Winter 12-11-2022

Risk compensation behaviors on cascaded security choices

Richard Henkenjohann
University of Goettingen, richard.henkenjohann@uni-goettingen.de

Manuel Trenz
University of Goettingen

Risk Compensation Behaviors on Cascaded Security Choices

Richard Henkenjohann[1] **and Manuel Trenz**
University of Goettingen
Goettingen, Germany

ABSTRACT

Organizations are interested in improving information security and make use of a range of technical, organizational, or behavioral measures. The different approaches to improving information security must not be viewed as being isolated, instead, different measures might influence each other. Security efforts fail when technical measures influence human behavior in a way that their security perceptions and behaviors are altered to the disadvantage of the security outcome. Those unintended consequences of information security practices can be classified as risk compensation behaviors, describing how users become more careless when they perceive some level of protection. This research in progress is interested in understanding risk compensation behaviors for cascaded security choices by different actors (e.g., security decisions made by organizations vs. decisions made by individuals) and presents a lab experiment to test this issue.

Keywords: Risk Compensation, Cascaded Security Choices, Rational Choice, Online experiment

[1] Corresponding author. richard.henkenjohann@uni-goettingen.de +49 551 39-21862

INTRODUCTION

"The more secure you make something, the less secure it becomes."
(Norman 2009)

Information Systems Security (ISS) is not a purely technical issue but, in fact, deals with technical, behavioral, managerial, philosophical, and organizational approaches to protect informational assets (Zafar and Clark 2009). The combined effects of all approaches determine the ultimate success of information security initiatives. Contrary to common assumptions, it is not necessarily the case that different measures add cumulatively to the overall ISS outcome but can have countervailing effects. For instance, technical measures such as security scanners for internet browsers do not protect against all risks (e.g., malicious data collection), but if technical measures are perceived as fully protective, less attentive behaviors may result. Those misperceptions indicate an undesirable interaction effect between technical and behavioral security measures. This would be the case, more generally speaking, if technical measures influence human behavior in a way that their security perceptions and behaviors are altered to the disadvantage of the security outcome. In addition, when technical measures are provided on an organizational level, individuals cannot fully understand the protective measure and are more likely to take mental shortcuts due to bounded rationality (Simon 1955).

Such behavioral realignments are known as risk compensation behaviors, in that people engage in more careless behaviors when they feel protected (Zhang et al. 2009). Research indicates risk compensation effects and shows that the perception of secure environments, whether through antivirus software or similar technical measures, results in lowered security behaviors and outcomes (Jardine 2020; Zhang et al. 2009). From a practical point of view, the observation that companies spend more on cyber security (Hiscox 2022) but, at the same time,

increasingly become victims of cyber-attacks (Accenture 2021) adverts advanced research on risk compensation behaviors. When risk compensation is an issue, investments in cyber security are better spent on behavioral than technical and organizational levels. From a theoretical perspective, even though risk compensation effects were observed and reported, it is still being determined how risk compensation differs when security measures are installed by individuals versus when an organization provides security measures. This distinguished view addresses conflicts in the literature and ultimately leads to understanding risk compensation in organizational settings. Taking this as a starting point, this research in progress asks: What are the impacts of endogenous vs. exogenously assigned technical ISS protection measures on individual risk-taking behaviors? This research-in-progress paper presents theoretical assumptions of risk compensation behaviors and proposes an online lab experiment to confirm corresponding effects.

RESEARCH ON RISK COMPENSATION IN INFORMATION SECURITY

In general, technical approaches and human behavior are interdependent: The decision to download files from the internet that pose an ISS risk might depend on whether antivirus software aiming at mitigating ISS risks is installed or not. Adjerid et al. (2018) introduce the concept of *cascaded (privacy) choices* in that a combination of "upstream" and "downstream" choices determine the ultimate behavioral outcome. Applying this nomenclature to the ISS context, upstream choices are being made *upfront*, e.g., the decision to install antivirus software, and *subsequent* downstream choices, e.g., to download files from the internet. As per this classification, upstream choices can be made either by individuals or assigned by organizations. These upstream and downstream choices are interdependent: the choice to download a file from the internet is influenced by the decision to install antivirus software and vice-versa. This

interdependence raises the question of whether individuals compensate for prior decisions in their downstream choices (Adjerid et al. 2018), thus engaging in riskier behaviors, and whether those compensation behaviors differ for endogenous vs. exogenous upstream decisions.

Some explanations in the literature show that risk compensation occurs and can void the effectiveness of upstream measures (Adjerid et al. 2018). The notion of behavioral information security is that people may undermine security due to convenience, ignorance, apathy, or risk calculations (Jardine 2020). In the case of risk compensation, technical measures improving ISS can make users feel safer, thus supporting riskier behaviors and voiding any positive effects of the security infrastructure (Jardine 2020).

Using rational choice theory (Becker 1968), we posit that risk compensation behaviors result from individual cost-benefit assessments. Rational choice theory has two basic assumptions: "(1) that decisions to offend are based on a balancing of both the costs and benefits of offending and (2) that what are important are the decision maker's *perceived* or subjective expectations reward and cost" (Paternoster and Simpson 1996, p. 553). The first assumption suggests that individuals choose cost-optimized options. In line with Adjerid et al. (2018), we posit that the balancing act also occurs for subsequent choices and that risk compensation behaviors shift costs of downstream behaviors to earlier choices. Costs involved in the balancing act of risk-taking may include the risks of data loss, formal and informal sanctions, or social censure from peers (Li et al. 2010), and the opportunity costs of missing information when neglecting ISS behaviors due to security concerns. The benefits of risk-taking include savings in time, convenience, and psychological needs fulfillment. The second assumption emphasizes the role of the individual and inter-individual (risk) perceptions that are subject to cognitive biases. Linked to the concept of bounded rationality (Simon 1955), individuals cannot fully assess the

functions of organizational-provided security measures and take mental shortcuts. As a result, the cost-benefit assessment is expected to differ for cases where upstream decisions are made by organizations or individuals.

Risk compensation behaviors in ISS have been examined in different contexts (e.g., Farahmand et al. 2008; Jardine 2020; Kearney and Kruger 2016; Pattinson and Anderson 2004; Renaud and Warkentin 2017; Zhang et al. 2009). For instance, Zhang et al. (2009) found that when individuals perceive high technical protection, they have a lower intention to comply with ISS. Based on a survey on ISS trust, Kearney and Kruger (2016) summarize that "[u]sers may become more careless […] when they know (or perceive) that adequate controls (e.g. spam filters) are in place." Recently, Jardine (2020) found that antivirus software users more often encounter cybersecurity events than nonusers due to risk compensation. However, to the best of our knowledge, no previous research demonstrated how risk compensation differs for endogenous vs. exogenous cascaded security choices.

PROPOSED RESEARCH

We plan to conduct an online experiment to find empirical evidence for risk compensation behaviors.

Hypotheses Development and Research Model

Organizations and individuals install ISS measures (e.g., antivirus software and backup mechanisms) to improve overall ISS outcomes. ISS measures not only add to an objective ISS protection but also change the user's perceptions about ISS security. Perceived ISS protection is the user's belief that the ISS measure is able to safeguard their system and personal information from security breaches (cf. Pavlou and Fygenson 2006). ISS risk beliefs are the expectation of high losses associated with unsafe ISS behaviors (cf. Malhotra et al. 2004). ISS measures add to

an individual's perception of ISS protection. At the same time, ISS measures might result in an overestimation of protection, thus lowering ISS risk beliefs. Hence,

H1a: ISS measure has a positive influence on perceived ISS protection.

H1b: ISS measure has a negative effect on ISS risk beliefs.

In line with rational choice theory, a balancing act of costs and benefits determines the behavioral outcome. We argue that perceptions of ISS protection offset the costs of risk-taking (e.g., risk of a data breach) through a sense of investment in ISS being made. When the offsetted costs through protection measures are higher than ISS risk beliefs (costs), one tends to risk-taking. Both factors determine the cost-optimized behavioral outcome. Hence,

H2: Perceived ISS protection has a positive effect on risk-taking.

H3: ISS risk beliefs have a negative effect on risk-taking.

We summarize our hypotheses in the research model of Figure 1.

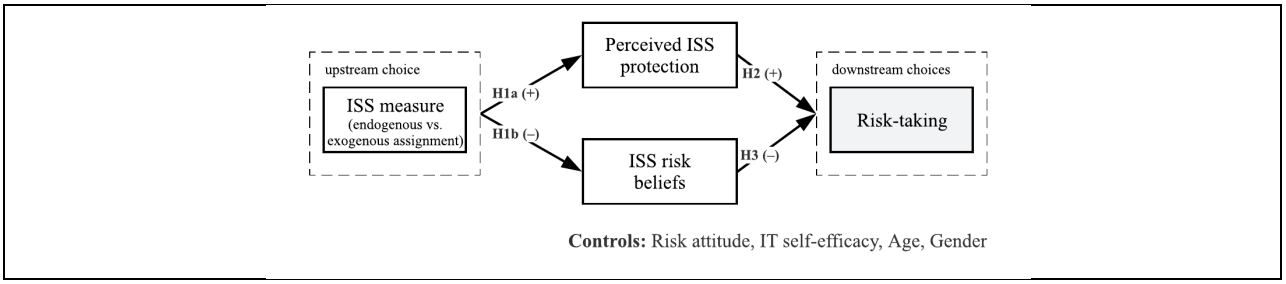

Figure 1. Summary of hypotheses to risk compensation for cascaded security choices.

Procedure

We propose an online lab experiment with a link-clicking scenario to test our hypotheses. Participants are given a research assignment and asked to write a summary of a given topic. They are shown a list of search results that are required to screen to fulfill the task. Each website displays a certain risk, allowing us to measure risk-taking by link-clicking. We incorporate a two-factor (ISS measure: endogenous vs. exogenous assignment) between-subjects design with repeated measures (ISS risk). After the task description, the participant is given the research task,

a text input, and a list of search results, each listing being equally relevant but differing in risk (repeated measures). The ISS risk is printed next to the listing as a percental value. Please consult Figure 2 for an illustration of the risk manipulations.

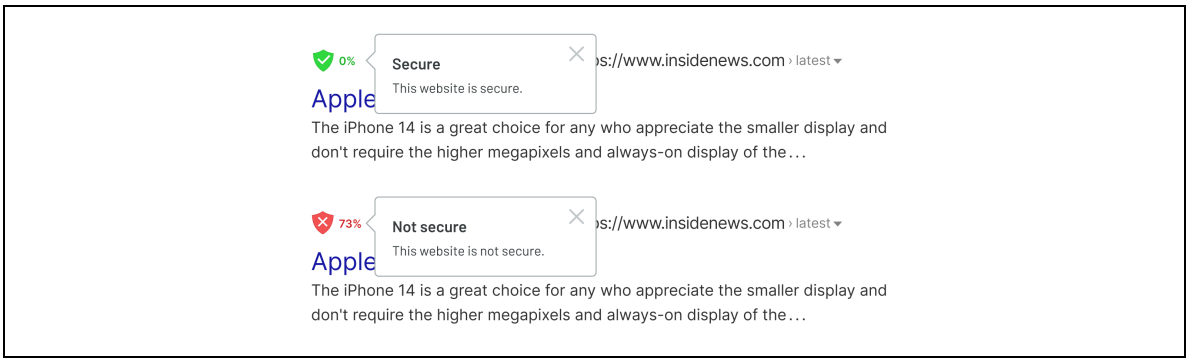

Figure 2. The ISS risk is implemented as a repeated measure. The screenshot shows how the presentation of ISS risk differs.

Participants are randomly assigned to either group "endogenous upstream choice," "exogenous upstream choice," or control. In either treatment condition, before opening the website, a "website scanner" will be shown, stating that the connection is secure after a short idle time[2]. In the "endogenous upstream choice" group, however, the measure must be enabled by the individual.

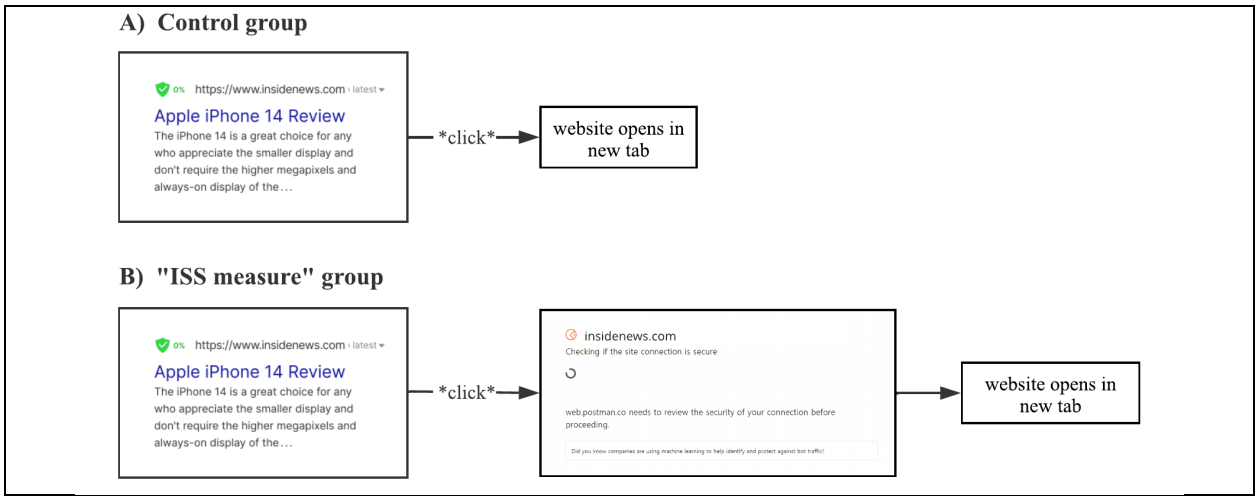

Figure 3. Between-subjects manipulation of ISS measure. In the treatment group, a "website scanner" is installed.

[2] The design of the "website scanner" is influenced by Cloudflare's commercial bot protection service.

Measures

The dependent variable. Risk-taking is operationalized as a link-click with the value of the actual ISS risk (0…1) when a user opens the website or 0 otherwise. We use a panel random effects regression.

Independent variables. Perceived ISS protection is measured using an adapted scale from Pavlou and Fygenson (2006). ISS risk beliefs are measured using a contextualized version of the risk beliefs scale from Malhotra et al. (2004). ISS measure, i.e., the upstream choice, indicates the experimental condition.

Control variables. *Risk attitude* is a significant determinant of risk-taking. We control for risk attitude using an adapted scale from Donthu and Gilliland (2002). Despite lacking evidence from Creese et al. (2013), we assume that *prior experience with a data breach* can lead to different risk perceptions, which is why we control for it. *IT Self-efficacy* controls for one's proficiency with IT in general and is measured using a shortened version from Compeau et al. (2022).

EXPECTED CONTRIBUTIONS

Our expected contributions are as follows: First, we contribute to the ISS and risk compensation literature by describing how decision-making processes differ for individual vs. organizational upstream decisions. Second, we contribute to practice by outlining how security measures in organizations must be designed to not offset any security efforts.

REFERENCES

Accenture. 2021. *Average Number of Cyber Attacks on Enterprise-Sized Companies Worldwide from 2020 to 2021*, Statista. (https://statista.com/de/statistics/1311781/average-number-of-cyber-attacks-per-company-worldwide/).

Adjerid, I., Acquisti, A., and Loewenstein, G. 2018. "Choice Architecture, Framing, and Cascaded Privacy Choices," *Management Science*, Mnsc.2018.3028. (https://doi.org/10.1287/mnsc.2018.3028).

Becker, G. S. 1968. "Crime and Punishment: An Economic Approach," in *The Economic Dimensions of Crime*, Springer, pp. 13–68.

Compeau, D., Correia, J., and Thatcher, J. B. 2022. "When Constructs Become Obsolete: A Systematic Approach to Evaluating and Updating Constructs for Information Systems Research," *MIS Quarterly* (46:2), pp. 679–711. (https://doi.org/10.25300/MISQ/2022/15516).

Creese, S., Hodges, D., Jamison-Powell, S., and Whitty, M. 2013. "Relationships between Password Choices, Perceptions of Risk and Security Expertise," in *Human Aspects of Information Security, Privacy, and Trust* (Vol. 8030), Lecture Notes in Computer Science, L. Marinos and I. Askoxylakis (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 80–89. (https://doi.org/10.1007/978-3-642-39345-7_9).

Donthu, N., and Gilliland, D. I. 2002. "The Single Consumer," *Journal of Advertising Research* (42:6), pp. 77–84. (https://doi.org/10.2501/JAR.42.6.77).

Farahmand, F., Atallah, M., and Konsynski, B. 2008. "Incentives and Perceptions of Information Security Risks," in *ICIS 2008 Proceedings*, Paris.

Hiscox. 2022. *Cyber Security as a Percentage of IT Spend among U.S. and European Companies from 2020 to 2022, by Country*, Statista. (https://statista.com/statistics/1245356/it-spend-on-cyber-security/).

Jardine, E. 2020. "The Case against Commercial Antivirus Software: Risk Homeostasis and Information Problems in Cybersecurity," *Risk Analysis* (40:8), pp. 1571–1588. (https://doi.org/10.1111/risa.13534).

Kearney, W. D., and Kruger, H. A. 2016. "Theorising on Risk Homeostasis in the Context of Information Security Behaviour," *Information and Computer Security* (24:5), pp. 496–513. (https://doi.org/10.1108/ICS-04-2016-0029).

Li, H., Sarathy, R., and Xu, H. 2010. "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems* (51), pp. 62–71.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355. (https://doi.org/10.1287/isre.1040.0032).

Norman, D. A. 2009. "When Security Gets in the Way," *Interactions* (16:6), pp. 60–63. (https://doi.org/10.1145/1620693.1620708).

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), p. 549. (https://doi.org/10.2307/3054128).

Pattinson, M. R., and Anderson, G. 2004. "Risk Homeostasis as a Factor of Information Security.," in *AISM*, Citeseer, pp. 64–72.

Pavlou and Fygenson. 2006. "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), p. 115. (https://doi.org/10.2307/25148720).

Renaud, K., and Warkentin, M. 2017. "Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact," in *Proceedings of the 2017 New Security Paradigms Workshop*, Santa Cruz CA USA: ACM, October, pp. 57–69. (https://doi.org/10.1145/3171533.3171534).

Simon, H. A. 1955. "A Behavioral Model of Rational Choice," *The Quarterly Journal of Economics* (69:1), p. 99. (https://doi.org/10.2307/1884852).

Zafar, H., and Clark, J. G. 2009. "Current State of Information Security Research In IS," *Communications of the Association for Information Systems* (24). (https://doi.org/10.17705/1CAIS.02434).

Zhang, J., Reithel, B. J., and Li, H. 2009. "Impact of Perceived Technical Protection on Security Behaviors," *Information Management & Computer Security* (17:4), pp. 330–340. (https://doi.org/10.1108/09685220910993980).