Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact

Karen Renaud
School of Arts, Media and Computer Games
Abertay University, Scotland
University of South Africa
k.renaud@abertay.ac.uk

Merrill Warkentin
College of Business
Mississippi State University
MS, USA
m.warkentin@msstate.edu

ABSTRACT

The central premise behind risk homeostasis theory is that humans adapt their behaviors, based on external factors, to align with a personal risk tolerance level. In essence, this means that the safer or more secure they feel, the more likely it is that they will behave in a risky manner. If this effect exists, it serves to restrict the ability of risk mitigation techniques to effect improvements.

The concept is hotly debated in the safety area. Some authors agree that the effect exists, but also point out that it is poorly understood and unreliably predicted. Other researchers consider the entire concept fallacious. It is important to gain clarity about whether the effect exists, and to gauge its impact if such evidence can indeed be found.

In this paper we consider risk homeostasis in the context of information security. Similar to the safety area, information security could well be impaired if a risk homeostasis effect neutralizes the potential benefits of risk mitigation measures. If the risk homeostasis effect does indeed exist and does impact risk-related behaviors, people will simply elevate risky behaviors in response to feeling less vulnerable due to following security procedures and using protective technologies.

Here we discuss, in particular, the challenges we face in confirming the existence and impact of the risk homeostasis effect in information security, especially in an era of ethical research practice.

NSPW'17, October 2017, Santa Cruz, CA, USA

ACM ISBN 978-1-4503-6384-6.
https://doi.org/10.1145/3171533.3171534

CCS CONCEPTS

• **General and reference → Empirical studies**; • **Security and privacy → Social aspects of security and privacy**;

KEYWORDS

Risk Homeostasis, Challenges

ACM Reference Format:
Karen Renaud and Merrill Warkentin. 2017. Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact. In *Proceedings of New Security Paradigms Workshop (NSPW'17).* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3171533.3171534

1 INTRODUCTION

To commence our discussion we start with the basics, defining *homeostasis*. The French psychologist Bernard first introduced the notion of homeostasis in 1878 [9] (cited by [20]). He argued that people naturally maintained particular internal variables within narrow boundaries. Any change in the external system might necessitate a change to their internal system in order to maintain the variable within the boundaries. Redolfo [70] provides some examples of this effect. The human body maintains a steady temperature by either sweating or shivering. The interaction of supply and demand keeps prices stable.

Pelzman [67] was one of the first to raise the idea that people would moderate their behaviors if safety measures made them feel that it was safe to take more risks. He had noted that the imposition of seat belt legislation had not resulted in the anticipated reduction in road fatalities. He surmised that some behavioral adaptation was taking place. Wilde [99], along the same lines, argues for this same behavioral adaptation, actively defending attacks on the existence and impact of what he calls *risk homeostasis theory* (RHT). The core concept is that people will take more risks when they feel safer in doing so, and that this behavioral adaptation

makes safety measures less powerful than they could be in terms of reducing harm.

NIST [42] defines risk as: "*A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*" There are thus three components to risk: (a) an external threat agent, (b) the likelihood that an adverse event will occur, and (c) the anticipated negative impact thereof. Personal risk assessment, thus, implicitly gauges all three of these. The risk homeostasis assertion is that the person then moderates his or her behavior in order to align the actual risk to his or her risk target level.

Such moderated behavior might be calculated to eliminate or reduce vulnerabilities, likelihood or impact. Behaviors are informed by perceptions, and, as Slovic [80] points out: "*Risk does not exist 'out there', independent of our minds and cultures, waiting to be 'measured'. Human beings have invented the concept risk to help them understand and cope with the dangers and uncertainties of life*"

Behavior thus depends on individual and societal perception of risk [40]. Risk perception is influenced by a number of different aspects of the risk, including voluntariness [39], controllability [77], immediacy of effect [78], whether it is manmade or natural [14], familiarity [82], habituation [49], potential benefits of risky behaviour [82] and the ease with which the risk impact is brought to mind [16]. Slovic [79] collapses the factors that impact risk perception into three categories: (1) dread [control, potential for catastrophe, benefits, consequences], (2) whether it is known or unknown [observability, knowledge of risks, immediacy and novelty], and (3) whether individuals, society or future generations are affected. These three factors will interact in unpredictable ways that make it difficult to predict how an individual will perceive a particular risk at any particular point in time.

Wilde [99] considers risk-taking to be an inherent part of the human psyche. He argues that people have a deep seated need to take risks and that this need is individually determined. He argues that we all have a "target level of risk." He suggests the concept of a personal "risk thermostat," indicating how much risk each person is prepared to tolerate. This implies that people assess risk and then act in a way that aligns with their risk tolerance. If anything in the environment changes, it is argued that they will compensate by moderating the riskiness of their actions to bring the risk back to within the boundaries of their own risk comfort zone. In other words, in the presence of new risk-reduction methods or technologies, RHT suggests that individuals will compensate by engaging in greater levels of risky behaviors.

For example, consider the person who wears a seat belt — he or she is taking action to reduce the negative consequences of an accident. If, as RHT suggests, this reduces the risk level to something below his or her target level, he or she might drive faster, thereby increasing the likelihood of an accident occurring. By so doing, he or she re-establishes the risk level to what it would have been without the seat belt.

There is a large body of literature related to risk homeostasis. It comes across as a polarizing issue, characterized by heated rebuttals and counter rebuttals. This is in no small part due to the difficulties related to confirming the existence of the effect, and the challenges of designing experiments that will be considered sound by everyone in the field.

We hope to contribute to the field by considering how we could go about confirming the existence and impact of this effect in the field of **Information Security**. The idea that such an effect might play a role has been posited by [41], [93] and [65]. It is important to explore the existence and impact of this effect in information security. If we do indeed confirm a risk homeostasis effect, we can propose ways of ameliorating it to ensure that our efforts to bolster cyber security are not neutralized by even more risky behaviors.

2 RISK HOMEOSTASIS

That people change their behavior in response to changes in external circumstances, when it comes to risky behaviors, has been argued by Hedlund [34], who says "*We all change our behavior in response to changes in our environment. . . . . Never assume that behavior will not change*" (p88).

Yet exactly *how* people change their behaviors is not always predictable. Historically, scholars assumed that decisions, including personal decisions about engaging in risky behaviors, were grounded in a rational assessment of fundamental decision criteria, including the relative costs and benefits of risky behaviors. Simon [76] suggested that human decision making was characterized by bounded rationality, which reflects imperfect information, imperfect decision-making abilities, and rapid choices made without full consideration of all costs and benefits [28]. This foundation has informed our understanding of decisions in the context of computer security hygiene, wherein researchers have assumed that individual computer users will adopt an essentially rational approach to determining the degree to which they will engage in inconvenient or onerous security behaviors (e.g. changing passwords, encrypting data, patching software) and avoid such behaviors when the costs are too high. This core boundary condition is also consistent with Fishbein and Ajzen's Theory of Reasoned Action (TRA) [29]. Whether individuals observe a rational decision-making process when determining the level of risk they will tolerate is an open question that demands further exploration.

Damasio and Damasio [20] point out that in living systems homeostasis controls can be either conscious and deliberate, or subconscious and automatic. Redolfo [70] considers homeostatic reactions to be both inevitable and automatic.

Even if the homeostasis effort *is* conscious, people might not be willing to admit to it [30], especially if taking such risks is socially unacceptable [64].

If it is automatically driven, as argued by the researchers, this makes the effect particularly hard to verify and prove. People might not even be aware enough of their behavioral motivations to be able to verbalize their reasons for changing the way they respond to risk mitigation measures. Like other latent constructs (e.g. attitudes and beliefs), there can be no direct (objective) measurement thereof.

Due to these difficulties, observations and measures of behavior change which reflect the latent construct are used as approximations. These side effects are studied, rather than the effect itself, because studying actual brain activity (e.g., with fMRI) is very challenging and not yet an exact science [94]. The use of these reflective (second-hand) measures implies that we cannot realistically identify the exact mechanisms that led to any changes that we observe. We cannot be confident that any change has occurred because of the brain's need for homeostasis. It might equally be a consequence of some other poorly-understood behavioral adaptation.

Some examples serve to illustrate the difficulties in confirming that RHT holds. Consider trapeze artists. They undeniably attempt far riskier maneuvers when safety nets are in place than when they are not. In other contexts adaptation of behavior in the presence of safety measures has also been observed. Klen [43] found that when Finnish loggers wore more protection they also behaved more carelessly. Both of these studies have been used to argue for the existence of risk homeostasis. However, as explained above, a mere behavioral change does not point infallibly to risk homeostasis; it might be caused by other factors that we have not yet identified or those that have not yet been linked to risky behaviors.

The question of whether motorcycle helmets are effective demonstrates the debate very well [1]. Adams [2] presents arguments both for and against compulsory wearing of helmets. He argues that risk compensation is simply common sense, and offers the data to support his argument, all the while acknowledging that others have analyzed the same data differently to arrive at the opposite conclusion. He uses cycling fatalities and the impact of helmet wearing legislation to make his argument. Between 1966 and 1969 a number of US states enacted laws to require bikers to wear helmets. After 1977 about half of the states repealed the law. The strange thing is that the number of fatalities increased by a greater percentage in states that had *not* repealed the law than in those that had. People wearing helmets might have behaved more recklessly, so that fatality rates did not decrease. The wearing of helmets, Adams argues, initiated a perverse response from bikers, and did not reduce harm.

Studies in other areas have delivered unconvincing results [1, 2]. Many risk homeostasis studies have been carried out in the traffic context, and consideration of the impact of seat belts has received a great deal of attention. The problem is that people report mixed results. For example, Evans [27] found that people wearing seat belts tended to follow other cars more closely than those without seat belts. Lund and Zador [52] and O'Neill *et al.* [62] examined the same issue and failed to discover an increase in risky behaviors.

These kinds of inconsistencies have led some researchers to deny the very existence of the risk homeostasis effect [26, 52, 55]. They argue that other behavioral pathways, or combinations of these pathways, lead to the observable behaviors that others attribute to a single risk homeostasis effect.

A number of researchers reject the RHT, and the idea that humans have a personal target level of risk tolerance [26, 52, 55, 63]. O'Neill and Williams consider it on a par with the flat earth hypothesis [63].

3 RISK HOMEOSTASIS & RISK MITIGATION

In many avenues of society legislative measures have been enacted to protect people and minimize harm. Authorities argue that safety features are desirable because at least "something is being done" to reduce injuries and fatalities. If, as Wilde argues, each person has an individual risk appetite, interventions might easily be less effective than intended and anticipated.

Hagel and Meeuwisse [31] bemoan the fact that mandated protection might, perversely, give people a false sense of security and lead to other kinds of risky behaviors which will result in different kinds of injuries, but not reduce fatalities. Their argument is that, in attempting to make people safer, such measures could actually be muddying the waters. Other, more effective, measures, might well be available, but the deployment of "something must be done" measures, and the inertia their engagement generates, might curtail investigations into more effective measures.

The idea that risk homeostasis could negate the potential positive effects of precautionary measures is clearly something those in authority are considering when risk mitigation measures are advanced. For example, Zimet *et al.* [104] reports concerns about promiscuous behavior of teenagers being prompted by a feeling of invincibility (RHT effect) due to having received the HPV vaccination. This argument was rejected and many authorities now offer the vaccine to 11 and 12 year old girls. This anecdote emphasizes the need

for more clarity in this area. The argument could well have gone the other way, leaving many teenagers vulnerable to cervical cancer, based on people believing in the impact of an effect whose existence is still being questioned.

4 EXPERIMENTING WITH RISK HOMEOSTASIS

Wilde *et al.* [100] admit that there is a lack of controlled experimental verification for the risk homeostasis effect. They blame two factors for this: (1) the shortcomings of the lab for testing the effect, and (2) complications inherent in the theory itself. We are adding another category to these two: (3) confounding factors.

4.1 (1) Limitations of Lab Studies

Confirming the existence and impact of risk homeostasis requires us to manipulate the risk levels, and then to monitor participants' behavior. However, ethical guidelines require us to ensure that participants are not placed at risk during any research we conduct. Hoyes and Glendon [36] argue that the absence of real harm in risk homeostasis studies might mean that such investigations uncover optimization strategies instead of risk homeostasis effects.

Other approximations have been proposed. Hoyes and Glendon [36] suggest that a way around this is to use a simulation engine; ensuring thereby that the participant him or herself is not at risk, nor their belongings. Some have expressed reservations about this technique since risky behaviors in simulation environments will have only virtual consequences, and might not be a realistic approximation of real-life behaviors [35]. Nor can anyone be sure that they are measuring a personal risk tolerance range and consequent behavioral adjustment. Since most of these games have a competitive element any observable change might be a consequence of natural competitiveness and behavioral optimizations used to win the game. Indeed [90] discovered in their experiments into the existence of risk homeostasis that achievement situations would confound such studies. Wilde himself [99] considered simulation studies a sham and a contradiction in terms.

Hoyes and Stanton [38] argue that monetary gain/loss could be used to induce risk (since it is as "real" to participants as other risks). So, an experimenter could conceivably give participants an endowment and then let them participate in some kind of game where they gain or lose money based on their behavior. The amount of money they're given would have to be substantial enough to make it realistic. The researchers' financial commitment is likely to be prohibitive enough to make this infeasible for academic scholars. Moreover, other confounding factors could be the student's personal financial status, their family background, and ability to handle money.

Laboratory experimental designs frequently use students as experimental subjects, who may, or may not, constitute an effective sampling frame. Students might be woefully inadequate for testing risk homeostasis. In the first place, [11] report that the use of precautionary measures increases with age, which might demonstrate a lower risk tolerance as people age. On the other hand, the older population is also less comfortable with technology and may, due to uncertainty, take fewer risks anyway. If we test for RHT effects with a young, less risk-averse population, our findings are unlikely to be generalizable to other population groups.

4.2 (2) RHT: The Theory

RHT is based on the concept of utility, and relies on the fact that people can assess ongoing risk accurately and realistically. Wilde [99] suggests that a road user intuitively compares actual and target risk, and moderates his/her behavior to align actual and target risk as closely as possible. Wilde [101] argues that a realistic assessment of risk is a requirement for risk homeostasis to mediate behavior.

There are some problems with this theory. The first is related to human ability and propensity to judge risk. The second is related to the completeness of the theory.

4.2.1 Judging Risk. RHT relies on people having an accurate conception of risk [56], and this basic requirement was confirmed by [68]. Yet we know that risk perception is often inaccurate and socially informed instead of realistic [36]. There is also the fact that humans resist seeing themselves statistically when it comes to risk [59]. Moreover, people are unrealistic in judging their own performance abilities [50, 60]. Risk, in a particular situation, is partly determined by performance, so this, too, makes risk assessment inaccurate.

The accurate risk assessment requirement might well make it impossible to test for risk homeostasis in many areas where people have less experience of judging risk. Information Security is a good example. Unlike traffic, which just about everyone has personal experience of, information technology is a relatively recent development and one that many people understand only poorly. The risks have not been quantified or understood, nor, perhaps, is it possible to do so, rendering any accurate calculation of the actual risk infeasible.

The other problem with the risk homeostasis idea is that a sober assessment of utility, and acting upon it, assumes rationality, something that is questioned by researchers in this area [21, 98]. There are many examples where people do not maximize utility, often for emotional reasons. For example, consider restaurant tipping behavior. People tip *after* they

have received a service, and if they do not plan to frequent that restaurant again there is no good reason to tip. Yet, even in these circumstances, people do tip: for no personal gain. This does not align with pure utility maximization.

It might be possible to approximate a situation where the actual risk is clear and obvious to a participant in an experiment. However, it would not be possible to guarantee that the findings of such an experiment would be generalizable to the real world of multiply-faceted risk decisions. Indeed, Runcie and Seaver [71], in their exploration of risk homeostasis, mention this unknowable nature of the risk as a real issue in the field of risk homeostasis studies.

4.2.2 Theory Incompleteness. O'Neill and Williams [63] explain that though people might change their behavior in response to changing levels of risk, this does not necessarily point to the applicability of a universal RHT. More research is required in order to understand the conditions under which this happens.

McKenna [56] offers a traffic-related explanation, arguing that measures that do not affect the individual's interaction with the environment (padded dashboards, shatter resistant windshields) will not initiate behavior change. Streff and Geller [86] tested driving with, and without, seat belts. Interestingly, they discovered that participants who used a seat belt, after having driven without one, drove faster while wearing the belt. A similar between-subjects experiment did not uncover any differences, suggesting that the experience of a direct change made the difference. The fact that they perceived a difference made their original, perhaps faulty, risk perceptions less important. The difference was detectable, and this led to the behavioral change, not actual and accurate risk assessment.

Risk homeostasis, if it does exist, can be achieved by [37]: (1) behavioral change within the environment; (2) mode migration; or (3) avoidance. Wilde's theory focuses primarily on the first of these, without giving much credence to the other two. So, for example, if you implement some safety traffic intervention, and you notice that traffic accidents have not decreased, you could consider this evidence of the risk homeostasis effect. It could also be that people have switched to public transportation and that the intervention has actually made driving less safe. This brings us back to the discussion right at the beginning — we're measuring side-effects, and it is impossible to measure all the factors that could lead to a change.

Haight [32] concludes that this theory is "incoherent." Evans [26] is also critical of the theory, saying that the evidence points clearly away from a risk homeostasis effect rather than towards it.

4.3 (3) Confounding Factors

4.3.1 Real-life Risky Behavior is Socially Informed. People might become aware of the fact that people mistrust a particular practice and adapt their own behavior as a consequence [36]. There is some evidence of this when it comes to traffic [6] and it might, or might not, apply equally to information security. Very few lab studies attempt to incorporate this, probably because it is particularly challenging to do so.

4.3.2 Feedback is Essential. Purely on a personal level, real life allows people to experience natural feedback. This, too, is hard to replicate effectively in a lab environment [99] where we attempt to control all possible confounding factors so that realistic feedback is often not provided, or provided inadequately. This might be due to ethical concerns related to scaring people when they behave too riskily.

4.3.3 Short Term Effects may not Endure. The short term nature of lab-based experiments is another confounding factor. Risky behavior evolves over time [36]. This brings into question the validity, and limits the generalizability of, the findings of short-term lab studies. Longitudinal research designs might capture the temporal effects, but they impose more challenges to ethics board approval and to valid implementations.

4.3.4 Uncertainty. Real risky behaviors have two imponderables (a) uncertainty of performance, and (b) uncertainty of consequence. So, for example, if someone drives he/she cannot be absolutely sure that they will always avoid having an accident. People might be distracted or drive into a slippery patch, making actual performance unpredictable. Also, if people do have an accident, they cannot know whether they will walk away unharmed or be seriously injured. Both uncertainties add yet another confounding factor to risk homeostasis studies.

There are two personal dimensions influencing performance: (a) high-level decision processes, and (b) low-level control performances. Summala [87] points out that when the two are combined the effect looks like risk homeostasis but, in fact, is merely an aggregation of differences in either or both of these aspects, Performance is influenced by driving conditions (the environment) but also by the individual's personal state of mind and body, whether or not he/she is fully aware of this fact.

4.3.5 Ethics. The Belmont report [22] presents three principles to which ethical research studies must adhere. (1) Respect for Persons, (2) Beneficence, and (3) Justice. These principles have been put into place to protect participants from the kinds of notorious experiments reported in the literature that did indeed harm participants [58, 103]. We

wholeheartedly endorse these principles, and it is instructive to consider how they impact risk homeostasis studies.

The first principle requires *respect for autonomy*. In a risk homeostasis study, we want to measure an effect that is probably subconscious. Making people consciously aware of the risks might well make it impossible to attribute any effect to risk homeostasis because such awareness might confound the study and interfere with activation of the risk homeostasis effect.

The second principle requires people to be *protected from harm*. Risk behaviors, by their very nature, have harm as their probable consequence.

The final principle, *justice*, requires burdens not to be unduly imposed. It could well be argued that allowing people to experience the consequences of risky behaviors, merely to confirm the existence of a risk homeostasis effect, might not meet this principle.

5 RISK TOLERANCE LEVEL STABILITY

The risk homeostasis effect relies on a core assumption of a personal, relatively stable, risk target level. It does not seem to have any way to incorporate the impact of other powerful factors that influence and change this level over time.

5.1 Habituation Effect

People's attitudes to risk change as they become more accustomed to engaging in a risky behavior: they habituate to the risk [19], especially if they feel they have the skills to manage it. People are less likely to comply with warnings about the danger of particular risky activities as they become more familiar with carrying out the activity [13, 92].

MacCurdy [53] provides some examples of this. For example, lion tamers know better than anyone else how dangerous it is to be close to lions yet they are happy to operate in such an environment, because they are confident in their ability to manage the risk. MacCurdy also points out that bomb disposal experts should actually be paralyzed by fear, given the potential consequences of a mistake. They are not, though, because they have the skills to cope with the risk (controllability [23]), and are accustomed to taking the risk (habituation).

These examples suggest that a stable risk appetite is not guaranteed. It could be argued that the people mentioned in the previous paragraph are unusual, and the usual risk homeostasis effect does not operate for them. In reality, we all behave in this way, albeit less sensationally. Every automobile driver essentially operates a moving vehicle that weighs tons, and the driver is at significant risk of being involved in a car accident whenever a number of cars share the road. It is rare to encounter someone who does not drive because of this particular risk; most drivers simply become used to it (habituation). They become more comfortable with the risk, suggesting a strong experiential influence on risk appetite. This is maintained until they have an accident, which activates the experience effect, discussed next.

5.2 Experience Effect

It seems logical that direct experience of risk would influence risk perception. Weinstein [97] carried out a study to explore this and reported that experience did *not* make a lasting and sustained impact on self-protective behavior. Norris *et al.* [61] revisited his hypotheses and reported that experience did indeed have lasting and substantial effects on behaviors. There is some evidence from other researchers for this [15, 25, 33, 57]. Moreover, other people's experiences, if vivid and perceived to be relevant personally, also impact people's future risk perceptions [85].

People who have experienced an event often respond by acting to prevent a re-occurrence. This means that the experience leads to more confidence, not less. This happens, Norris *et al.* [61] argue, because they go through the cognitive actions required to establish control over the situation. This depends on two aspects (1) response efficacy, and (2) their own self-efficacy [4, 69, 97].

5.3 Disposition, Predilection & Emotion

People are uniquely different from one another. One particular difference that impacts behavior in risky situations is optimism bias [95].

For example, Aspinwall and Brunbart [7] found that dispositional optimism impacted the processing of health risk information. On the other hand, Pedruzzi and Swinbourn [66] did not find a similar impact on processing of road risk information. They posit that this is due to the fact that people feel more in control of their road risks, where health risks might seem somewhat arbitrary. There is evidence that controllability of a risk leads people to downplay the likelihood and severity of risks [23], so their argument makes sense.

Tekeli-Yeşil *et al.* [89] found that gender and socio-economic factors also impacted risk perception. Although this could be used to argue for a personal risk target, as Pelzman and Wilde do, there is also evidence that personality is not necessarily stable over our lifetimes [10].

Adam Smith famously wrote that passions combine with reason to lead to the decisions that people take [83]. More recently a number of researchers have written about the role of emotions in decision making [8, 51, 81]. Decision making is impacted by both current (emotional state at the time of the decision) and anticipated emotions (based on expected outcomes) [74]. These contribute to the unpredictability of human behavior.

5.4 Summary

The influence of these idiosyncratic factors appears to negate the notion of a stable risk target level. What is indicated by the literature is a level that fluctuates as we go through life, influenced by our malleable and changeable perceptions, our personal experiences, the experiences of those close to us and those we read about in the media. It might be that what is identified as a risk homeostasis effect is, in fact, the impact of an increased perception of the controllability of a risk. The literature on the impact of controllability on risk behaviors is well established, and this impact widely accepted, unlike the risk homeostasis effect. Hence a small matter of the imposition of a risk mitigation strategy, such as a seat belt, might well be drowned out by the stronger influences of other factors.

6 THE INFORMATION SECURITY CONTEXT

The security of any organization, personal computer, or mobile device depends on the behavior of those who use them. A number of technical measures are implemented on systems in order to repel hacking attacks. Other technical measures ensure the availability of data by performing automatic backups of information.

If we consider the parallels between the information security and safety fields we have to wonder whether these measures make people adjust their behavior so that they take more risks, simply because existing measures are deemed to protect them from harm.

This kind of trade-off was reported by Ruotti *et al.* [72]. Their study's participants were more willing to use their credit cards online because they knew that banks would refund charges if they were fraudulent. This example demonstrates that risk homeostasis, if it does indeed exist, can lead to positive outcomes by encouraging people to take actions online that they would otherwise be too risk-averse to attempt.

On the other hand, if people are mistaken in their perception of the actual risks, this could lead to real harm. Wash and Rader [96] investigated beliefs about information security and the actions that people take and found that many people were informed or wrongly informed about security and the efficacy of the actions they currently take. They conclude that there is a need to acknowledge a wide range of beliefs which directly inform risky or protective behaviors.

One particular confounding factor, in terms of testing for risk homeostasis in information security, is that there is possibly a **moral** dimension in this field. Information security professionals talk about "poor" security behaviors [45] and "bad" or "good" passwords [88]. These are judgmental terms.

Hoyes and Glendon [36] explain that studies of changed behaviors linked to risk homeostasis are only valid when there is no right or wrong course of action. If there is a "good" and "bad" course of action then risk homeostasis is not being tested, but rather something else. In this case we might be observing the results of a social desirability adaptation rather than a personal risk homeostasis effect.

Finally, as pointed out in the previous section, people can actually be more comfortable with risk if they have experienced a bad event and have determined how to control it. Yet hacking attacks are so frequent and unpredictable, and 100% security so unattainable, that this kind of controllability is probably infeasible. Indeed, Creese *et al.* [17] investigated whether experience of a breach led to a change in risk perception, and did not detect any behavioral change.

Moreover, Norris *et al.* [61] point out that behavior changes more reliably when proactive and vigilant behaviors are needed than when the person needs to adopt disciplined behaviors, perhaps requiring self denial. These two behavior types are different in a profound way, so we can expect the behavioral change mechanisms to be different too. Hazard defence is changed by experience, but a switch to more disciplined behaviors is far more complex. It might be naïve to consider that mere exposure to a negative experience will lead to more disciplined behaviors.

7 RHT & INFORMATION SECURITY

Research designs strive to maximize three criteria when collecting evidence: generalizability, precision, and realism. Each research design favors one or another of these goals and therefore exhibits known flaws [54].

Survey research is high in generalizability, lab experiments are high in precision, and field experiments (and case studies) are high in realism. Researchers utilizing laboratory experiments to study individual security behaviors may rigorously examine individual subjects in a controlled environment where many research variables can be carefully controlled, but in this case realism suffers because this artificial setting only mimics reality. Generalizability also suffers because specific conditions and research subjects were used, and the results may not apply to different conditions and/or people.

Field experiments are considered highly realistic as they examine natural environments, but are challenging (or impossible) in the context of risk homeostasis, and so precision and generalizability will suffer.

Survey research has high generalizability, especially when survey instruments are distributed across multiple organizations in multiple industries, and are commonly used in security behavior research [18]. However, surveys lack realism and precision. To investigate risk homeostasis, we cannot simulate the perception of risk — we must observe subjects

who feel actual risk in a realistic setting. There are many challenges in achieving this.

Having ruled out a lab study, based on the weaknesses pointed out earlier, we now consider the use of naturalistic experiments.

Hedlund [34] says that if the risk compensation effect is to be avoided, the measure needs to score low on four factors. We consider these as they might apply in information security:

Hedlund Number 1.
The safety measure has to be detectable and discernible. Anti-virus and other technical security measures mostly do their jobs invisibly so are arguably not visible enough to be detectable;

Hedlund Number 2.
The safety measure has to affect the individual. Many organizations implement technical measures to protect devices from SPAM. If these measures never prevent one of their personal emails from being delivered, the person would not be aware of how the software is protecting them. In this case, the risk homeostasis effect cannot come into play. The threat and the protection must be personally relevant to the individual person. This is illustrated by the findings of a study carried out by Egelman and Schechter [24] who found that people disregarded warnings during the experiment (while using the researcher's laptop). They said they did not care because their own devices would not be harmed, only the researcher's computer.

Hedlund Number 3.
There must be a reason for users to change their behavior. This suggests that when they feel less at risk they are motivated to behave more riskily. Information security behaviors might well satisfy this requirement since it has been shown that if people become more aware of risk they adapt their behavior accordingly [47, 48]. However, this adaptation happens at a conscious level and might not satisfy the automaticity required by the risk homeostasis effect.

Hedlund Number 4.
They must have discretionary control. Behavior must not be tightly controlled or firmly mandated with monitoring and sanctions for non-compliance. If an employer implements an Information Security Policy (with prescribed policies and procedures), then any change in behavior could simply be due to employees' desire to comply with the rules or to avoid sanctions, or due to recent Security Training and Awareness programs or campaigns, rather than being a risk homeostasis behavioral adjustment.

7.1 Observational Studies

Spring *et al.* [84] points out that observations are an essential first step before actual risk-related experiments can be carried out.

Given the ethical constraints, as enumerated in Section 4.3.5, how could an experiment be designed to test the risk homeostasis effect? The main issue is that experimental participants should not be harmed. Could we perhaps make people believe that actual risk is higher than it really is, and see whether they then reduce the riskiness of their behaviors?

Given the objections to lab experiments detailed in Section 4.1, we would have to deploy an instrumented application that would (1) facilitate a range of actions of varying levels of riskiness, and (2) log all user actions. Such an app would signal different levels of risk to alter risk perceptions. We could then determine how people react in response to signals about the level of risk, in terms of engaging in risky behaviors.

Lévesque *et al.* [44] carried out a longitudinal experiment that simply monitored people's laptops for infections and also monitors behaviors. The authors report that the experiment produced insights that would not have been possible without this observational experiment. Akawe and Felt [5] carried out an observational investigation into how web surfers respond to browser warnings. They wanted to understand how well people respond to different kinds of warnings. Bravo-Lillo *et al.* [12] carried out a between-subjects study to test the efficacy of different warning designs in order to find the best design in terms of drawing user attention to important information.

7.2 No Experimental Manipulation

One way of testing for risk homeostasis is to collect real world data either before and after an intervention or to compare two equivalent areas where one has had an intervention applied and the other not. This is carried out in other risk contexts where it would be unethical to manipulate real risk as part of an experiment. So, for example, Adams [2] collected information about cycling fatalities in US states with and without helmet legislation in order to see whether helmets led to fewer fatalities.

It might be possible to collect information about information security incidents (as an measure of the outcome of risky behaviors) in organizations with different implemented risk-reduction measures. For example, some organizations permit their employees and contractors to use their own devices without hindrance, whereas others implement a BYOD policy that mandates that the organizations install technical packages on the device if it is to be used on the organization's network [46]. The difficulty would lie in finding comparable

organizations. They would have to have the same, or roughly equivalent, information security policies. They would have to exercise the same kind of control over their employees (Hedlund number 4). The employees ought to be made aware of the efficacy of the particular measure (Hedlund number 1).

Some organizations have switched to Google as a mail server instead of maintaining their own mail servers (Hedlund number 2). Google has superior Phish detection capabilities. We could try to find two equivalent organizations, one using their own servers and another using Google. Employees should be told about Google's superiority in detecting Phish messages (Hedlund number 1), and trained to be aware of Phishing (Hedlund number 3). We could count the number of successful phish attacks in each organization for a fixed period of time. This might demonstrate that people are more willing to click on an emailed link if it came in via Google (considering it less risky).

The issue, naturally, will lie in finding comparable organizations. It is impossible to control for, or even uncover, all confounding differences between organizations which could be responsible for any observed change [91].

7.3 Quasi-Experimental Approach

Another option is deliberately to assess a situation by taking a number of measurements both before and after a particular intervention: a quasi-realistic study. This allows for a more fine-grained measurement of impact than statistics reported by organizations which could be incomplete or incorrect.

While this might seem a reasonable way to test for risk homeostasis, testing in this kind of quasi-experimental study has the following issues, as discussed before:

(1) RHT does not predict the behavioral pathway through which an effect manifests itself. It is hard to separate cause from effect to judge conclusively that it was risk homeostasis that led to a particular outcome.
(2) The effect might be short-term, with re-establishment of previous behavior in the long term.
(3) The participants could be over-compensating because they are aware of the experimental conditions (required by ethical guidelines).
(4) It only addresses the consequences of a change in intrinsic risk perception. It does not help us to decide whether individuals are characterized by an individual target level of risk, or whether any such target can be shifted via changes in utilities.

The difficulties are demonstrated by a study carried out by [73] into whether drivers with antilock brakes and airbags took more risks than those without. They reported differences in driving but also acknowledged the likely impact of dense traffic, driver background and car characteristics. This made it impossible to draw reliable conclusions about the impact of these protection measures, or any invocation of the risk homeostasis effect.

7.4 Areas for Investigation

There are a number of information security behaviors that could feasibly be impacted by a risk homeostasis adaptation. We suggest a few:

(1) **Clicking links**: if people know that their email provider has phish detection functionality, would they be more likely to click on links in emails? Or if users know that their web browser actively blocks known malware-laden sites (with drive-by downloads), would they be more likely to visit unknown sites, especially those that may be associated with gambling, porn, or other "gray area" activities?
(2) **Password choice**: would people choose weaker passwords for websites that they consider more secure (under the assumption that these websites are less likely to be hacked)?
(3) **Data backup**: if people have anti-virus software installed that has detected ransomware recently, would they be less assiduous about making regular backups?
(4) **Downloading files**: would people be more willing to download files if they have anti-malware software installed?
(5) **Smartphone protection**: if someone's smartphone offers the option of wiping or destroying the phone remotely, would they be less likely to use a strong PIN/password to prevent a thief from gaining access to their phone's functionality?
(6) **App installation**: would smartphone users who believe that their app provider tests apps before listing them, be more likely to install downloaded apps?
(7) **Website trust**: would users who feel that third parties (such as trust seal providers or regulators) monitor and regulate eCommerce providers be more likely to buy from unknown websites?

7.5 An Experimental Investigation

Zhang *et al.* [102] carried out an investigation into possible risk homeostasis effects in order to incorporate the presence of a technical protection measure into the theory of planned behavior.

They conducted a survey with 176 respondents. They observed that the participants demonstrated a lower intention to comply with security policies if there was a high perception of technical protection. The researchers state that this "*suggests possible risk compensation effects in the information security context.*" They investigated the role of "perceived behavioral control," (PBC) which Ajzen [3] defines as the

individual's expectation regarding the degree to which they feel capable of performing the target behavior, combined with the extent to which they perceive that they have the necessary resources. Zhang *et al.*'s empirical results indicated that PBC acts as a mediating variable between beliefs regarding the protection provided by the mechanism and the intention to engage in safe or risky behaviors. So, the direct impact on behavioral intention may be the degree of control that the individual feels, rather than a risk homeostasis activation.

Zhang *et al.*'s study appears to confirm the impact of a sense of control, and once again demonstrates the difficulty of pinning down the real reasons behind behavioral intentional modifications.

8 QUO VADIS?

In summary, let us consider the premises of the RHT. It posits that (1) people have an individual risk tolerance level, and (2) that they assess the current situation and adjust their behaviors in order to maintain this level.

These premises have been challenged in this review. In the first place, it does not seem to be reasonable to assume stability of a person's individual risk tolerance level. There is also good reason to question the human species' ability to judge risk correctly and objectively. Risk homeostasis is completely unlike the well-known and widely-accepted homeostasis effects such as maintenance of a constant body temperature. Risk is not a physiological effect, and poorly understood, as demonstrated by the discussion in this paper.

8.1 Identified Challenges

Even if we ignore the flawed nature of these two premises, and proceed to attempt to test for the risk homeostasis effect, we face almost insuperable difficulties in so doing.

Ethical Challenges. We have outlined the extensive challenges involved in proving that the risk homeostasis mechanism exists in a way that is ethical and dependable.

The need to carry out our research ethically is particularly constraining in this context. For example, in a carefully controlled lab experiment, we could invite volunteers to bring their own personal devices, both with and without malware protection pre-installed. We could ask them to engage in some potentially risky activity to see whether the protected subjects exhibit more risky behaviors. However, a typical ethics board (IRB in the US) would never permit this experiment, nor any other where harm might result.

Risk homeostasis, in the safety arena, involves people taking risks that could result in physical harm. Trying to verify the effect in the information security domain, in a realistic way, would entail allowing people to take real risks with their own information and resources. This would be unethical.

Measurement Challenges. The core difficulty is that risk homeostasis experiments measure secondary effects, basically because that is all we are able to do. If one observes an effect, one cannot know what unseen cognitive processes have contributed towards it. Separating cause from effect is non-trivial in these kinds of experiments [38].

In Summary. It does not seem as if anyone, in safety or security, has thus far been able to deliver compelling evidence as to the validity of the risk homeostasis effect.

We, too, are unable to propose any reliable experiments that would be able to avoid all the difficulties the literature has uncovered in confirming the existence of the risk homeostasis effect as it applies in the information security context. In the following section we suggest some avenues for further investigation in this area.

8.2 A Way Forward

A number of directions for future investigation can be pursued:

- **Talk to IRBs**: The Menlo Report on principles guiding Information and Communications Technology (ICT) research [75] explains that this principle does not mean that no harm results, only that "*risks to individual subjects are weighed against the benefits to society*" (p. 9). They explain that review boards ought to consider the kinds of risks people would actually experience in day to day ICT usage and be convinced that the experiment is worth conducting. This means that if we want to carry out risk homeostasis studies we should write well-argued motivations for our studies, in terms of benefits to society as a whole. Assuming that such studies would be turned down is perhaps overly naïve.
- **Risk Perception Complexities and Risk Homeostasis**: Our discussion in this paper, while acknowledging the complexity of individual risk perception, does not really explore the interaction of risk perception and risk homeostasis responses. In particular, the issue of risk controllability in the information security context would be a promising direction for future investigation.
- **Risk is Socially Informed:** Risk perception's social nature, and its interaction with a risk homeostasis response, is something that would be interesting to explore in an information security context.
- **Observational Studies:** We plan to learn from the studies carried out by Lévesque *et al.* [44]. We want

to design an observational study to see whether we can detect a risk homeostasis response to experimental manipulations in the long term.

9 CONCLUSION & FUTURE WORK

This paper has presented a synopsis of the research into risk homeostasis. We have elucidated the challenges of confirming or denying the effect and presented some studies arguing both for and against it. Our purpose was to propose some experimental designs for testing for the existence and impact of this effect in the information security context. Having conducted this review of the literature we have concluded that it would be impossible to isolate the impact of risk homeostasis in an experimental study that was both realistic and ethical.

We could wait until the research giants in this area have concluded that RHT does indeed predict human behaviors. If this happens, we can use these researchers' proven techniques to assess its influence in the information security context. It seems futile to carry out any risk homeostasis-related experiments while the debate continues to rage, without either side conclusively proving their point of view.

On the other hand, we have suggested a number of avenues for future investigation to advance the field and enhance our understanding of this fascinating field.

ACKNOWLEDGEMENTS

This research was carried out while the first author was a Cyber Security Fulbright Scholar at Mississippi State University.

We would like to thank Julie Thorpe and Mary Ellen Zurko for shepherding this paper. We also thank the NSPW conference attendees for their helpful comments that we have used to improve the discussion in this paper.

REFERENCES

[1] John Adams and Mayer Hillman. 2001. The risk compensation theory and bicycle helmets. *Injury Prevention* 7, 2 (2001), 89–91.

[2] John G U Adams. 1983. Public safety legislation and the risk compensation hypothesis: the example of motorcycle helmet legislation. *Environment and Planning C: Government and Policy* 1, 2 (1983), 193–203.

[3] Icek Ajzen. 2002. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology* 32, 4 (2002), 665–683.

[4] Icek Ajzen. 2005. *Attitudes, Personality, and Behavior*. McGraw-Hill Education (UK), Berkshire, England.

[5] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *USENIX security symposium*, Vol. 13.

[6] Robert M Arthur. 2011. Examining traffic flow and speed data: Determining imitative behavior. *Traffic Injury Prevention* 12, 3 (2011), 266–273.

[7] Lisa G Aspinwall and Susanne M Brunhart. 1996. Distinguishing optimism from denial: Optimistic beliefs predict attention to health threats. *Personality and Social Psychology Bulletin* 22, 10 (1996), 993–1003.

[8] David E Bell. 1985. Disappointment in decision making under uncertainty. *Operations Research* 33, 1 (1985), 1–27.

[9] Claude Bernard. 1879. *Leçons sur les phénomènes de la vie commune aux animaux et aux végétaux*. Baillière.

[10] Wiebke Bleidorn, Christopher J Hopwood, and Richard E Lucas. 2016. Life Events and Personality Trait Change. *Journal of Personality* (2016).

[11] Nils I Bohlin. 1967. *A statistical analysis of 28,000 accident cases with emphasis on occupant restraint value*. Technical Report. SAE Technical Paper.

[12] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 6.

[13] Bonnie Brinton Anderson, Anthony Vance, C Brock Kirwan, David Eargle, and Jeffrey L Jenkins. 2016. How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems* 25, 4 (2016), 364–390.

[14] Wibecke Brun. 1992. Cognitive components in risk perception: Natural versus manmade risks. *Journal of Behavioral Decision Making* 5, 2 (1992), 117–132.

[15] John Chapin and JoAnn Chirico. 2001. Why It Won't Happen to Me: How Older Adolescents Make Personal Risk Assessments. In *Annual Meeting of the National Communication Association (87th, Atlanta, GA)*. ERIC. November1-4.

[16] Vincent Covello and Peter M Sandman. 2001. Risk communication: evolution and revolution. *Solutions to an Environment in Peril* (2001), 164–178.

[17] Sadie Creese, Duncan Hodges, Sue Jamison-Powell, and Monica Whitty. 2013. Relationships between password choices, perceptions of risk and security expertise. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 80–89.

[18] Robert E Crossler, Allen C Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. 2013. Future directions for behavioral information security research. *Computers & Security* 32 (2013), 90–101.

[19] David G Curry, Robert D Quinn, David R Atkins, and Tage CG Carlson. 2004. Injuries & the Experienced Worker. *Professional Safety* 49, 9 (2004), 30–34.

[20] Antonio Damasio and Hanna Damasio. 2016. Exploring the concept of homeostasis and considering its implications for economics. *Journal of Economic Behavior & Organization* 126 (2016), 125–129.

[21] Robyn M Dawes. 2001. *Everyday irrationality: How pseudo-scientists, lunatics, and the rest of us systematically fail to think rationally*. Westview Press, Boulder, CO.

[22] Department of Health, Education, and Welfare. 1979. The Belmont Report. (1979). tps://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/.

[23] Mary Douglas. 1986. *Risk acceptability according to the social sciences*. Vol. 11. Russell Sage Foundation, USA.

[24] Serge Egelman and Stuart Schechter. 2013. The importance of being earnest [in security warnings]. In *International Conference on Financial Cryptography and Data Security*. Springer, 52–59.

[25] Louise Eriksson. 2014. Risk perception and responses among private forest owners in Sweden. *Small-Scale Forestry* 13, 4 (2014), 483–500.

[26] Leonard Evans. 1986. Risk homeostasis theory and traffic accident data. *Risk Analysis* 6, 1 (1986), 81–94.

[27] Leonard Evans, Paul Wasielewski, and Calvin R Von Buseck. 1982. Compulsory seat belt usage and driver risk-taking behavior. *Human Factors* 24, 1 (1982), 41–48.

[28] Ezzat A Fattah. 1993. The rational choice/opportunity perspectives as a vehicle for integrating criminological and victimological theories. *Routine Activity and Rational Choice: Advances in Criminological Theory* 5 (1993), 225–258.

[29] Martin Fishbein and Icek Ajzen. 1977. *Belief, attitude, intention, and behavior: An introduction to theory and research.* Addison-Wesley, Reading, MA.

[30] Pamela Grimm. 2010. Social desirability bias. *Wiley International Encyclopedia of Marketing* (2010).

[31] Brent Hagel and Willem Meeuwisse. 2004. Risk compensation: a "side effect" of sport injury prevention? *Clinical Journal of Sport Medicine* 14, 4 (2004), 193–196.

[32] Frank A Haight. 1986. Risk, especially risk of traffic accident. *Accident Analysis & Prevention* 18, 5 (1986), 359–366.

[33] Peter Harris. 2007. The impact of perceived experience on likelihood judgments for self and others: An experimental approach. *European Journal of Social Psychology* 37, 1 (2007), 141–151.

[34] James Hedlund. 2000. Risky business: safety regulations, risk compensation, and individual behavior. *Injury Prevention* 6, 2 (2000), 82–89.

[35] Thomas W Hoyes. 1992. *Risk homeostasis theory in simulated environments.* Ph.D. Dissertation. Aston University.

[36] Thomas W Hoyes and Aleck Ian Glendon. 1993. Risk homeostasis: issues for future research. *Safety Science* 16, 1 (1993), 19–33.

[37] Thomas W Hoyes and Neville A Stanton. 1995. Testing risk homeostasis theory in a simulated process control task: implications for alarm reduction strategies. In *Human Factors in Alarm Design*. Taylor & Francis, Inc., 45–58.

[38] Thomas W Hoyes, Neville A Stanton, and RG Taylor. 1996. Risk homeostasis theory: A study of intrinsic compensation. *Safety Science* 22, 1 (1996), 77–86.

[39] Helmut Jungermann and Paul Slovic. 1993. Die Psychologie der Kognition und Evaluation von Risiko. In *Risiko und Gesellschaft*. Springer, 167–207.

[40] Jeanne X Kasperson, Roger E Kasperson, Nick Pidgeon, and Paul Slovic. 2003. The social amplification of risk: assessing fifteen years of research and theory. *The social amplification of risk* 1 (2003), 13–46.

[41] Wayne Derek Kearney. 2016. *Risk homeostasis as a factor in information security.* Ph.D. Dissertation. Computer Science, North West University.

[42] Richard Kissel. 2013. NISTIR 7298 Revision 2. Glossary of Key Information Security Terms. (2013). nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[43] Tapio Klen. 1997. Personal protectors and working behaviour of loggers. *Safety Science* 25, 1 (1997), 89–103.

[44] Fanny Lalonde Lévesque, Jude Nsiempba, José M Fernandez, Sonia Chiasson, and Anil Somayaji. 2013. A clinical study of risk factors related to malware infections. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 97–108.

[45] John Leach. 2003. Improving user security behaviour. *Computers & Security* 22, 8 (2003), 685–692.

[46] James Lee Jr, Merrill Warkentin, Robert E Crossler, and Robert F Otondo. 2016. Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. *Journal of Computer Information Systems* (2016), 1–10.

[47] Huigang Liang and Yajiong Xue. 2009. Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly* (2009), 71–90.

[48] Huigang Liang and Yajiong Xue. 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems* 11, 7 (2010), 394.

[49] Maria Luisa Lima. 2004. On the influence of risk perception on mental health: living near an incinerator. *Journal of environmental psychology* 24, 1 (2004), 71–84.

[50] Robert L Linn, M Elizabeth Graue, and Nancy M Sanders. 1990. Comparing state and district test results to national norms: The validity of claims that "everyone is above average". *Educational Measurement: Issues and Practice* 9, 3 (1990), 5–14.

[51] Graham Loomes and Robert Sugden. 1982. Regret theory: An alternative theory of rational choice under uncertainty. *The Economic Journal* 92, 368 (1982), 805–824.

[52] Adrian K Lund and Paul Zador. 1984. Mandatory belt use and driver risk taking. *Risk Analysis* 4, 1 (1984), 41–53.

[53] John Thompson MacCurdy. 1943. *The Structure of Morale.* Cambridge University Press, New York.

[54] Joseph E McGrath. 1995. Methodology matters: Doing research in the behavioral and social sciences. In *Readings in Human-Computer Interaction: Toward the Year 2000 (2nd ed)*. Citeseer, San Francisco.

[55] Frank P McKenna. 1985. Do safety measures really work? An examination of risk homoeostasis theory. *Ergonomics* 28, 2 (1985), 489–498.

[56] Frank P McKenna. 1987. Behavioural compensation and safety. *Journal of Occupational Accidents* 9, 2 (1987), 107–121.

[57] Qing Miao and David Popp. 2014. Necessity as the mother of invention: Innovative responses to natural disasters. *Journal of Environmental Economics and Management* 68, 2 (2014), 280–295.

[58] Stanley Milgram. 1963. Behavioral Study of obedience. *The Journal of Abnormal and Social Psychology* 67, 4 (1963), 371–378.

[59] Arwen Mohun. 2012. *Risk: Negotiating Safety in American Society.* JHU Press.

[60] Richard E Nisbett and Timothy D Wilson. 1977. The halo effect: Evidence for unconscious alteration of judgments. *Journal of Personality and Social Psychology* 35, 4 (1977), 250–256.

[61] Fran H Norris, Tenbroeck Smith, and Krzysztof Kaniasty. 1999. Revisiting the experience–behavior hypothesis: the effects of hurricane Hugo on hazard preparedness and other self-protective acts. *Basic and Applied Social Psychology* 21, 1 (1999), 37–47.

[62] Brian O'Neill, Adrian K Lund, Paul Zador, and Steve Ashton. 1985. Mandatory belt use and driver risk taking: An empirical evaluation of the risk-compensation hypothesis. In *Human Behavior and Traffic Safety*. Springer, 93–118.

[63] Brian O'Neill and Allan Williams. 1998. Risk homeostasis hypothesis: A rebuttal. *Injury Prevention* 4, 2 (1998), 92–93.

[64] Jan E Paradise, Jennifer Cote, Sara Minsky, Ana Lourenco, and Jonathan Howland. 2001. Personal values and sexual decision-making among virginal and sexually experienced urban adolescent girls. *Journal of Adolescent Health* 28, 5 (2001), 404–409.

[65] Malcolm R Pattinson, Marcus A Butavicius, Kathryn Parsons, Agata McCormac, and Cate Jerram. 2015. Examining Attitudes toward Information Security Behaviour using Mixed Methods.. In *International Symposium on Human Aspects of Information Security & Assurance*. Lesvos, Greece, 57–70.

[66] Rebecca Pedruzzi and Anne Swinbourne. 2009. "It won't happen to me:" optimism, biases, and recall of road-risk information. In *Proceedings of the Australian College of Road Safety Conference*. Perth, WA, Australia, 1–12.

[67] Sam Pelzman. 1975. The Effects of Automobile Safety Regulation. *Journal of Political Economy* 83, 4 (1975), 677–726.

[68] Colin Powell. 2007. The perception of risk and risk taking behavior: Implications for incident prevention strategies. *Wilderness and Environmental Medicine* 18, 1 (2007), 10–15.

[69] James O Prochaska, Carlo C DiClemente, and John C Norcross. 1992. In search of how people change: Applications to addictive behaviors. *American Psychologist* 47, 9 (1992), 1102.

[70] Kelvin Redolfo. 2000. What is homeostasis? *Scientific American* (January 2000).

[71] D Runcie and DA Seaver. 1991. *Inadequate Self-Discipline as a Causal Factor in Human Error Accidents.* Technical Report. DTIC Document.

[72] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. 2017. Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, 211–228.

[73] Fridulv Sagberg, Stein Fosser, and Inger-Anne F Sætermo. 1997. An investigation of behavioural adaptation to airbags and antilock brakes among taxi drivers. *Accident Analysis & Prevention* 29, 3 (1997), 293–302.

[74] Thomas Schlösser, David Dunning, and Detlef Fetchenhauer. 2013. What a feeling: the role of immediate and anticipated emotions in risky decisions. *Journal of Behavioral Decision Making* 26, 1 (2013), 13–30.

[75] USA Homeland Security. 2012. The Menlo Report. (2012).

[76] Herbert A Simon. 1957. *Models of Man; Social and Rational.* Wiley, New York.

[77] Lennart Sjöberg. 2000. Factors in risk perception. *Risk analysis* 20, 1 (2000), 1–12.

[78] Lennart Sjöberg, Bjørg-Elin Moen, and Torbjørn Rundmo. 2004. Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research. (2004). Rotunde publikasjoner. Norwegian University of Science and Technology, Department of Psychology.

[79] P Slovic. 1987. Perception of Risk. *Science* 236, 4799 (1987), 280–5.

[80] Paul Slovic. 1992. Perception of risk: Reflections on the psychometric paradigm. In *D. Golding and S. Krimsky (Eds.), Theories of Risk. New York: Praeger.*

[81] Paul Slovic, Melissa L Finucane, Ellen Peters, and Donald G MacGregor. 2004. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis* 24, 2 (2004), 311–322.

[82] Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein. 1986. The psychometric study of risk perception. In *Risk evaluation and management.* Springer, 3–24.

[83] Adam Smith. 2010. *The theory of moral sentiments.* Penguin.

[84] J Spring, T Moore, and D Pym. 2017. Practicing a Science of Security. In *New Security Paradigms Workshop (NSPW).* Santa Cruz, USA. October.

[85] Diederik A Stapel and Aart S Velthuijsen. 1996. "Just as if it happened to me": The impact of vivid and self-relevant information on risk judgments. *Journal of Social and Clinical Psychology* 15, 1 (1996), 102–119.

[86] Fredrick M Streff and E Scott Geller. 1988. An experimental test of risk compensation: Between-subject versus within-subject analyses. *Accident Analysis & Prevention* 20, 4 (1988), 277–287.

[87] Heikki Summala. 1996. Accident risk and driver behaviour. *Safety Science* 22, 1 (1996), 103–117.

[88] Wayne C Summers and Edward Bosworth. 2004. Password policy: the good, the bad, and the ugly. In *Proceedings of the Winter International Symposium on Information and Communication Technologies.* Trinity College Dublin, 1–6.

[89] Sıdıka Tekeli-Yeşil, Necati Dedeoğlu, Charlotte Braun-Fahrlaender, and Marcel Tanner. 2010. Factors motivating individuals to take precautionary action for an expected earthquake in Istanbul. *Risk Analysis* 30, 8 (2010), 1181–1195.

[90] Ulrich Tränkle and Christhard Gelau. 1992. Maximization of subjective expected utility or risk control? Experimental tests of risk homeostasis theory. *Ergonomics* 35, 1 (1992), 7–23.

[91] Rüdiger M Trimpop. 1996. Risk homeostasis theory: problems of the past and promises for the future. *Safety Science* 22, 1 (1996), 119–130.

[92] Alison G Vredenburgh and H Harvey Cohen. 1995. High-risk recreational activities: skiing and scuba — what predicts compliance with warnings. *International Journal of Industrial Ergonomics* 15, 2 (1995), 123–128.

[93] Merrill Warkentin, Robert E Crossler, and Nirmalee Malimage. 2012. Are You Sure You're Safe? Perceived Security Protection as an Enabler of Risky IT Behavior. In *Proceedings of the 2012 International Federation of Information Processing (IFIP) International Workshop on Information Systems Security Research, Dewald Roode Information Security Workshop.*

[94] Merrill Warkentin, Allen C Johnston, Eric Walden, and Detmar William Straub. 2016. Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems* 17, 3 (2016), 194–215.

[95] Merrill Warkentin, Zhengchuan Xu, and Leigh A. Mutchler. 2013. I'm Safer than You: The Role of Optimism Bias in Personal IT Risk Assessments. In *Proceedings of 2013 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, Niagara, NY, October.*

[96] Rick Wash and Emilee J Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *SOUPS*. 309–325.

[97] Neil D Weinstein. 1989. Effects of personal experience on self-protective behavior. *Psychological Bulletin* 105, 1 (1989), 31–50.

[98] Ryan West. 2008. The psychology of security. *Commun. ACM* 51, 4 (2008), 34–40.

[99] Gerald JS Wilde. 1982. The theory of risk homeostasis: implications for safety and health. *Risk Analysis* 2, 4 (1982), 209–225.

[100] Gerald JS Wilde, Stephen P Claxton-Oldfield, and Peter H Platenius. 1985. Risk homeostasis in an experimental context. In *Human Behavior and Traffic Safety*. Springer, 119–149.

[101] Gerald J S Wilde. 1985. Assumptions necessary and unnecessary to risk homoeostasis. *Ergonomics* 28, 11 (1985), 1531–1538.

[102] Jie Zhang, Brian J Reithel, and Han Li. 2009. Impact of perceived technical protection on security behaviors. *Information Management & Computer Security* 17, 4 (2009), 330–340.

[103] Philip G Zimbardo. 1972. Comment: Pathology of imprisonment. *Society* 9, 6 (1972), 4–8.

[104] Gregory D Zimet, Marcia L Shew, and Jessica A Kahn. 2008. Appropriate use of cervical cancer vaccine. *Annual Review Medicine* 59 (2008), 223–236.