Replication: Application of Security Attitudes Scale to Japanese Workers

Takeaki Terada, *Fujitsu Limited*, Kazuyoshi Furukawa, *Fujitsu Limited*

Abstract

The SA-6, a six-item scale for assessing people's security attitudes, measures the attitude toward security measures, and consists of only six questions. However, since the SA-6 was developed based on the response data of Americans, it is not clear whether it correlates with actual security behavior for Japanese as well as the original paper. Also, in 2020, COVID-19 may have increased security attitudes as more people are now working remotely. Therefore, we applied the SA-6 to Japanese and Americans. As a result, we confirmed the correlation for the Japanese, but not for the Americans. We also confirmed the growing security attitudes. In addition, we conducted a survey on SA-13 (an extended version of SA-6), which is being developed by the authors of SA-6. As a result, we confirmed that there is a correlation between SA-13 and actual security behavior for both Japanese and Americans.

1. Introduction

The SeBIS (Security Behavior Intentions Scale) [1] is a well-known set of questions that quantitatively measures the behavioral performance of security measures. Specifically, it measures the frequency of taking specific security measures, such as locking the screen with a password when leaving the seat or checking the URL of a link. However, the frequency of security measures varies depending on the devices and applications that people use. For example, when it comes to screen locks, if a person has two devices and one of them has facial recognition, he or she will probably use a password less often. In addition, if you have installed a highly reputable security service and have full confidence in it, you are unlikely to check the URLs in advance yourself. In response to the above issues, Fakralis et al [2] developed a set of questions aimed at measuring users' threat avoidance in various situations by asking them about their attitude toward security measures, such as beliefs and emotions.

However, since the SA-6 was developed using responses from Americans, it is not clear whether it will correlate with actual security behavior for Japanese as well as the results in the original paper. When considering security measures for our company, which is mainly based in Japan, if we can use SA-6 to understand the security attitude of our employees, we can spend the budget on measures for departments with many employees with relatively low attitudes. It is also possible that many people began to work re-motely due to COVID-19, and that their security attitudes increased due to requests from their organizations to comply with PC usage rules. Therefore, we conducted a survey of Japanese and Americans as of the year 2020.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8 -- 10, 2021, Vancouver, B.C., Canada.

2. Related Work

2.1. Original paper

To estimate a user's ability to evade various security threats, regardless of the device or app they are using, it is important to capture the attitude of users toward security measures. Therefore, many studies have been conducted to capture this attitude, but most of them were qualitative analyses using interviews. Faklaris et al. developed SA-6, to measure attitudes in a quantitative and less time-consuming way [2]. In developing the scale, they first prepared 48 questions based on extensive research on attitudes toward various things in psychology and previous research on users' perceptions of security measures. These questions were then narrowed down to six items through multiple rounds of questionnaire surveys to complete the SA-6. Validation of the SA-6 using the U.S. Census-tailored panel (N=209) showed that the SA-6 was significantly correlated with the SeBIS (Security Behavior Intentions Scale), which measures security behavior intention. The SA-6 was also significantly correlated with previous research measures of privacy awareness, impulsivity, and self-efficacy. In addition, the SA-6 score varied according to the presence or absence of cyber victimization experience, age, gender, education, and household income, and was also correlated with actual security behavior.

2.2. Modern context

Like SA-6, Vishwanath et al. [3] proposed the concept of "cyber hygiene" based on the concept of public health to measure the attitude toward security measures. Cyber hygiene proposes a methodology to develop a scale to measure the level of awareness of security measures, rather than the security behavior itself, by using a set of questions that are independent of the devices, apps, services, or organizations people are using or working for. Vishwanath et al. developed the Cyber Hygiene Inventory (CHI), an 18-item psychometric scale to measure the attitude toward security measures, based on the concept of cyber hygiene. The results show that the CHI is positively correlated with cyber security self-efficacy, analytical thinking based on knowledge possessed, and non-impulsive behavior when shopping online.

While Faklaris et al. showed that the attitude toward security measures as measured by SA-6 is correlated with the intention and actual behavior of implementing security measures, Al-Shanfari et al. [4]took a different approach to analyze these correlations. They integrated the literature with statistical analyses of psychological factors that influence the intention to take security measures and actual behavior. The results showed that regardless of cultural differences such as cronyism, carelessness, and fear of losing face, the intention and actual behavior of security measures are universally influenced by psychological factors such as subjective norms, attitudes, perceived vulnerability, and self-efficacy.

In addition to psychological factors and incentives, there is also "herd mentality" as a determining factor for people to take security measures. This is the concept that the information that "many people are taking this measure" has a significant impact on people's behavior. Vedadi et al. [5] succeeded in promoting security countermeasure behavior by artificially providing this herd mentality-based stimulus to the experimental group.

3. Preliminarries

3.1. SA-6

The SA-6 consists of the following six questions (Table 1). The response options are on a 5-point Likert-type agreement scale (1=Strongly disagree, 5=Strongly agree).

Table 1: SA-6 scale items

	Items
Q1	I seek out opportunities to learn about security measures that are relevant to me.
Q2	I am extremely motivated to take all the steps needed to keep my online data and accounts safe.
Q3	Generally, I diligently follow a routine about security practices.
Q4	I often am interested in articles about security threats.
Q5	I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.
Q6	I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

3.2. SA-13

SA-13 [6] is a scale under development by the authors of SA-6 and is an extended version of SA-6. SA-13 is an extension of SA-6 with the addition of the following four questions on resistance and three questions on concern for security (Table 2, 3). Questions 7-10 are reversal questions. When analyzing them together with other questions, it is necessary to reverse the response values. In other words, answer values 1, 2, 3, 4, and 5 should be read as 5, 4, 3, 2, and 1.

Table 2: 'Resistance' in SA-13 scale items

	Items
Q7	I am too busy to put in the effort needed to change my security behaviors.
Q8	I have much bigger problems than my risk of a security breach.
Q9	There are good reasons why I do not take the necessary steps to keep my online data and accounts safe.
Q10	I usually will not use security measures if they are inconvenient.

Table 3: 'Concernedness' in SA-13 scale items

	Items
Q11	I want to change my security behaviors to improve my protection against threats (e.g. phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.
Q12	I want to change my security behaviors in order to keep my online data and accounts safe.
Q13	I worry that I'm not doing enough to protect myself against threats (e.g. phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.

3.3. Recalled security actions in the past week

Faklaris et al. developed RSec (Recalled Security Actions) [7], a set of nine questions asking about security actions in the last week, to examine the correlation between SA-6 and actual security actions (Table 4). The response options are "Yes", "No", "I'm not sure", "NA" (this question does not apply to me), and NA responses were excluded from the analysis.

Table 4: Questions of 'Recalled Security Actions'

	Items
R1	In the past week, I have changed a password for at least one of my online accounts.
R2	In the past week, I have downloaded and installed at least one available update for my computer's operating system within 24 hours of receiving a notification that it was available.
R3	In the past week, I have left my laptop or desktop computer unlocked at least once when I walked away from it.
R4	In the past week, I have used a password/passcode at least once to unlock my tablet.
R5	In the past week, I have used at least one password that contains 10 or more characters.
R6	In the past week, I have used the exact same password for at least two online accounts.
R7	In the past week, I have verified at least once that I am running antivirus software that is fully updated.
R8	In the past week, I have verified that at least one app or software program that I use is fully updated.
R9	In the past week, I have verified the URL of at least one internet link that I received in email before deciding whether to click on it.

4. Research Questions

Due to COVID-19, many people have started to work remotely. At the same time, they are required by their organizations to be more compliant with PC usage rules. As a result, their security awareness may have increased, regardless of age, gender, etc. Therefore, we formulate the following hypothesis.

H1: Compared to the survey conducted by Faklaris et al. in 2018, there will be no difference in SA-6 scores in this 2020 survey, regardless of age, gender, education, or household income.

In addition, while the request for compliance with PC usage rules raises security awareness, we believe that many people will act without locking their screens regardless of their security awareness because the need to lock their PC screens is diminished when working at home. Therefore, we formulate the following hypothesis.

H2: The correlation between SA-6 scores and RSec will be weaker in this 2020 study compared to the study conducted in 2018 by Faklaris et al.

5. Method

This section provides details on the survey targets and questionnaires for applying SA-6 to people in the year 2020.

5.1. Survey targets

The survey was conducted in December 2020 among Japanese and US citizens. The Japanese respondents were 18 years of age or older, living in Japan, and working at a company where their work is mainly done on a PC (regardless of whether they hold a position or not, and regardless of the type of business or industry). For Americans, the target population was people over 18 years old and living in the United States. The recruitment process was conducted using Amazon Mechanical Turk (MTurk for short). We did not add the "Masters Qualification" condition. The reason for this is that we wanted to include users who are not careless about security as a possible target of this survey. The reason for the difference in recruitment conditions between Japanese and American applicants is described below. For the Japanese, as mentioned in the introduction section, we added company employees to the recruitment criteria to use the SA-6 to identify departments with many employees with low security awareness. For the Americans, we aligned the recruiting conditions to the same conditions as in the study by Faklaris et al. This would allow us to examine the impact of the spread of remote work triggered by COVID-19 on the SA-6 score.

5.2. Composition of the questionnaire

In addition to the SA-6, the questionnaire included questions about the victimization experience and knowledge of victimization cases of themselves and their acquaintances, age, gender, education, annual income, and actual recalled security actions in the past week), based on the questionnaire used by Faklaris et al. In addition, a question to detect invalid respondents (one question) and the SA-13 (a measurement scale being developed by the authors of the SA-6, an extended version of the SA-6) were included in the questionnaire. We commissioned a major Japanese research firm to conduct the survey for us. The compensation for MTurk users living in the U.S. was set at $2.00 based on the response time of the preliminary survey with a small number of respondents (median: 12 minutes) and the market price of compensation for other HIT (Human Intelligence Task). The available response time was set at 30 minutes to avoid rushing respondents.

5.3. Translation of the questionnaires

We decided on the Japanese translation of SA-6, SA-13, and RSec after reviewing the translation results from paid translation services and by our research team of eight members.

5.4. Ethics

For the questionnaire survey, we explained the contents to our company's Ethics Review Committee and obtained their approval that the survey would not infringe on the privacy of the respondents.

6. Results

6.1. Factor structure of security attitudes

6.1.1. Factor structure of SA-6

The results of the exploratory factor analysis (EFA) showed that there was one potential common factor indicated by the responses to the SA-6 for both Japanese and Americans. This result is in line with Faklaris's design.

The results of the confirmatory factor analysis (CFA) showed that the CFI (Comparative Fit Index; 0.9 or higher is desirable) and SRMR (Standardized Root Mean Square Residual; 0.08 or lower is desirable) were 0.97 and 0.94 for the American respondents and 0.98 and 0.03 for the Japanese respondents, respectively. The one-factor model of SA-6 was also supported in this study.

6.1.2. Factor structure of SA-13

The results of the exploratory factor analysis (EFA) showed that there were three potential common factors indicated by the responses to the SA-13 for both Japanese and Americans. This is the same structure of the SA-13 as reported by Faklaris et al., but the breakdown was different in the Japanese data (Table 5).

Table 5: Factor analysis results for SA-13 responses by Japanese

SA-13		Factor loading			Alpha if item deleted
	Subscale				
Q1	SA-6 (Engagement & Attentiveness)	0.21	**0.60**	-0.07	0.66
Q2		**0.65**	0.37	0.14	0.65
Q3		0.29	**0.51**	0.06	0.66
Q4		**0.66**	0.33	0.12	0.65
Q5		**0.79**	0.12	0.05	0.66
Q6		**0.83**	-0.07	-0.04	0.68
Q7	Resistance	0.33	-0.11	**0.73**	0.73
Q8		-0.37	0.05	**0.46**	0.77
Q9		-0.33	0.18	**0.71**	0.76
Q10		-0.31	-0.10	0.21	0.78
Q11	Concerned ness	0.04	**0.82**	0.09	0.66
Q12		0.11	**0.70**	0.05	0.66
Q13		-0.18	**0.68**	-0.33	0.70

6.2. Differences in SA-6 scores between groups

We used the same groupings as in Faklaris et al.'s analysis for security breach experience (TFV: Themselves falling victim to a security breach) and experience of seeing or hearing about security breaches (CF: Close friends or relatives falling victim to a security breach; HSB: Heard about security breaches in the past year), age, gender, education (CA: College Attendance), and household income, and analyzed the difference in the mean SA-6 scores between the groups (Table 6). We tested the differences between the groups using Mann-Whitney U test because most of the data distributions of each group did not satisfy equivariance and normality. As a result, there were no statistically significant differences in "Gender" and "CA" for both Japanese and American data. Therefore, the hypothesis “H1” that the SA-6 score of people in 2020 is independent of age, gender, education, and household income is generally supported.

6.3. Correlation between RSec and security attitudes

6.3.1. Correlation between RSec and SA-6

We examined the correlation between the SA-6 score and the RSec score (calculated as 2 points for "Yes", 1 point for "No" and "Not Sure", and 0 points for 'NA') using Spearman's correlation coefficient r. The result for Japanese was r=.295, p<.001, which was weaker than Faklaris et al.'s result (r=.398, p<.001). For Americans, the correlation was r=-0.090, p=0.19, and no correlation was found. Therefore, the hypothesis “H2” that the correlation between SA-6 scores and RSec will be weaker in 2020 than in 2018 is valid for both Japanese and Americans.

6.3.2. Correlation between RSec and SA-13

We also examined the correlation between SA-13 and RSec, and found r=.358, p<.001 for the Japanese data and r=.230, p<.001 for the American data, indicating that there was a significant correlation between SA-13 and RSec for both data. As for the reason why, the correlation is stronger than that of SA-6, SA-13 includes a question asking about "resistance" to security measures, and we expect that this may have influenced the correlation with RSec.

Table 6: Means, standard deviations, and test of difference for security breach experience and demographic variables. TFV: Themselves falling victim to a breach; CF: Close friends or relatives falling victim to a breach; HSB: Heard about security breaches in the past year; CA.: College attendance; Income: household income; n.s.: not significant

	2020 JP (N=219)			2020 U.S.(N=208)		
	SA-6 Mean（SD）		p	SA-6 Mean（SD）		p
	Low	High		Low	High	
TFV	2.91 (.64)	3.18 (.47)	p<.05	3.58 (.86)	3.97 (.46)	p<.005
CF	2.90 (.63)	3.18 (.51)	n.s.	3.55 (.74)	3.96 (.26)	p<.001
HSB	2.70 (.54)	3.23 (.56)	p<.001	3.06 (.67)	3.91 (.38)	p<.001
	18-39	40+		18-39	40+	
Age	2.75 (.61)	3.14 (.55)	p<.001	3.76 (.54)	3.78 (.49)	n.s.
	Male	Female		Male	Female	
Gender	2.99 (.55)	2.89 (.69)	n.s.	3.79 (.44)	3.71 (.69)	n.s.
	No college	Attend.college		No college	Attend.college	
CA	2.79 (.54)	2.98 (.63)	n.s.	3.59 (.64)	3.78 (.52)	n.s.
	Below $25K	Abobe $25K		Below $25K	Abobe $25K	
Income	2.78 (.64)	2.95 (.70)	n.s.	3.52 (.65)	3.81 (.49)	p<.05

7. Discussion

We will discuss why there was no correlation between SA-6 and RSec for Americans. As a result of analyzing the difference in SA-6 scores between the "Yes" group and the "No or Not sure" group for each RSec question, no difference was found for six of the nine RSec questions Here we will discuss our views on some of them, namely “R1” and “R4”. The rest of the questions could not be reasonably interpreted, so we will leave them for future work. “R1” asks whether people change their passwords frequently. In 2017, NIST stated in its "Guidelines for Electronic Authentication" that it is more important to have strong passwords than to change them regularly [8], and this was widely reported by the news media. Therefore, it is possible that more people who got to know this information stopped changing their passwords frequently. “R4” asks whether passwords/passcodes are used to lock tablet screens, but it is possible that more people will be working from home in 2020, and that more people will not need to lock their screens.

Acknowledgement

We would like to thank Faklaris et al., the authors of SA-6, for their kind permission for this replication. And we also would like to thank Prof. A. Kanaoka from Toho University for his valuable comments.

References

[1] S. Egelman, E. Peer, Scaling the security wall. Developing a security behavior intentions scale (SeBIS). Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM, pp. 2873–2882. April 2015.

[2] C. Faklaris, L. Dabbish, and J. I. Hong. A Self-Report Measure of End-User Security Attitudes (SA-6). in the Proceedings of the Fifteenth Symposium on Usable Privacy and Security, Aug. 2019.

[3] A. Vishwanath, L. Seng N., P. Goh, S. Lee, M. Khader, G. Ong, and Jeffery Chin. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems vol. 128, Jan. 2020.

[4] I. Al-Shanfari, W. Yassin, and R. Abdullah. Identify of Factors Affecting Information Security Awareness and Weight Analysis Process. International Journal of Engineering and Advanced Technology (IJEAT). ISSN: 2249 – 8958, Volume-9 Issue-3, Feb. 2020.

[5] A. Vedadi, and M. Warkentin. Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions. Journal of the Association for Information Systems (JAIS), vol. 21(2), pp.428-459, 2020.

[6] The SA-13 scale. https://socialcybersecurity.org/

[7] The RSec inventory. https://socialcybersecurity.org/

[8] NIST Special Publication 800-63B https://pages.nist.gov/800-63-3/sp800-63b.html