Risk Compensation in Home-User Computer Security Behavior: A Mixed-Methods Exploratory Study

Sarah Pearman
spearman@cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Arnab Kumar
arnabk@andrew.cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Nicholas Munson
nmunson@andrew.cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Charu Sharma
charusharma@cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Leeyat Slyper
lslyper@cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Jeremy Thomas
thomasjm@cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Lujo Bauer
lbauer@cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Nicolas Christin
nicolasc@andrew.cmu.edu
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213

Serge Egelman
egelman@cs.berkeley.edu
ICSI, 1947 Center St., Suite 600
Berkeley, CA 94704

Abstract

Risk homeostasis theory claims that individuals adjust their behaviors in response to changing variables to keep what they perceive as a constant accepted level of risk [8]. Risk homeostasis theory is used to explain why drivers may drive faster when wearing seatbelts. Here we explore whether risk homeostasis theory applies to end-user security behaviors. We use observed data from over 200 participants in a longitudinal in-situ study as well as survey data from 249 users to attempt to determine how user security behaviors and attitudes are affected by the presence or absence of antivirus software. If risk compensation is occurring, users might be expected to behave more dangerously in some ways when antivirus is present. Some of our preliminary data suggests that risk compensation may be occurring, but additional work with larger samples is needed.

Author Keywords

security; usable security; risk homeostasis theory; risk compensation

ACM Classification Keywords

H.1.2 [User/Machine Systems]: Human factors

Introduction

Risk homeostasis theory posits that people adjust their behaviors to compensate for factors that raise or lower risk in order to maintain a constant accepted risk level [8]. This theory is most often discussed in safety science literature. We are interested in understanding whether this theory can be applied to end-user computer security behavior. Insights from such work could inform interface design and behavioral interventions intended to improve users' security outcomes. Here, we combine in-situ observations with survey data and present some of the first research findings on the application of risk homeostasis theory to computer security behavior.

Our behavioral data from the Security Behavioral Observatory (SBO) sample offers a unique opportunity to observe unparalleled breadth and depth of ecologically-valid home-user behavioral data, and we are able to compare this data to self-reports from the same users as well as from a demographically-contrasting Mechanical Turk sample in an attempt to draw conclusions about the relationships between users' attitudes and their observed behaviors.

Background

In his work on risk homeostasis theory, Wilde [8] claims that individuals establish a target level of risk and then adjust behaviors in response to changing variables so that perceived risk continues to match the target level. This theory is most often applied to the study of traffic science: for example, it is employed to explain why drivers might be more likely to exceed speed limits while wearing seat belts. Janssen and Tenking [3] indicate that risk homeostasis theory can prove useful in the prediction of decision making even if complete stasis is not observed. This framework may be a useful tool for understanding the internal negotiations that lead end users towards unsafe behaviors.

In 2004, Pattinson and Anderson [4] were, to our knowledge, the first to apply risk homeostasis theory to computer security behavior, but little work has been done since to test related hypotheses in user studies. Here, we are interested in determining whether users are more likely to engage in specific risky behaviors (such as visiting unsafe websites or ignoring security patches) when they believe that they are protected by antivirus software. Some work does suggest that users engage in this type of risk compensation behavior: for example, one study found that the presence of antivirus made users more willing to run potentially-malicious software [1].

Methodology

We conducted a two-part exploratory study with both *in-situ* observation and survey data collection.

Study 1: In-situ data collection

First, we drew data from the Security Behavior Observatory (SBO, [2]), which has recorded longitudinal data about the computer states and behaviors of over 200 home Windows users over nearly two years. Users were divided into two groups: those whose machines showed evidence of active third-party antivirus software and those whose machines did not. We analyzed data regarding two variables: Windows update settings (automatic vs. non-automatic vs. disabled) and frequencies of visits to unsafe websites (based on data from the Google Safe Browsing API).

Study 2: Survey

Our survey asked users questions about their computer configuration and usage, including their usage of antivirus software. We also probed for attitudes and understandings regarding the purpose and usefulness of antivirus software. Finally, we requested basic demographic information.

	No AV	AV
Never cont.	47.5%	58.9%
Sometimes	47.5%	38.3%
Always	5.0%	1.0%

Figure 1: Browser warning reactions

	No AV	AV
W/in 1 day	7.7%	12.1%
Eventually	23.1%	29.0%
Never	5.1%	0.5%

Figure 2: OS update installation timeframes

	No AV	AV
W/in 1 day	35.1%	33.3%
Eventually	43.2%	51.2%
Never	0.0%	1.9%

Figure 3: Application update installation timeframes

The survey was deployed to both populations via SurveyGizmo. We obtained responses from 135 Mechanical Turk workers as well as 114 of the approximately 139 currently-active SBO participants.

Findings

Survey findings: Likert questions
Participants were asked to indicate their level of agreement or disagreement with several Likert statements relevant to security behaviors and usage of antivirus software. Some results from these items are highlighted below. Statistical results below are based on Pearson chi-squared tests and a significance level of 95% unless otherwise specified.

Participants who had antivirus installed were much more likely to agree that they worried about viruses on their computers (χ^2(1, N=223) = 13.325, p < .001). 67.9% of participants with antivirus agreed with the Likert statement regarding worrying about viruses, while only 33.3% of those without antivirus agreed with the statement. Participants who did not have antivirus software installed were also slightly more likely to agree that they were at low risk of getting a virus, but this relationship was not statistically significant (χ^2(1, N=184) = 1.328, p < .249)

Additionally, participants who had antivirus software installed were significantly more likely to agree that updates made their computers safer (χ^2(1, N=211) = 10.191, p = .001). As discussed below, this attitude did not always correspond to users' self-reports about update *behaviors*.

Survey findings: Browser warning questions
Most participants reported having seen browser warnings in the past. There was no significant relationship between having antivirus and having seen a browser warning (χ^2(3, N=247) = 1.643, p = .650). When asked about their reactions to browser warnings, users without antivirus were slightly more likely to report that they would sometimes or always continue past a warning, but this relationship was not significant (χ^2(3, N=249) = 5.659, p = .129).

Survey findings: Operating system update behavior
58% of participants reported that their operating systems updated automatically, and 41.2% said that their OSes did not update automatically. The latter group was then asked whether they installed updates "Within a day," "When I get around to it," or "Never" (with additional "I don't know" and "Other" options). Participants with antivirus were slightly more likely to choose "Within a day" or "When I get around to it," which would support the application of risk homeostasis theory, but the presence or absence of antivirus was not a statistically significant predictive factor for responses to this item (χ^2(4, N=246) = 8.321, p = .081).

Survey findings: Application update behavior
Participants were also asked specifically about updates to software other than the operating system. When asked about their timelines for installing software updates, approximately half of participants chose "When I get around to it." Participants with antivirus were slightly more likely to choose "When I get around to it," "Never," or "Other" for this question, while participants without antivirus were slightly more likely to choose "Within a day," but the results were not statistically significant (χ^2(4, N=244) = 4.265, p = .371).

Survey findings: Reasons for delaying updates
Participants were asked in open-ended questions on the survey why they chose to delay operating system and software updates. 25 of the 78 people asked (32.1%) said that they were in the middle of something at the time of update and therefore delayed the update to a later time. One respondent told us, "[I]f I sit down to use my computer, it's because I have a task in mind. I don't want to stop to do other things at that moment, including installing updates."

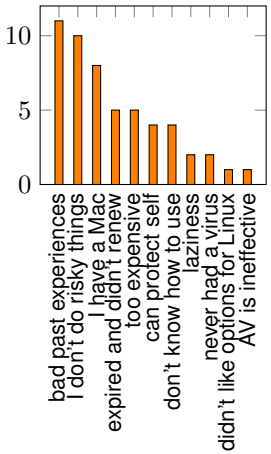

Figure 4: Reasons offered for not using antivirus software (as coded from survey free response items)

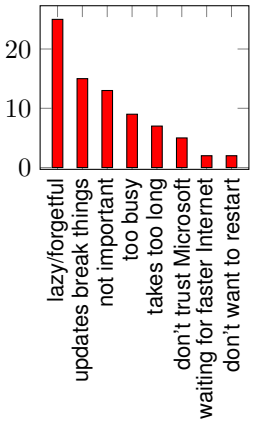

Figure 5: Reasons offered for delaying or declining OS updates (as coded from survey free response items)

Many respondents also claimed that laziness and time constraints were reasons they delayed updates, which is consistent with past findings regarding update avoidance [5, 6, 7]. Some users also cited fears that updates might cause problems or mentioned wanting “to make sure it’s real" as reasons for delaying updates. This is less discussed in past findings, and we believe that this may result from users over-extending the application of common advice such as “don’t install unknown programs." Future work is needed to understand whether users are confusing updates with new software and are putting themselves at more risk while trying to exercise caution.

Survey findings: Past experience with viruses

Overall, 65.8% of participants reported having had viruses or malware on their computers in the past. The presence of antivirus software was strongly predictive of responses to this question ($\chi^2(2, N = 234) = 14.898, p = .001$). Of participants with antivirus, 70.7% reported past experience with viruses, while only 38.9% of participants without antivirus had ever had viruses.

In-situ data: Update settings

Based on Windows registry data on installed software, SBO client machines were sorted into two groups: those that appeared to have third-party antivirus installed, and those that did not. These two groups were compared using Mann-Whitney U tests to determine whether the presence of antivirus was a predictive factor for the update settings on the computer, the absolute number of malicious websites visited on the machine during data collection, or the ratio of malicious websites visited to total websites visited.

90.3% of users had automatic updates fully enabled. 1.4% were set to “notify before installation" and 3.7% to “notify before download." Small portions of the sample had updates “not configured" (0.9%) or fully disabled (3.7%). Users with antivirus were slightly more likely than those without antivirus to have updates fully disabled (4.5% versus 1.7%), but presence of antivirus was not a statistically significant predictive factor (χ^2(4, N=216) = 6.208, p = .184).

In-situ data: Browsing behavior

19 participants out of 191 with relevant browsing data (9.9%) had visited at least one website on the Google Safe Browsing blacklist during the course of data collection. No significant relationship was detected between the presence/absence of antivirus and either the absolute count of malicious websites visited or the ratio of malicious to total websites visited. Those with antivirus had slightly higher absolute counts, but those without antivirus had slightly higher ratios of malicious to total websites visited. However, the differences in the absolute counts between the two groups were not statistically significant (Mann Whitney U, *U* = 3474.0, p = .908). The differences between the ratios of malicious to total websites between the two groups were also barely detectable and probably attributable to chance based on a Mann Whitney U test (*U* = 3464.5, p = .982).

Conclusion

Users with antivirus were more likely to have OS updates fully disabled and were more likely to delay or decline software updates, which hints risk homeostasis theory might hold. However, our results on other measures were conflicting, and not all results were statistically significant, so further work with larger samples is needed. We also intend to delve deeper in our in-situ data to distinguish users with fully-functional anti-virus from those with non-functional security software (e.g., outdated definitions or unpaid subscriptions) as well as to obtain precise metrics regarding users’ delays in installing updates.

REFERENCES

1. N. Christin, S. Egelman, T. Vidas, and J. Grossklags. 2011. It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice. In *Proceedings of the 15th International Conference of Financial Cryptography and Data Security (FC '11)*. https://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf
2. A. Forget, S. Komanduri, A. Acquisti, N. Christin, L.F. Cranor, and R. Telang. 2014. *Security Behavior Observatory: Infrastructure for Long-Term Monitoring of Client Machines*. Technical Report. Carnegie Mellon University CyLab. https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14009.pdf
3. W. Janssen and E. Tenkink. 1988. Risk Homeostasis Theory and its Critics: Time for an Agreement. *Ergonomics* 31, 4 (1988), 429–433. DOI: http://dx.doi.org/10.1080/00140138808966689
4. M.R. Pattinson and G. Anderson. 2004. Risk Homeostasis as a Factor of Information Security. In *Proceedings of the 2nd Australian Information Security Management Conference*. School of Management Information Systems, Edith Cowan University, Perth, Western Australia, 64–72.
5. K. Vaniea, E. Rader, and R. Wash. 2014. Betrayed By Updates: How Negative Experiences Affect Future Security. In *Proceedings of the 32nd Annual Conference on Human Factors in Computing Systems (CHI '14)*. ACM, 2671–2674.
6. K. Vaniea and Y. Rashidi. 2016. Tales of Software Updates: The Process of Updating Software. In *Proceedings of the 34th Annual Conference on Human Factors in Computing Systems (CHI '16)*. ACM.
7. R. Wash, E. Rader, K. Vaniea, and M. Rizor. 2014. Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS '14)*. 89–104.
8. G.J.S. Wilde. 1998. Risk Homeostasis Theory: An Overview. *Injury Prevention* 4 (1998), 89–91.