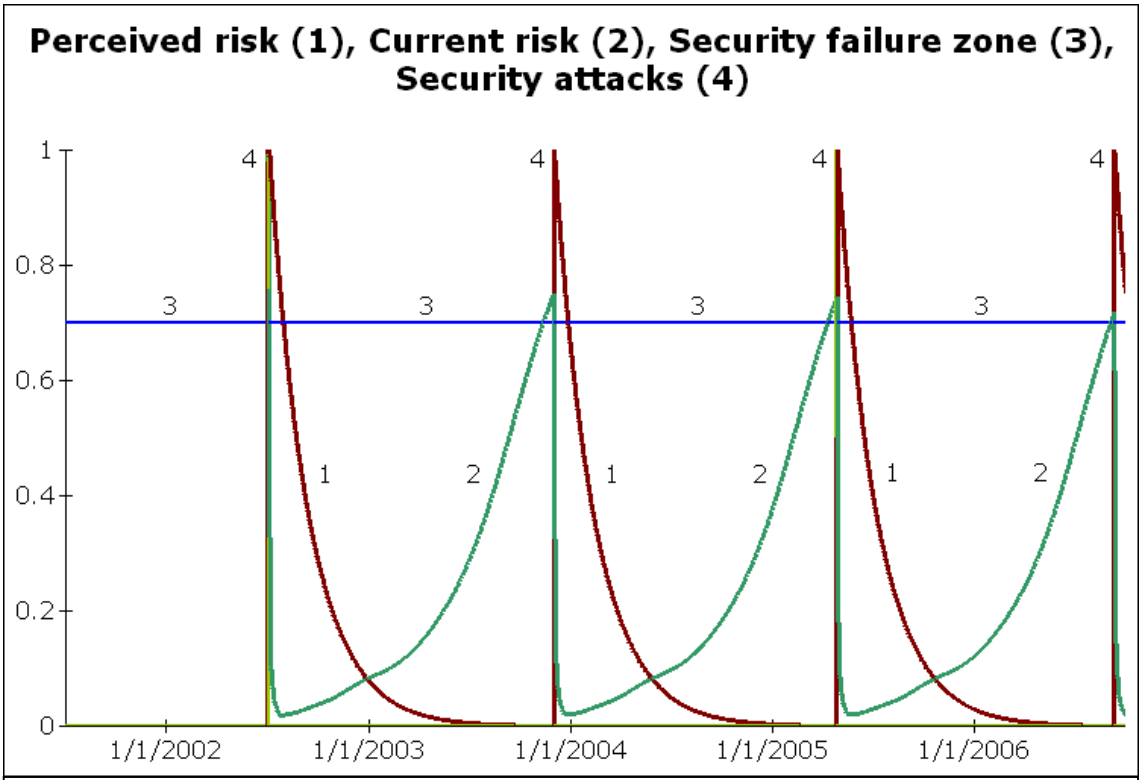


Figure 13 Actual (current) risk and perceived risk are at odds for most of the time. Attacks succeed once the current risk exceeds a threshold ('Security failure zone').

Figure 13 above shows the behavior of '*Current risk*' and '*Perceived risk*' and the occurrence of security failures once '*Current risk*' exceeds a threshold ('*Security failure zone*'). Due to a stochastic element (regulated by the probability that an attack succeeds) the duration of "risk perception cycles" is variable. During a cycle, risk is misperceived as too low for most of the time. It is well-known that most people have problems to estimate risk correctly (Kahneman and Tversky 2000a, 2000b).

Figure 14 illustrates the behavior of actual and preferred compliance level. '*Preferred compliance level*' is strongly influenced by the occurrence of security failures. Due to an assumed long time constant for the extinction of conditioned behavior and the low probability of security failures the actual compliance level decays slowly (lags behind).

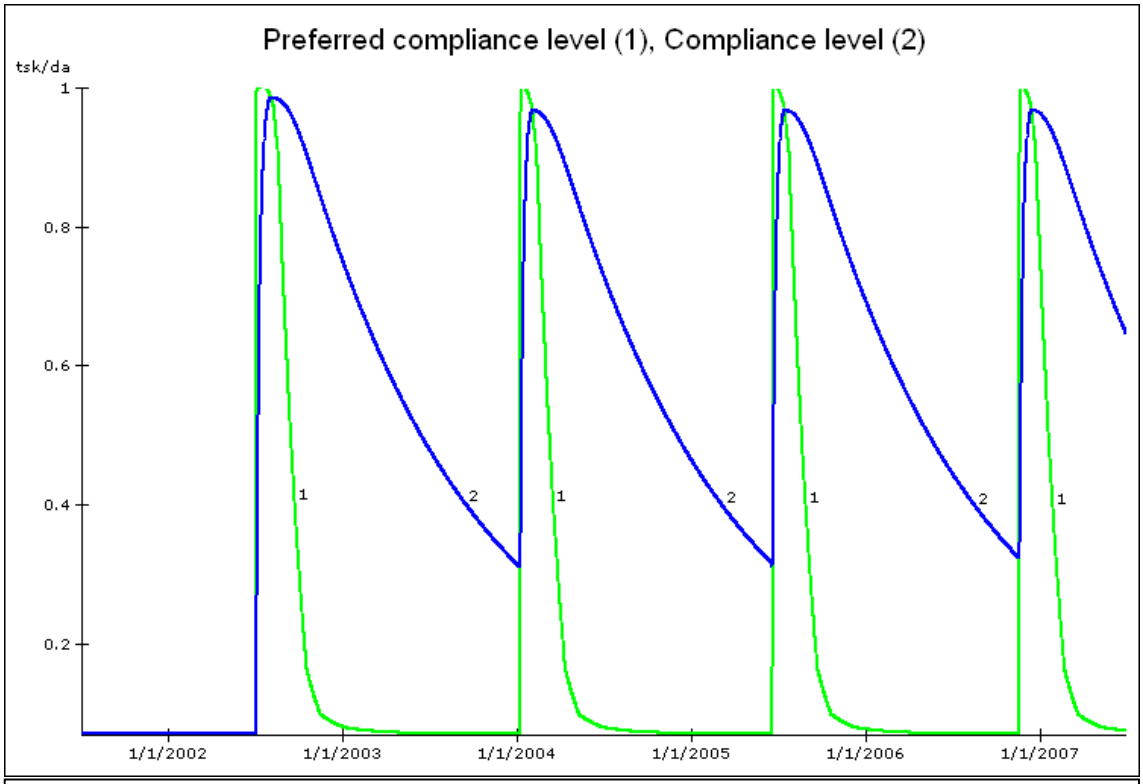


Figure 14 Behavior over time of preferred and actual compliance level.

Analysis of model behavior

In Figure 15 the behavior of preferred and actual security level is shown for a risk cycle. One can distinguish two zones in a "risk perception cycle", depending on whether '*Preferred compliance level*'>'*Compliance level*' or '*Preferred compliance level*'<'*Compliance level*'. The first case is the "conditioning zone" – the subject's risk perception correctly leads to reinforcement of compliance;[10] the second one is the "extinction (of conditioned compliance) zone" – and this has quite troublesome and counterintuitive aspects. Indeed, conditioning of compliance only occurs during a short interval in a cycle. Misperception of risk and the rare success of attacks even when compliance is low – modern technology is forgiving – act during a much longer interval to slowly extinguish conditioned behavior, promoting noncompliance.

Why is the zone of conditioning (learning) of compliance short and the zone of extinction of compliance correspondingly long? And why is this a problem? The answer to the second question should be straightforward: In the extinction zone one has contiguity between noncompliant behavior and lack of security failures – due to the very success of modern security technology that wards off most attacks (modern security technology is a victim of its own success). Accordingly, the "extinction zone" is a favorable setting for "superstitious learning" (Hogarth 1987, p. 229-30; Sterman 1997).

[10] Remember that we are equating the security level – measured in terms of security-related tasks per day – with Kim's compliance with the prescribed security measures.

The answer to the first question is compounded: First, instrumental conditioned behavior is much more persistent if the reinforcement schedule is "partial", i.e. reinforcement is not given every time (Domjan 2000, p. 113ff) – and this is likely to be the case in a normal working environment where various demands and time pressures might interfere with delivery of reinforcement (here in the satisfactory sense of feeling safe from risk). Second, the low probability of successful attack in modern information security settings means that noncompliance can occur for long time without apparent negative consequences. In other words, the forgiving nature of modern security technology makes the zone of extinction of conditioned compliance comparatively long thus promoting and sustaining "superstitious learning" – wrong inferences about risk, consequences of risk and the impact of noncompliance (cf. Figure 15).

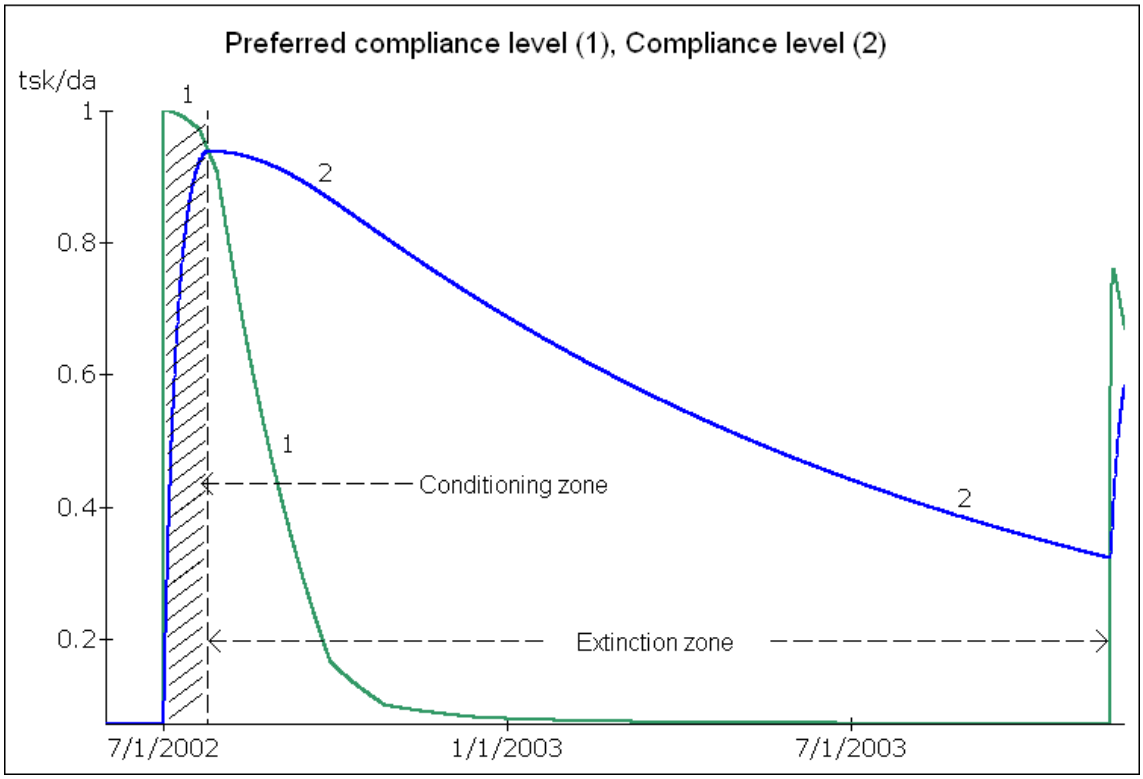
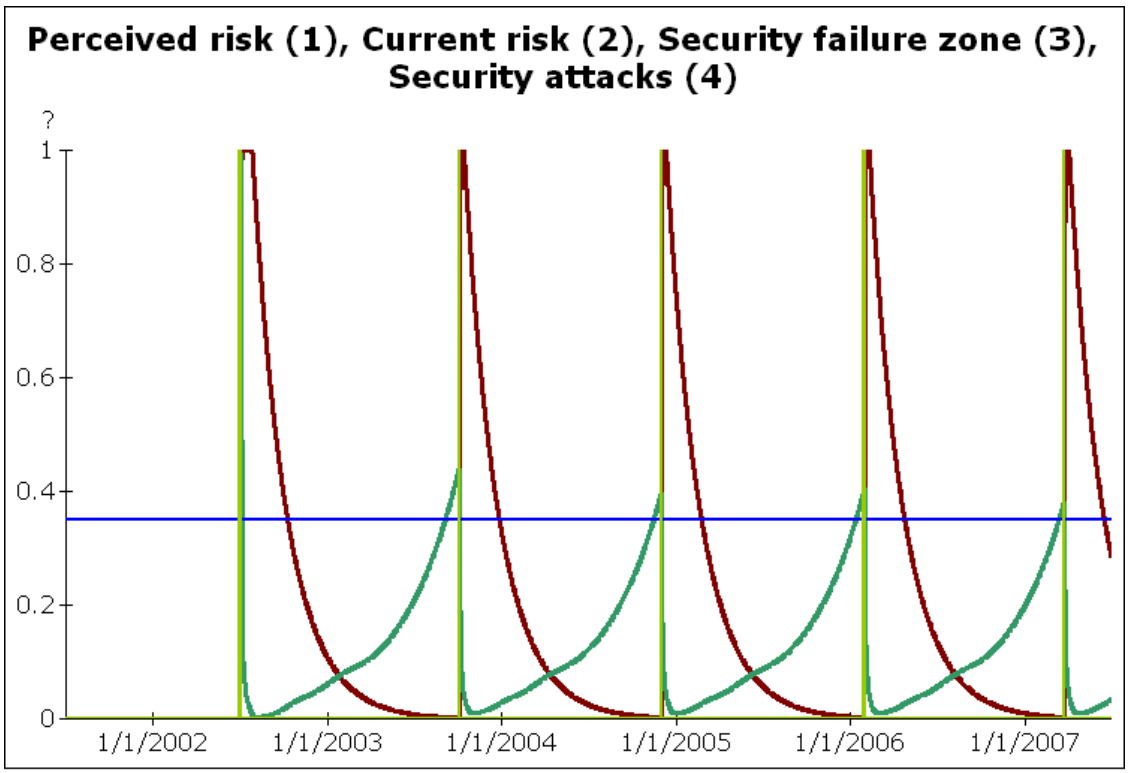


Figure 15 Learning of compliance by instrumental conditioning occurs during a short time period in a risk perception cycle. Extinction of compliance happens slowly over a much longer time interval.

Finally, we simulate the impact of different levels for the security technology (described in our model by the parameter '*Security failure zone*'). Our model (Figure 16) suggests that improving the technology makes security failures (and near failures) rarer. At first sight this sounds obvious and like good news. Second thoughts would indicate that absence of visible risks may cause impaired human ability to learn the right lessons, thus entrenching the bad habit of noncompliance. (Actually, the simulation in the upper half of Figure 16 contradicts our assumptions that Kim would learn the right lesson after three heavy security failures and change her habits. But the point in case should be clear enough.)



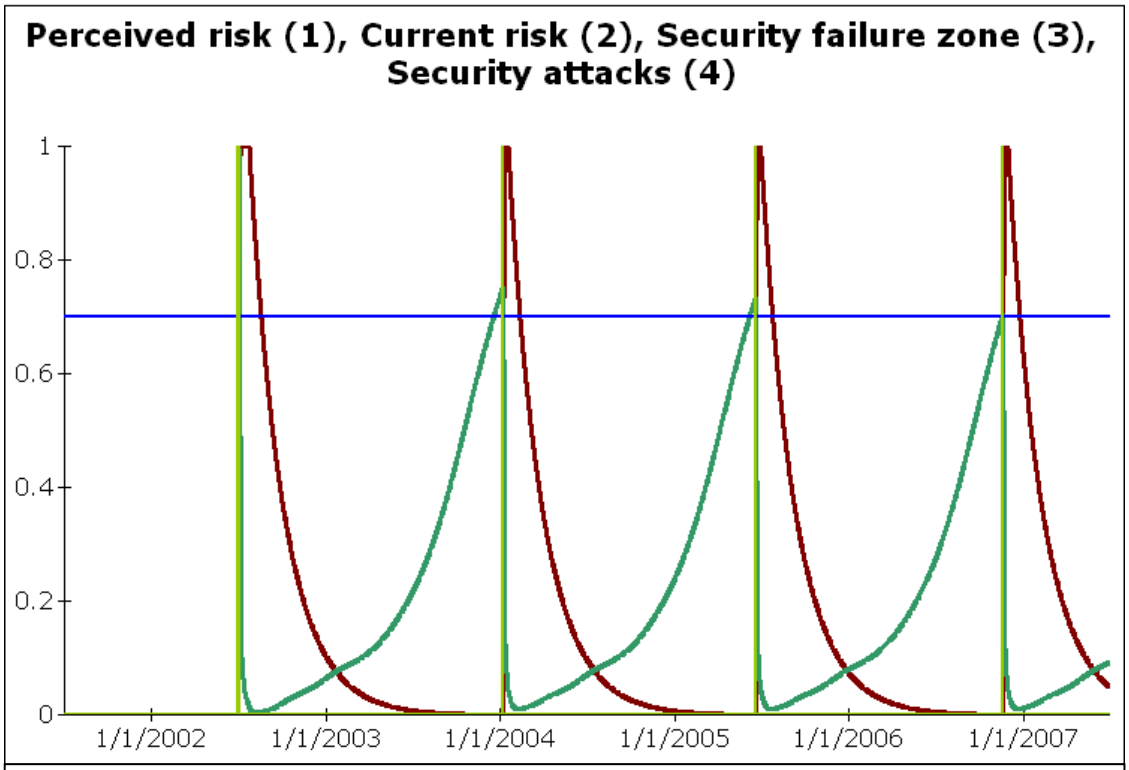


Figure 16 Better security technology (lower half) means less frequent accidents… but it may have undesired consequences for security culture.

Policies suggested by our model

How can one escape the vicious circle of security failures suggested by our model? Remember that Kim is most compliant when she perceives the risk as sufficiently high. Kim's perception of risk is "updated" by security failures: Their occurrence increases her perceived risk sharply; their absence decreases her perceived risk and, as a consequence, her compliance. From the point of view of policy design, the positive effect security failures have on compliance is interesting. For obvious reasons, security failures themselves are not a viable policy tool for improvement of information security. We need other ways to sustain an appropriate level of risk perception. Also, it appears desirable that compliance with security measures is kept above a safe level (avoiding that the system enters the security failure zone), preferably before Kim enters the extinction of conditioned behavior zone. Both aims can be served by "risk perception renewals" that lift the declining risk perception to a higher, more accurate level. Various trainings, publications, seminars and other kind of interventions focusing on IT-risks may be suggested as potentially effective tools for increasing and refreshing the security knowledge among the IT-system users (and here we talk about both the systems' end-users as well as their managers). Indeed, organizations are introducing such training-like interventions as part of their security policies. Mitnick and Simon (2002, p. 130-1) write: "From the corporate perspective, there is a fundamental need for good training. But there is also a need for something else: a variety of ways to remind people of what they've learned. Examples: splash screens with different security messages each day… series of security reminders – an awareness program needs to be ongoing and never-ending… short blurbs in the company newsletter." Note that such interventions must be appropriately scheduled to be most effective: As suggested by our model, interventions to emulate the positive impact of security failures on compliance should occur at the start of periods of decaying risk perception, to avert superstitious learning and to ensure a correction of course before the system becomes too vulnerable.

But it is doubtful that "crying wolf" is likely to be sufficiently effective – in fact, it might be counterproductive. After all, if the result of security campaigns is to make people uneasy about risks the lack of perceived threats – security technology mostly works – will over time discredit such security campaigns ("the wolf does not arrive").

We need a realistic perception of how recurrent risks, even when their probability of occurrence is low, nevertheless threaten security; in other words: a security culture. A security culture could arguably be created by a "learning from incidents" system (see Cooke 2003a and references quoted therein). Security failures nearly always have precursor incidents: For every flight crash there are tens or hundreds of near-crashes; the famous software time bomb at Omega was preceded by many indications that the malicious insider intended to attack (Gaudin 2000; Melara et al. 2003); the 9-11 terrorist attack in 2001 was preceded by the bomb in the World Trade Center in 1993 and many other precursor incidents that were not perceived for what they were (Emerson 2002). Learning from incidents could occur in terms of an instructional system ensuring that incidents – even seemingly harmless ones – are registered, analyzed and shared in the organization. Such setting would combine realistic risk perception with a correct understanding of the role of precursor incidents as omens of security failures, thus presumably counteracting the erosion of

compliance. More precisely, such mechanism of learning from incidents would be a natural counter mechanism to the insidious 'superstitious' learning induced by our proposed mechanism of risk-modulated instrumental conditioning.

Discussion and conclusion

In fact, the last remark in the previous section becomes additional weight by the observation that risk-modulated instrumental conditioning must not be seen as a factor that *competes* with other proposed causative mechanisms for erosion of compliance. Rather, we proposed that risk-modulated instrumental conditioning is an inseparable aspect, adding to and enhancing erosion of compliance, no matter what the driving mechanism is. In fact, the very concept of homeostatic defense of the behavioral bliss point – the preferred distribution of activities – encompasses the notion of priority conflicts (throughput vs security, organizational vs personal, etc). The actual value of the behavioral bliss point – a vector in activity space – would be shaped by such preferences – whether conscious or unconscious – and then conditioning of – mostly – inadequate security behavior would follow. In other words, risk-modulated instrumental conditioning of security behavior would be *inseparable* from behavioral economics factors and other causative mechanisms.

An important remark: As indicated before (see *Erosion of compliance as risk-modulated instrumental conditioning* section), the hypothesis that the erosion of compliance is driven by reinforcement (see e.g. Battmann and Klumb 1993; Dörner 1975; Dörner and Reither 1978; Gonzalez 1995) is not quite correct. Our work suggest a slightly different interpretation: Rather than a reinforcement of noncompliance, one has a transient reinforcement of compliance while risk is perceived as high, followed by extinction of compliance when risk is perceived as low… implying a return to the behavioral bliss point, i.e. a failure and attack prone situation.

The risk homeostasis theory (Wilde 1994), described in the corresponding section above, assumes that subjects act to match perceived risk with some target risk. This sounds appealing at first sight, but the poor human ability to perceive and assess risk seems difficult to reconcile with the assumption that such blurred and obscured parameters should serve as beacons for decision-making. On the other hand, risk – though difficult to perceive and assess – is a key parameter for security failures. Also, risk perception shapes people behavior. Since our theory ties risk perception to compliance, including the choice of a target security level, one could state that this implies an implicit target risk. Thus, in a sense our proposed theory is gives support to Wilde's risk homeostasis theory.

Information security systems need a sound management policy in accord with human nature. Alas, too often one relies solely on technical issues. Either are human factors in security systems treated as "obvious" marginalities or considered unmanageable, hoping that technological solutions should automate security. Such approach is futile: The literature on human error emphasizes the "ironies of automation": Trivial tasks can be technologically addressed, leaving more demanding tasks to people (Reason 1990). Concerning the interaction between people and technology Schneier (2000) states "…this interaction is the biggest security risk of them all."

To improve the robustness of modern information security systems an increased understanding of the role of human factors – especially, of their dynamics – is essential. Gaining insight into the intrinsic interactions between people, technology and working environment in security systems is a main goal of our research. The problem requires an interdisciplinary approach involving relevant knowledge from technology, information science, psychology and management. Understanding its dynamics means understanding the causal structure of the problems and opening paths for more successful policies. For further progress one need high-quality case studies of security failures. For obvious reasons organizations are reluctant to share such data. But for obvious reasons too, without such data human failures will continue to be resilient aspects of the general security problem.

Acknowledgement

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

References

Allison, J. 1989. The nature of reinforcement. In *Contemporary learning theories: Instrumental conditioning theory and the impact of biological constraints on learning*, edited by S. B. Klein and R. R. Mower. Hillsdale, NJ: Erlbaum.

Anderson, Ross J. 2001. *Security Engineering: A Comprehensive Guide to Building Dependable Distributed Systems*. New York, NY: John Wiley & Sons.

Battmann, Wolfgang, and Petra Klumb. 1993. Behavioural economics and compliance with safety regulations. *Safety Science* 16:35-46.

Brehmer, Brendt, and Robert Allard. 1991. Dynamic decisions making: The effects of task complexity and feedback delay. In *Distributed Decision Making: Cognitive Models for Cooperative Work*, edited by J. Rasmussen, J. Laplat and B. Brehmer: John Wiley & Sons.

Carayon, Pascale, and Sara Kraemer. 2002. Macroergonomics in WWDU: What about computer and information system security? Proceedings of the 6th International Scientific Conference on Work With Display Units – WWDU 2002 – World Wide Work, at Berlin.

Cooke, David L. 2003a. Learning from Incidents. Proceedings of the 21st International Conference of the System Dynamics Society, at New York, NY, USA.

———. 2003b. A system dynamics analysis of the Westray mine disaster. *System Dynamics Review* 19 (2).

Domjan, Michael. 2000. *The Essentials of Conditioning and Learning*. 2 ed. Belmont, CA: Wadsworth/Thomson Learning.

Dörner, Dietrich. 1980. On the difficulties people have in dealing with complexity. *Simulation & Games* 11:87-106.

———. 1989. *Die Logik des Mißlingens*. Reinbek: Rowohlt.

———. 1996. *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations*. Translated by R. Kimber and R. Kimber. Reading, MA: Addison-Wesley. Original edition, Originally published in 1987 under the title *Die Logik des Misslingens* by Rowohlt Verlag.

———, ed. 1975. *Über das Problemlösen in sehr komplexen Realitätsbereichen*. Edited by W. H. Tack, *Proceedings of 29. Kongreß der Deutschen Gesellschaft für Psychologie (Salzburg 1974)*. Göttingen: Hogrefe.

Dörner, Dietrich, and Franz Reither. 1978. Über das Problemlösen in sehr komplexen Realitätsbereichen. *Zeitschrift für experimentelle und angewandte Psychologie* 25 (4):527-51.

Emerson, Steven. 2002. *American Jihad: The Terrorists Living Among Us*. New York: The Free Press.

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

Gaudin, Sharon. 2002. *Case Study of Insider Sabotage: The Tim Lloyd/Omega Case*. Computer Security Journal 2000 [cited 20 October 2002]. Available from http://www.gocsi.com/pdfs/insider.pdf.

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

———. 2002a. Modeling Erosion of Security and Safety Awareness. *Proceedings of the Twentieth International Conference of the System Dynamics Society July 28 - August 1, 2002 Palermo, Italy*.
———. 2002b. 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, Jose J, and Agata Sawicka. 2002. A Framework for Human Factors in Information Security. Proceedings of the WSEAS International Conference on Information Security (ICIS'02), at Rio de Janeiro, Brazil.
———. 2003a. Modeling compliance as instrumental conditioning. Proceedings of the Fifth International Conference on Cognitive Modeling (ICCM 2003), at Bamberg, Germany.
———. 2003b. Modeling instrumental conditioning – The behavioral regulation approach. Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS 36), at Big Island, Hawaii.
Guthrie, E R, and G P Horton. 1946. *Cats in a Puzzle Box*. New York, NY, USA: Rinehart.
Hogarth, Robin M. 1987. *Judgement and Choice: The Psychology of Decision*. 2nd ed. Chicester: John Wiley & Sons. Original edition, 1st ed. published in 1980.
Kahneman, Daniel, and Amos Tversky. 2000a. *Choices, Values, and Frames*: Cambridge University Press.
———. 2000b. Prospect theory: An analysis of decision under risk. In *Choices, Values, and Frames*, edited by D. Kahneman and A. Tversky: Cambridge University Press.
McKenzie, R.B., and G. Tullock. 1975. *The New world of Economics: Exploration into the Human Experience*. Chicago, IL: Rand McNally.
Melara, Carlos, Jose Maria Sarriegui, Jose J Gonzalez, Agata Sawicka, and David L Cooke. 2003. A system dynamics model of an insider attack on an information system. Proceedings of the 21st International Conference of the System Dynamics Society July 20-24., at New York, NY, USA.
Mitnick, Kevin D, and William L Simon. 2002. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN, USA: Wiley Pub.
Navon, D., and D. Gopher. 1979. On the economy of the human processing system. *Psychological Review* 86:214-255.
Ono, Koichi. 1987. Superstitious behavior in humans. *Journal of Experimental Analysis of Behavior* 47:261-71.
Reason, James. 1990. *Human Error*. New York: Cambridge University Press.
———. 1997. *Managing the Risks of Organizational Accidents*. Aldershot, Hants, UK: Ashgate Publishing Ltd. Original edition, 1997.
Sawicka, Agata, and Jose J Gonzalez. 2003. Choice under risk in IT-environments according to cumulative prospect theory. Proceedings of the 21st International Conference of the System Dynamics Society July 20-24, 2003. New York, NY, USA.
Schneier, Bruce. 1994. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, Inc.
———. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.

Skinner, Burrhus F. 1948. "Superstition" in the pigeon. *Journal of Experimental Psychology* 38:168-72.
Sterman, John. 1989. Modeling managerial behavior: Misperceptions of feedback in a dynamic decision making experiment. *Management Science* 35 (3):321-339.
Sterman, John D. 1997. Superstitious learning. *The Systems Thinker*:1-5.
Timberlake, W. 1980. A molar equilibrium theory of learned performance. In *The psychology of learning and motivation*, edited by G. H. Bower. Orlando, FL: Academic Press.
———. 1984. Behavioral regulation and learned performance: Some misapprehensions and disagreements. *Journal of the Experimental Analysis of Behavior* 41:355-75.
Vyse, Stuart A. 1997. *Believing in Magic: The Psychology of Superstition*. 1 ed. New York, N.Y.: Oxford University Press, Inc.
Wagner, Gregory A, and Edward K Morris. 1987. "Superstitious" behavior in children. *The Psychological Record* 37 (471-88).
Weick, Karl E. 1987. Organizational culture as a source of high reliability. *California Management Review* 29 (2):112-127.
Wilde, Gerald J. S. 2001. *Target Risk*. Gerald J.S. Wilde, 10.02.1996 1994 [cited 15.10.2001 2001]. Available from http://pavlov.psyc.queensu.ca/target/index.html.
Zeitlin, Lawrence R. 1994. Failure to follow safety instructions: Faulty communication or risky decisions? *Human Factors* 36 (1):172-181.

Back to the Top