Security Behavior Intention of Employees with Hearing Difficulties: An Empirical Comparison Study

Wisdom Umeugo *wumeugo@gmail.com*
Ph.D. University of the Cumberlands
Independent Researcher
Ottawa, Canada

Abstract

Human factors are frequently cited as the weakest link in the information security defense chain. Numerous studies have characterized employees as potential insider threats. Yearly industry reports persistently cite unsafe employee behavior as a leading cause of vulnerabilities and data breaches, especially in security-critical sectors such as the education, finance, government, information technology, legal, and medical sectors. Organizations spend vast sums on information security awareness (ISA) programs to improve employee security behavior. Employee security behavior intentions (SeBI) must be measured as part of gauging and tuning the effectiveness of ISA programs. Many studies measuring employee SeBI independently and as part of general employee ISA measurements have focused on homogenous populations, performing varying analyses based on information security experience, position, academic program, age, gender, and education levels. None have provided insights from the standpoint of deafness and hearing issues. This study surveyed employees in the education, finance, government, information technology, legal, medicine, military, and Policing sectors for their self-reported SeBI. The resulting SeBI scores were average. No statistically significant difference in SeBI scores was found between groups with and without hearing difficulties, although SeBI scores were slightly less for employees with hearing difficulties. The results suggested that more ISA training is needed for employees in the surveyed sectors.

Keywords: Information Security Awareness, Security Behavior, SeBIS, Deaf Security Awareness.

1. INTRODUCTION

The number and sophistication of cybersecurity attacks and information security breaches have risen over the years (Nastasiu, 2016). Organizations are in a never-ending race to keep their security systems updated. Some employment sectors are highly targeted due to the value of the data they process, store and transmit. This is reflected in various industry cybersecurity reports. Check Point Software (2022) reported that the education industry was the most attacked globally in the third quarter of 2021. CloudSek (2022) stated that the government sector was the prime target for cybercriminals in 2022. Ransomware attacks notoriously target the healthcare industry(check Point Software, 2022; PurpleSec, 2022). The healthcare industry has the highest number of ransomware attacks, with data breaches costing the US healthcare industry about $6.2 billion annually (check Point Software, 2022; PurpleSec, 2022). The financial and military sectors are also high-value targets of malicious attacks. According to PurpleSec (2022), in 2022, 67% of financial institutions reported an increase in cyberattacks. Check Point Software (2022) revealed that the government and Military were the second most attacked industry in 2022, increasing by as much as 20% from the previous year. Despite all the technology and tools deployed to improve information security, the human element remains the weakest link in the security chain and a source of critical security vulnerabilities (Griffiths, 2023). Almost 82% of successful data breaches involved a human element (Griffiths, 2023). Social engineering attacks that exploit human vulnerabilities caused about 41% of higher education breaches, and employee negligence caused about 81% of healthcare cyber security incidents (PurpleSec, 2022). Improper usage or

violation of acceptable usage policies by authorized users was the cause of about 31% of security incidents in Federal agencies (U.S. Government Accountability Office, 2020). Various research has emphasized the importance of human factors in information security (Cuchta et al., 2019; Kadena & Gupi, 2021; Nifakos et al., 2021; Pollock, 2017; Prabhu & Thompson, 2022; Rahman et al., 2021). Regardless of the sophistication of any security implementation, the lack of employee security awareness and poor security behavioral intentions will be its weakest link (Badie & Lashkari, 2012).

Promoting employees' information security awareness (ISA) has become integral to protecting organizations from cyber threats (Parsons et al., 2017). Organizations now institute information security awareness programs to correct unsafe information security behaviors of their employees. While research published on employee ISA measurement efforts have focused on homogenous populations frequently segmented by information security experience, position, academic program, age, gender, and education levels, none have provided insights from the standpoint of deafness and hearing issues (Alzamil, 2012; Arisya et al., 2020; Farooq et al., 2015; Filippidis et al., 2018). Murbach (2019) noted the dearth of cybersecurity research considering deafness and hearing difficulties, advocating for more cybersecurity research to include the deaf population. Very little is understood of deaf experiences and awareness in security practices (Murbach, 2019). Information security awareness training programs' effectiveness can be determined for employees with hearing difficulties if their awareness is estimated and compared to their hearing counterparts. This will help determine if information security awareness programs should be tailored more effectively for employees with hearing difficulties. This study attempts to estimate the impact of hearing difficulties on the security behavior intention (SeBI) of employees in security-critical education, finance, government, information technology, legal, medicine, military, policing, and the STEM sector. The results of this study will help inform information security managers in security-critical sectors of the need to develop more effective and inclusiveISA programs.

2. BACKGROUND AND LITERATURE REVIEW

Behavioral Intentions are often studied in information security and information systems research as a precursor of planned behavior (Egelman et al., 2016; Jenkins et al., 2021). Several studies have shown behavioral intention to correlate positively with intended behavior, such as adoption, use behavior, and policy compliance (Chao, 2019; Egelman et al., 2016; Mosleh et al., 2020; Shropshire et al., 2015). Jenkins et al. (2021) noted that although positive correlations may exist between behavioral intention and actual behavior, there are situations where users with positive behavioral intent do not undertake the expected behavior. In information security, this disparity between intention and actual behavior may be due to usability problems of security controls (Egelman et al., 2016). Security behavior intention has also been shown to correlate positively with ISA awareness (Moletsane & Tsibolane, 2020; Ngoqo & Flowerday, 2014).

Existing studies on behavioral intention have focused on determining the factors impacting behavioral intentions to undertake specific behaviors. Several of these studies have based their factors on theories such as the Theory of Planned Behavior (TPB), Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Conservation of Resource theory (COR), extended Unified Theory of Acceptance and Use of Technology (UTAUT), and General Deterrence Theory (GDR) (Chao, 2019; Hong et al., 2023; Lebek et al., 2014). Among the theories, the TPB deals directly with perceived behavioral intention, making it the widely applied behavioral intention theory in information systems research. However, this descriptive study estimates security behavioral intention as actual scores. Estimating security behavior intentions are typically part of information security awareness (ISA) measurements and are performed using various measurement instruments. Since ISA training is conducted to improve employees' knowledge, attitude, and behavior toward information security, ISA measurement scales are often based on the Knowledge Attitude Behavior (KAB) dimensional awareness model. Examples of published KAB-based ISA measurement instruments are the awareness measurement prototype by Kruger and Kearney (2006) and the Human Aspects of Information Security Questionnaire (HAIS-Q)

proposed by (Parsons et al., 2014). Other scales not based on KAB have been published, such as the Security Behavior Intentions Scale (SeBIS) developed by Egelman and Peer (2015) for measuring SeBI.

Various research has been published directly estimating and reporting the SeBI scores of various demographic populations. Kruger and Kearney (2006) demonstrated their prototype awareness measurement tool by surveying employees of an Australian company's regional office. Their tool consisted of the three dimensions of KAB and six focus areas: adherence to policies, keeping passwords secret, e-mail and internet, mobile equipment, reporting security incidents, and actions and consequences. Weightings of 30, 20, and 50 were assigned to the knowledge, attitude, and behavior dimensions, respectively. The tool expressed awareness measurements in percentage values. Scores between 80-100% were rated good awareness level, 60-79% rated average, and 59 and less judged to be poor awareness. The calculated score on the behavior dimension was 54%, an average score for the surveyed region.

Candiwan et al. (2022) evaluated the ISA levels of 317 telemedicine application users in Indonesia using HAIS-Q. Candiwan et al. (2022) assigned weights of 30%, 20%, and 50% to the knowledge, attitude, and behavior dimensions, respectively. The awareness criteria level of the study was 77.7% - 100% for good awareness level, 55%-77.7% for average awareness, and 33.3% - 55.5% for poor awareness. The study recommended immediate remediation action for average and poor awareness levels. The scores in the behavior focus areas were all found to be good. Participants scored 95% overall in the behavior awareness dimension.

Salem et al. (2021) evaluated the ISA level of 200 Palestinian students using HAIS-Q with five focus areas: password, social media, email use, mobile devices, and social engineering. A scale based on the mean score was used to assess the ISA level, where a mean score above 4.5 was judged to be a high awareness level, a score between 4.0 and 4.5 was an average awareness score, and mean scores below four were judged to be low. Respondents were found to have a mean score of 4.35 in the behavior dimension, which was an average score.

Puspitaningrum et al. (2018) measured the ISA levels of employees of the Ministry of Communication and Information Technology of the Directorate General of Resources Management and Postal and Information Technology Equipment, Indonesia. A survey consisting of seventy-two 5-point Likert scale HAIS-Q questions covering eight focus areas across KAB dimensions was administered to a sample of 28 employees. The total score of the behavior dimension was 78.96%, considered a medium score (60%-79%). The total score across the knowledge and attitude dimensions was also medium.

Fadhilah et al. (2021) investigated the ISA level of digital wallet users, citing the variety and prevalence of digital wallet fraud. A questionnaire consisting of 51 Likert-scale questions on seven HAIS-Q focus areas across all three KAB dimensions was administered to a sample of 156 Indonesian digital wallet users. Using the dimensional weight distribution and ISA level criteria used by Kruger and Kearney (2006), the total score for the behavior dimension was 78.44%, an average score. Participants had a good ISA score in the knowledge and attitude dimensions. Fadhilah et al. (2021) recommended monitoring and potential improvement for remediating dimension scores in the average range.

While various studies have estimated the SeBI of employees as part of organizational ISA measurement or gauging ISA program effectiveness, none have attempted to measure ISA and SeBI across security-sensitive industries. The education, finance, government, information technology, legal, medicine, military, and Policing sectors are consistently cited as targets of malicious activities in yearly industry cybersecurity reports. Furthermore, there is a knowledge gap on the effects of hearing difficulties on the security behavior intentions of employees. Individuals with hearing difficulties have specific learning needs, but appropriate teaching media is rarely provided, making it difficult to effectively assimilate new knowledge (Luangrungruang & Kokaew, 2022). However, employees with hearing difficulties work in the employment sectors

mentioned above and constitute potential human security vulnerabilities when they lack adequate ISA awareness and engage in risky security behaviors. Therefore, the effect of hearing impairment on employees' SeBI must be investigated.

3. SECURITY BEHAVIOR MEASUREMENT AND QUESTIONNAIRE DEVELOPMENT

Employees' information security behavior is usually included in ISA measurements. ISA is focused on enhancing employee knowledge of unsafe security practices and improving employee commitment to behave according to security best practices outlined in the organization's information security policies (Parsons et al., 2017). There are existing proposed scales for measuring the security behavior intention of employees. Šolić et al. (2013) proposed a model for assessing users' security behavior when using e-mail services, developing a questionnaire derived from mapping an ontologically-defined knowledge domain of users' risky security behavior. Galba et al. (2015) used the questionnaire developed by Šolić et al. (2013) to develop the Users' Information Security Awareness Questionnaire (UISAQ) for measuring Internet users' awareness, knowledge, and behavior. UISAQ consisted of 33 questions divided into two subscales, one for risky security behavior and the other for users' security knowledge and awareness. Parsons et al. (2014) developed the Human Aspects of Information Security Questionnaire (HAIS-Q), a holistic information security awareness measurement instrument based on the knowledge-attitude-behavior model (KAB). HAIS-Q consists of 63 items assessing seven focus areas: password management, email use, internet use, social media use, mobile devices, information handling, and Incident reporting. Each focus area has its own knowledge, attitude, and behavior dimension. Several studies have used HAIS-Q to measure user ISA in organizations (Cindana & Ruldeviyani, 2018; Papp & Lovaas, 2021; Pattinson et al., 2016; Zulfia et al., 2019). Egelman and Peer (2015) developed the Security Behavior Intentions Scale (SeBIS) as a standard measurement tool for end-user security behaviors. SeBIS measures users' adherence to safe computer security practices using four dimensions: device securement, password generation, proactive awareness, and updating (Egelman & Peer, 2015). Hadlington (2017) developed the Risky Cyber security behaviors scale (RScB) based on SeBIS, which included common risky cybersecurity behaviors that lead to breaches. RScB consisted of 20 survey items with a score of 0-50. Higher RScB scores indicate more risky cybersecurity behavior.

SeBIS, developed by Egelman and Peer (2015), was used in this study to measure employee security behavior intention because it captures employees' self-reported and actual security behaviors. SeBIS subscale scores have also been proven to predict specific security behaviors. Egelman et al. (2016) found that high SeBIS scores on proactive awareness positively correlated with greater phishing website identification, higher SeBIS password selection scores positively correlated with creating stronger passwords, and higher SeBIS device securement subscale scores positively correlated with securely locking devices. SeBIS has been used to measure SeBI in some existing studies. Gratian et al. (2018) correlated human characteristics of risk-taking preferences, decision-making styles, demographics, and personality traits with cybersecurity behavior intention using a refined version of SeBIS that had all reverse-scored items reversed. Sawaya et al. (2017) performed a cross-cultural measurement of users' security behavior using SeBIS and correlated the scores with Gender, Income level, Area, Culture, and Knowledge. SeBIS consists of 16 questions, some of which are reverse-scored, measured with Likert-scale measures Never (1), Rarely (2), Sometimes (3), Often (4), and Always (5). SeBIS was used unrefined in this study.

4. RESEARCH QUESTIONS

This study aimed to answer four research questions:

Research Question One: What are the estimated security behavior intention scores for employees working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM sectors?

Research Question Two: What are the employment sectors' estimated security behavior intention scores?

Research Question Three: What are the estimated security behavior intention scores of employees with and without hearing difficulties working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors?

Research Question Four: Is there a significant difference between the estimated security behavior intention scores of people with and without hearing difficulties working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors?

5. RESEARCH METHOD

The study used a descriptive quantitative research design approach to measure the SeBIS of employees in the employment sectors of interest using a closed-ended online questionnaire as the research instrument. The data were analyzed using descriptive statistics to calculate SeBIS scores. ANOVA statistical analysis was used to determine if differences between groups of employees with and without hearing difficulties were significant.

The study administered an online survey to a random sample of Prolific audience aged eighteen years or more who work full-time in an organization in the United States categorized in the education, finance, government, information technology, legal, medicine, military, policing, and STEM sectors. A minimum sample size of 210 was calculated by power analysis using G*Power ANOVA fixed effects, omnibus, one-way test at 0.25 effect size, 0.05 error probability, 0.95 power, and two groups. The SeBIS questionnaire was used in the survey. The survey was closed-ended with 16 SeBIS five-point Likert scale variable measurement questions. The Likert scale measurement used was Never (1), Rarely (2), Sometimes (3), Often (4), and Always (5). Two attention check questions were included in the survey to detect poor responses. To reduce social desirability bias, participants were informed of the anonymous nature of the survey and asked to answer truthfully. A total of 410 people participated in the survey, of which 386 valid responses were accepted after removing incompletes, speeders, and failed attention check responses. The data and respondent demographics provided separately by Prolific were downloaded and joined. The resulting data was imported into Jamovi for statistical analysis. SeBI scores were calculated and expressed as a percentage of the maximum possible score. No weights were assigned to the subscales. The SeBI interpretation scale by Arisyaet al. (2020) was used where a score of 80%-100% was considered good, 60%-79% average, and 59% or less interpreted as poor awareness. The high score requirement for a good awareness level reflects the high-security requirements of the surveyed sectors.ANOVA test was performed to determine the significance of the SeBIS score difference between groups of employees with and without hearing difficulties.

6. RESULTS

A total of 386 valid responses were accepted. Two hundred fifty-four males and 132 females participated in the study. Most of the participants were aged between 25 and 44 years old. About 48% (*n* = 187) of the participants had an undergraduate degree as their highest educational qualification. A Graduate degree (*n*=96) was the second highest education qualification held by 25% of participants. Information technology (*n*=82), education & training (*n*=74), and medicine (*n*=72) were the majority of the sectors the participants were employed in, accounting for 21%,19%, and 19% of participants' employment sectors, respectively. Of the 386 participants, 147, or 38.1%, had hearing difficulties. Table 1 shows the participant demographics.

Demographic	Category	Frequency (n)	Percent (%)
Sex	Female	132	34.2 %

	Male	254	65.8 %
Age	18-24	24	6.2 %
	25-34	148	38.3 %
	34-44	105	27.2 %
	44-54	72	18.7 %
	54+	37	9.6 %
Education	Doctorate degree (Ph.D./other)	30	7.8 %
	Graduate degree (MA/MSc/MPhil/other)	96	24.9 %
	High school diploma/A-levels	29	7.5 %
	Secondary education (e.g., GED/GCSE)	1	0.3 %
	Technical/community college	43	11.1 %
	Undergraduate degree (BA/BSc/other)	187	48.4 %
Employment sector	Education & Training	74	19.2 %
	Finance	49	12.7 %
	Government & Public Administration	39	10.1 %
	Information Technology	82	21.2 %
	Legal	10	2.6 %
	Medicine	72	18.7 %
	Military	3	0.8 %
	Policing	2	0.5 %
	Science, Technology, Engineering & Mathematics	55	14.2 %
Hearing difficulties	No	239	61.9 %
	Yes	147	38.1 %

TABLE 1: Sample Demographics.

The questionnaire reliability was assessed using Cronbach alpha. The questionnaire showed adequate reliability, with scores greater than 0.6 for the subscales or dimensions. The full SeBI scale had a reliability score of 0.8. The reliability results of Cronbach alpha testing are shown in Table 2.

Variable	Cronbach α
Device Securement	0.623
Password Generation	0.716
Proactive Awareness	0.666
Updating	0.691
Security Behavior Intention	0.799

TABLE 2: Reliability Test Results.

5.1 Research Question One

Research question one asked, “What are the estimated security behavior intention scores for employees working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM sectors?” Table 3 shows all participants' dimension scores and overall security behavior scores. The scores are expressed as a percentage of the maximum attainable sum of the score. Participants scored highest on the Device securements scale with an overall score of 81.83% which showed that participants had good device securement security behavior. Participants had average scores ranging between 69% and 79.5% for the other three security behavior dimensions. Participants scored lowest in the Updating security behavior subscale with a score of 69.2%. All participants' overall SeBI scale score was 75.83%, an average score.

Variable	N	Mean	Sum of scores	Maximum attainable sum of scores	Overall Score (%)
Device Securement	386	16.4	6317	7720	81.83
Password Generation	386	14	5421	7720	70.22

Proactive Awareness	386	19.9	7668	9650	79.46
Updating	386	10.4	4009	5790	69.24
Security Behavior Intention	386	60.7	23415	30880	75.83

TABLE 3: Security Behavior Scores.

5.2 Research Question Two

Research question two asked, “What are the employment sector's estimated security behavior intention scores?” Table. 4 shows the group descriptives and scores by employment sector for all security behavior dimensions and the SeBI score. All sectors had good device securement scores except Education & Training (77.91%) and Legal (76%) which had average scores. Password generation behavior scores were average in all the sectors, with the legal sector scoring the lowest (62.5%). Only the Military (93.33%), policing (90%), information technology (85.07), and government & public administration (81.64%) sectors had good proactive awareness behavior, while the other sectors had average proactive awareness behavior. All sectors had average scores for updating behavior, with policing scoring the highest (76.67) and Legal scoring the lowest (63.33). In overall SeBI scale scores, participants in the policing (86.25%), military (82.50%), and information technology (80.06%) sectors had good scores. Other sectors had average scores, with Legal sector participants scoring the lowest (69.75%).

Variable	Employment sector	N	Mean	Score (%)
Device Securement	Education & Training	74	15.58	77.91
	Finance	49	16.49	82.45
	Government & Public Administration	39	16.85	84.23
	Information Technology	82	16.72	83.60
	Legal	10	15.2	76
	Medicine	72	16.29	81.46
	Military	3	18.33	91.67
	Policing	2	20	100
	Science, Technology, Engineering & Mathematics	55	16.51	82.55
Password Generation	Education & Training	74	13.5	67.50
	Finance	49	13.55	67.76
	Government & Public Administration	39	14.59	72.95
	Information Technology	82	15.26	76.28
	Legal	10	12.5	62.50
	Medicine	72	13.6	67.99
	Military	3	13.33	66.67
	Policing	2	15	75.00
	Science, Technology, Engineering & Mathematics	55	13.89	69.45
Proactive Awareness	Education & Training	74	19.72	78.86
	Finance	49	19.47	77.88
	Government & Public Administration	39	20.41	81.64
	Information Technology	82	21.27	85.07
	Legal	10	18.6	74.4
	Medicine	72	18.76	75.06
	Military	3	23.33	93.33
	Policing	2	22.5	90.00
	Science, Technology, Engineering & Mathematics	55	19.33	77.31
Updating	Education & Training	74	10.62	70.81
	Finance	49	9.94	66.26
	Government & Public Administration	39	11.08	73.85
	Information Technology	82	10.8	72.03
	Legal	10	9.5	63.33
	Medicine	72	9.78	65.19
	Military	3	11	73.33
	Policing	2	11.5	76.67
	Science, Technology, Engineering & Mathematics	55	10.24	68.24

Security Behavior Intention	Education & Training	74	59.42	74.27
	Finance	49	59.45	74.31
	Government & Public Administration	39	62.92	78.65
	Information Technology	82	64.05	80.06
	Legal	10	55.8	69.75
	Medicine	72	58.43	73.04
	Military	3	66	82.50
	Policing	2	69	86.25
	Science, Technology, Engineering & Mathematics	55	59.96	74.95

TABLE 4: Employment Sector Group Scores.

5.3 Research Question Three

Research question three asked, "What are the estimated security behavior intention scores of employees with and without hearing difficulties working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors?" Table 5 shows the group scores by hearing difficulty for all security behavior dimensions and overall SeBI. The SeBI score for the group with hearing difficulties was 75.26%, and 76.18% for those without hearing difficulties. Not much difference was observed between the scores for either group for all the security behavior dimensions. The difference in scores between the groups in all security behavior dimensions did not exceed 3%, and the largest difference was in updating behavior. However, the scores of participants with hearing disabilities were less in all behavior dimensions except device securement and SeBI.

Variable	Hearing difficulties	N	Mean	Sum	Score (%)
Device Securement	No	239	16.3	3892	81.42
	Yes	147	16.5	2425	82.48
Password Generation	No	239	14.2	3393	70.98
	Yes	147	13.8	2028	68.98
Proactive Awareness	No	239	19.9	4761	79.68
	Yes	147	19.8	2907	79.10
Updating	No	239	10.5	2519	70.26
	Yes	147	10.1	1490	67.57
Security Behavior Intention	No	239	60.9	14565	76.18
	Yes	147	60.2	8850	75.26

TABLE 5: Hearing Difficulty Group Scores.

5.4 Research Question Four

Research question four asked, "Is there a significant difference between the estimated security behavior intention scores of employees with and without hearing difficulties working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors?" To answer research question four, an ANOVA analysis was performed. The data were tested for ANOVA assumptions of linearity and homogeneity of variance. The data failed the linearity test because all dependent variables had statistically significant Shapiro-wilk test results, as shown in Table 6. However, all dependent variables passed Levene's test for homogeneity of variance with statistically insignificant p-values, as shown in Table 7.

Variable	Shapiro-Wilk W	Shapiro-Wilk p
Device Securement	0.893	< .001
Password Generation	0.976	< .001

Proactive Awareness	0.956	< .001
Updating	0.971	< .001
Security Behavior Intention	0.989	0.006

TABLE 6: Shapiro-Wilk Test Results.

Variable	Statistic	df	df2	p
Device Securement	0.0379	1	384	0.846
Password Generation	0.2740	1	384	0.601
Proactive Awareness	2.8992	1	384	0.089
Updating	1.1896	1	384	0.276
Security Behavior Intention	0.4235	1	384	0.516

TABLE 7: Levene's Test Result.

The non-parametric equivalent of ANOVA, the Kruskal-Wallis test, was conducted because the data failed the ANOVA linearity assumption. Table 8 shows the result of the Kruskal-Wallis test for the difference in mean between the hearing difficulty groups for all the dependent variables. There were no statistically significant differences between groups of hearing difficulty for device securement ($\chi 2$ (1) = 0.649, p =.421), password generation ($\chi 2$ (1)= 0.925, p =.336), Proactive Awareness ($\chi 2$ (1) = .458, p =. 499), Updating ($\chi 2$ (1) = 2.563, p =0.109), and SeBI ($\chi 2$ (1) =0.452, p =.501). Therefore, there is no significant difference between the estimated security behavior intention scores of people with and without hearing difficulties working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors.

Variable	χ^2	df	p
Device Securement	0.649	1	0.421
Password Generation	0.925	1	0.336
Proactive Awareness	0.458	1	0.499
Updating	2.563	1	0.109
Security Behavior Intention	0.452	1	0.501

TABLE 8: Kruskals-Wallis test Result.

7. DISCUSSION

The overall security behavior intention score of employees across all the surveyed employment sectors was 75.83, an average score. Updating and password generation behavior scores were the lowest. Therefore, organizations in security-sensitive sectors should implement password strength, reuse, and expiration policies while increasing awareness of more secure password generation habits. Password creation and change interfaces should also remind employees not to re-use passwords used across external websites. The average score for updating shows that employees cannot be fully trusted to keep their antivirus and other software updated. Organizations can enforce deadlines for manual updating, after which the software is forcefully updated. Network access protection should be used to enforce software updates for Bring-your-own-devices (BYOD) connecting to organizations' networks. More information security awareness training may help improve the security behavior intention of employees.

Out of all the employment sectors, only employees in the information technology, military, and policing sectors had good security behavior intention scores. The sectors such as medicine, finance, education, and government, frequently cited as high-value targets of malicious actors in industry cybersecurity reports, had surprisingly average security behavior intention scores. The medicine and finance sector employees had low scores in password generation, proactive awareness, and updating dimensions. Employees in the government & public administration had average scores for password generation and updating. The legal and education & training sectors had average scores in all security behavior dimensions. The legal sector had the worst scores,

including in device securement. The small sample size of legal sector employees in the study may not have been adequate, but the scores are a cause for concern and should be further investigated. The education sector, being highly targeted, also need to improve the security behavior of its employees in all dimensions.

There was little observable difference in the scores across all dimensions for employees with and without hearing difficulties. This is reflected in the lack of a statistically significant difference reported in the Kruskal-Wallis test. The result implies that the information security awareness training programs have similar effectiveness across both groups. However, the groups with hearing difficulty scores were lower, with device securement and updating dimensions accounting for the most considerable differences. The reasons for the noted differences in the device securement and updating dimensions are unclear and should be investigated. Organizations in the surveyed sectors may need to take action to ensure this gap is closed and that their employees' overall security behavior intention scores are above the average range.

8. LIMITATIONS

Several limitations were observed in the conduct of this study. The sample size does not fully represent the population of employees across the surveyed sectors. A relatively small sample size was obtained from the police, military, and legal sectors. The use of a third-party audience service limited the study's recruitment options. The study relied on participant information given to prolific for participant recruitment. The study did not consider the different hearing difficulty levels in its analysis. The study is also limited to employees in the United States working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors. For this reason, the study's result cannot be generalized beyond the surveyed sectors and outside the United States.

9. IMPLICATIONS

Unlike previous studies that studied security behavior as a factor in theoretical applications to various problems or that estimated security behavior intention of a narrowly focused demographic, this study estimated employees' SEBI broadly across various employment sectors. The sectors studied are security-critical sectors that experience a consistently high rate of malicious attacks. Due to the broad scope of the study and the nature of the employment sectors studied, the study has several practical implications. The study utilized a standard general scale that measures employees' intended and actual security behavior. This permitted uniform comparison of SeBI scores across the surveyed employment sectors. The uniform comparison enables information security administrators and policymakers to identify differences in security behaviors across the employment sectors. The SeBI dimensions also provide more precise insights into which security areas each sector's employees have poor or average security habits for investigation and troubleshooting. For example, the medicine sector had its lowest SeBI score in the updating dimension, which may indicate why ransomware attacks plague the sector. Based on the study's results, information security administrators and policymakers may take appropriate action to remediate employees' average and poor SeBI scores.

The information and opportunity provided by this study to information security administrators and policymakers to identify and remediate poor security behavior of employees offer potential for social change. The study may help reduce the success of malicious attacks. Behavior is generally considered the most critical component of ISA. This is reflected in the higher weight given to the behavior dimension in various KAB-based ISA measurement studies. Therefore, more secure employee behavior will help reduce vulnerabilities. The potential reduction in the attack success rate translates to reduced data breach incidents, losses, and damages to organizations in the surveyed sectors.

The study also provided novel insights into the impact of hearing disabilities on employees' SeBI. The impact of hearing difficulties on information security is rarely studied. This study argued for greater awareness and consideration of hearing difficulties by information security administrators.

Considering hearing difficulties is essential in sectors with many employees with hearing difficulties. The study provided valuable comparison insight into the SeBI scores of employees with and without hearing difficulties. Updating and password generation were the SeBI dimensions employees with hearing difficulties scored the lowest. Security administrators in the surveyed sectors could use this knowledge to improve the security behavior of their employees with hearing disabilities in the two dimensions or assess the effectiveness of ISA training covering the two dimensions for their employees with hearing difficulties.

10. CONCLUSION

Human factors are the weakest links in the security chain. Unsecure employee behavior is a source of security vulnerability. Organizations in security-critical sectors need to measure and monitor employee security behavior intentions continuously. This study measured the security behavior intention of employees based in the united states that work in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors. Employees of all the sectors had a combined SeBi score of 75.83%, an average score. Dimension-wise, employees had a good score in only device securement. The study provided the scores of each studied employment sector. The security behavior intention was average among employees in the education & training, finance, government & public administration, legal, medicine, and STEM sectors. Organizations in the sectors mentioned earlier should improve their employees' security behavior intention because they are vulnerable targets of malicious actors. Employees in the legal sector scored the lowest in all SeBI dimensions, which should be a cause for concern for information security administrators in organizations in the Legal sector. Corrective security behavior awareness training is highly recommended for employees in the Legal sector. Information security administrators and policymakers may find that the results of this study provide insights into the prevailing security behavior of employees in their sector. SeBI is a predictor and precursor of actual security behavior. Therefore, a higher SeBI score is indicative of good security behavior. Information security administrators and policymakers in the studied sector should aim to increase the average SeBI scores of the employees.

The impact of hearing disability on employee SeBI scores was investigated in the study. A comparison was made between scores of employees with and without hearing difficulties across all the studied sectors. There was a slight disparity in the scores between the two hearing difficulties groups. Employees with hearing difficulties scored less in all SeBI dimensions except device securement. However, an investigation of the statistical significance of the observed difference using the Kruskal-Wallis test showed that the difference was not statistically significant. The disparity should be corrected by information security administrators in the surveyed sectors. Information security administrators and policymakers should consider hearing difficulties in their ISA training and measurements. Improving the SeBI scores of all employees to above average should be the primary focus for security administrators.

There are several opportunities for future research. Future studies can perform the study individually for each employment sector to get a deeper insight into the security behavior intention of employees in that sector. This may help shed more light on the security behavior intentions of employees in the legal sector, which were found to be the lowest among all the sectors. The reasons for the noted differences in the device securement and updating dimensions between the hearing difficulty groups should be investigated. Furthermore, the study can be conducted with an expanded hearing difficulties group, including the Deaf, deafened, and hard of hearing. Such a study will provide deeper insight that can help security administrators tailor information security awareness programs to each hearing difficulty group.

11. REFERENCES

Alzamil, Z. A. (2012). Information security awareness at Saudi Arabians' organizations: an information technology employee's perspective. *International Journal of Information Security and Privacy (IJISP)*, *6*(3), 38-55.

Arisya, K. F., Ruldeviyani, Y., Prakoso, R., & Fadhilah, A. L. (2020, November). Measurement of information security awareness level: A case study of mobile banking (m-banking) users. In *2020 Fifth International Conference On Informatics And Computing (Icic)* (pp. 1-5). IEEE.

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. Journal of Basic and Applied Scientific Research, 2(9),9331–9347.

Candiwan, C., Sari, P. K., & Sharif, O. O. (2022). Information Security Awareness Evaluation of Telemedicine Application Users using Human Aspect Information System Questionnaire. *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, 1.

Chao, C.-M. (2019). Factors determining the behavioral intention to use mobile learning: an application and extension of the UTAUT model. *Frontiers in Psychology*, p. *10*, 1652. https://doi.org/10.3389/fpsyg.2019.01652.

Check Point Software. (2022, October 26). *Check Point Research: Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends*. Retrieved January 16, 2023, from https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/.

Cindana, A., & Ruldeviyani, Y. (2018, October). Measuring information security awareness on employee using HAIS-Q: Case study at XYZ firm. In *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 289-294). IEEE.

CloudSek. (2022, December 30). *Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022 - CloudSEK*. CloudSEK - Digital Risk Management Enterprise | Artificial Intelligence Based Cybersecurity. Retrieved January 16, 2023, from https://cloudsek.com/whitepapers_reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022/.

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., ... & Stephenson, R. J. (2019, September). Human risk factors in cybersecurity. In *Proceedings of the 20th annual SIG conference on information technology education* (pp. 87–92).

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 2873-2882).

Egelman, S., Harbach, M., & Peer, E. (2016, May). Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 5257-5261).

Fadhilah, A. L., Ruldeviyani, Y., Prakoso, R., & Arisya, K. F. (2021). Measurement of information security awareness level: A case study of digital wallet users. *IOP Conference Series: Materials Science and Engineering*, *1077*(1), 012003. https://doi.org/10.1088/1757-899X/1077/1/012003.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015, August). Information security awareness in educational institution: An analysis of students' individual factors. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 352-359). IEEE.

Filippidis, A. P., Hilas, C. S., Filippidis, G., & Politis, A. (2018, May). Information security awareness of greek higher education students—preliminary findings. In *2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST)* (pp. 1-4). IEEE.

Galba, T., Solic, K., & Lukic, I. (2015). An information security and privacy self-assessment (ISPSA) tool for internet users. *Acta PolytechnicaHungarica*, *12*(7), 149-162.
Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *computers & security*, *73*, 345-358.

Griffiths, C. (2023, January 6). *The Latest Cyber Crime Statistics (updated January 2023) | AAG IT Support*. AAG IT Services. Retrieved January 16, 2023, from https://aag-it.com/the-latest-cyber-crime-statistics/.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346.

Hong, Y., Xu, M., & Furnell, S. (2023). Situational support and information security behavioural intention: a comparative study using conservation of resources theory. *Behaviour & Information Technology*, pp. 1–17. https://doi.org/10.1080/0144929X.2023.2177825

Jenkins, J., Durcikova, A., University of Oklahoma, USA, Nunamaker, J., & University of Arizona, USA. (2021). Mitigating the Security Intention-Behavior Gap: The Moderating Role of Required Effort on the Intention-Behavior Relationship. *Journal of the Association for Information Systems*, *22*(1), 246–272. https://doi.org/10.17705/1jais.00660.

Kadena, E., & Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security science journal*, *2*(2), 51-64.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085.

Luangrungruang, T., & Kokaew, U. (2022). E-Learning Model to Identify the Learning Styles of Hearing-Impaired Students. *Sustainability*, *14*(20), 13280. https://doi.org/10.3390/su142013280.

Moletsane, T., & Tsibolane, P. (2020). Mobile information security awareness among students in higher education : an exploratory study. *2020 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. https://doi.org/10.1109/ICTAS47918.2020.233978.

Mosleh, M., Pennycook, G., & Rand, D. G. (2020). Self-reported willingness to share political news articles in online surveys correlates with actual sharing on Twitter. *Plos One*, *15*(2), e0228882. https://doi.org/10.1371/journal.pone.0228882.

Murbach, K. (2019). Self-efficacy in information security: a mixed methods study of deaf end-users.

Nastasiu, C. I. (2016). Cyber security strategies in the internet era. *Scientific research and education in the air force-afases*, 619-624.

Ngoqo, B., & Flowerday, S. (2014). Linking student information security awareness and behavioural intent. *HAISA*, p. 162.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.

Papp, G., & Lovaas, P. (2021). Assessing Small Institutions' Cyber Security Awareness Using Human Aspects of Information Security Questionnaire (HAIS-Q). In *Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3* (pp. 933-948). Springer International Publishing.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, pp. *66*, 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, pp. *42*, 165–176.

Pattinson, M. R., Butavicius, M. A., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The Information Security Awareness of Bank Employees. In *HAISA* (pp. 189-198). Pollock, T. (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS).

Prabhu, S., & Thompson, N. (2022). A primer on insider threats in cybersecurity. *Information Security Journal: A Global Perspective*, *31*(5), 602–611.

PurpleSec. (2022, October 17). *2022 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends*. https://purplesec.us/resources/cyber-security-statistics/.

Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., Hidayanto, A. N., Solikin, & Hapsari, I. C. (2018). Measurement of employee information security awareness: case study at A government institution. 2018 Third International Conference on Informatics and Computing (ICIC), 1–6. https://doi.org/10.1109/IAC.2018.8780571.

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June). Human factors in cybersecurity: a scoping review. In *The 12th International Conference on Advances in Information Technology* (pp. 1-11).

Salem, Y., Moreb, M., & Rabayah, K. S. (2021). Evaluation of Information Security Awareness among Palestinian Learners. *2021 International Conference on Information Technology (ICIT)*, 21–26. https://doi.org/10.1109/ICIT52682.2021.9491639.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, pp. *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Šolić, K., Jović, F., & Blažević, D. (2013). An approach to the assessment of potentially risky behavior of ICT systems' users. *Technical Gazette*, *20*(2), 335-342.

U.S. Government Accountability Office. (2020, December 15). *Cybersecurity: An overview of cyber challenges facing the nation, and actions needed to address them*. U.S. GAO. Retrieved January 16, 2023, from https://www.gao.gov/cybersecurity.

Zulfia, A., Adawiyah, R., Hidayanto, A. N., & Budi, N. F. A. (2019, April). Measurement of employee information security awareness using the human aspects of information security questionnaire (HAIS-Q): Case study at PT. PQS. In *2019 5th International Conference on Computing Engineering and Design (ICCED)* (pp. 1-5). IEEE.