Health Informatics Journal

Regular Article

Health Informatics Journal
2020, Vol. 26(1) 461–473

DOI: 10.1177/1460458219832048
journals.sagepub.com/home/jhi
SAGE

Information security climate and the assessment of information security risk among healthcare employees

Stacey R Kessler
Montclair State University, USA

Shani Pindek
University of Haifa, Israel

Gary Kleinman
Montclair State University, USA

Stephanie A Andel and Paul E Spector
University of South Florida, USA

Abstract

Since 2009, over 176 million patients in the United States have been adversely impacted by data breaches affecting Health Insurance Portability and Accountability Act–covered institutions. While the popular press often attributes data breaches to external hackers, most breaches are the result of employee carelessness and/or failure to comply with information security policies and procedures. To change employee behavior, we borrow from the organizational climate literature and introduce the Information Security Climate Index, developed and validated using two pilot samples. In this study, four categories of healthcare professionals (certified nursing assistants, dentists, pharmacists, and physician assistants) were surveyed. Likert-type items were used to assess the Information Security Climate Index, information security motivation, and information security behaviors. Study results indicated that the Information Security Climate Index was related to better employee information security motivation and information security behaviors. In addition, there were observed differences between occupational groups with pharmacists reporting a more favorable climate and behaviors than physician assistants.

Corresponding author:
Stacey R Kessler, Department of Management, Montclair State University, 1 Normal Ave., BSN 456, Montclair, NJ 07043, USA.
Email: stacey.kessler@gmail.com

Keywords
cybersecurity, information security, electronic health records, information protection, organizational climate

Introduction

Despite both legislation and sophisticated technology designed to safeguard patients' electronic health records, data breaches have been on the rise[1–4] with over 2100 reported data breaches affecting Health Insurance Portability and Accountability Act (HIPAA)-covered US healthcare providers since 2009. These breaches exposed the data of over 176 million patients, with the pace of breaches ramping up in recent years. Importantly, this figure represents a significant underestimate of data breaches and of the number of patients impacted as US federal reporting guidelines only apply to data breaches affecting over 500 patients. Moreover, a recent study by the Ponemon Institute[5] indicated that the majority of breaches reported affected *under* 500 patients.[6,7] In addition, the costs associated with rectifying the effects of data breaches are substantial, as each breach is estimated to cost over US$2.2 million with total costs to the US healthcare industry of US$6.2 billion annually.[5] While the media and popular press often attribute data breaches to external "hackers," research indicates that approximately 70 percent of data breaches are either directly or indirectly the result of employee carelessness and/or failure to comply with existing information security (IS) regulations, policies, and procedures.[8] In a survey of software development personnel, 69 percent believed that the lack of the appropriate culture, attitude, and mind-set accounted for numerous data security–related issues.[9] Indeed, healthcare industry experts seem to concur with this assessment and have even argued that data security practices are far below that of other industries.[10] Specifically, in a recent *JAMA* editorial, Dr David Blumenthal highlighted the vulnerability of patients' health information and argued that preventing data breaches involves fundamentally changing behavior within the field—both that of the healthcare providers and of healthcare institutions.[10,11]

Based on this research and answering a recent call[12] for research on information security within healthcare, we directly target employees' attitudes and behavior surrounding IS, by taking an organizational climate approach, a concept which is distinct from but often used interchangeably with organizational culture. Organizational climate, "the shared perceptions of and the meaning attached to the policies, practices, and procedures employees experience and the behaviors they observe getting rewarded and that are supported and expected,"[13] approaches have been used successfully to change employees' domain-specific attitudes and behaviors. Examples include but are not limited to ethics climate,[14] safety climate,[15] diversity climate,[16] and service climate.[17] Common across these areas is that while relevant rules, policies, procedures, and training often existed, they were not sufficient to change corresponding behavior. Therefore, organizational climate approaches were employed to highlight social aspects of the work environment, making certain characteristics more salient to employees, thus cueing a change toward desired behaviors.[18] The goal of this study, therefore, is to provide healthcare researchers and practitioners with a validated, parsimonious tool to assess the climate surrounding IS throughout their organizations. As such, it would provide practitioners with information regarding where IS interventions should be targeted.

A contextual approach: organizational culture/climate

There has been a growing body of research that focuses on the use of environmental cues to encourage employee compliance with existing IS policies and procedures.[19–30] Most research in the area takes an organizational culture approach over that of organizational climate (exceptions[25,26]). Although similar, these two constructs differ along several key points.

First, since organizational culture has both sociological and anthropological roots, it is understood at a deeper, almost unconscious level.[31] As such, it is most often studied qualitatively, allowing researchers a more in-depth examination of these embedded processes.[13,31] Indeed, most efforts to study organizational culture quantitatively have been unsuccessful in the organizational studies literature.[32] These difficulties extend to the IS literature where in order to measure key components of Schein's[33] model, one instrument[27] consisted of 85 items assessed across seven dimensions. This makes for a lengthy organizational survey, especially when trying to assess additional variables. These challenges in quantifying organizational culture are consistent with Schein's[33] explanation that

> culture is best revealed through interaction … [and that] this process of deciphering [culture] cannot be standardized because organizations differ greatly in what they allow the outsider to see. Instead you have to think like the anthropologist, lean heavily on observation, and then follow up with various kinds of inquiry.

Second, values, a key component of Schein's[33] model, can be difficult to change and tend to be distal predictors of workplace behavior.[33–35] Given that the central focus of the organizational culture approach is to fundamentally change employees' values, this method might not be as effective as an organizational climate approach, which focuses directly on changing employees' behavior.

A third inherent component of the organizational culture approach, and by extension, existing scales, is the focus on the role of top management[20,24] with an underlying assumption that if top management values IS, these values will trickle-down throughout the organization. While top management's commitment to the domain-specific goal is important, organizational climate research suggests that the direct supervisor has more of an impact on employee behavior than does the top leadership.[36,37] This is because while top management might set policies and procedures for the entire organization, the implementation of these policies and procedures occurs at lower levels of the organization, often in the form of supervisor discretion in the support of daily practices and enforcement of policies and procedures. It is then this implementation that drives employees' climate perceptions and subsequent behaviors.[36]

Finally, inherent to the organizational climate approach is its focus on a specific domain and operationalization in relation to a competing priority.[36] Often employees disregard existing policies and procedures surrounding the domain-specific area because these policies and procedures conflict with a competing priority. For example, Zohar and Luria[38] consider safety in regard to expediency. In a strong safety climate, the focus is on ensuring that employees behave safely and comply with safety policies and procedures, even when doing so compromises expediency, and ultimately, productivity. Therefore, an organizational climate approach is applicable to IS since researchers[20,39] suggest that employees compromise IS to be more productive. Within a healthcare setting, the competing priority is more serious given that in addition to productivity, healthcare providers must also balance patient safety/care with patient confidentiality.

This study

For many of these reasons, organizational culture approaches in the IS literature have taken more of an in-depth case study of a single organization's approach to IS. However, an organizational climate approach is quantitative with the goal of improving organizational effectiveness in a specific area.[31] Organizational climate researchers[15,16] have had much success in developing parsimonious and well-validated measures of domain-specific organizational climate scales. These scales focus on contextual aspects of the environment with the goal of changing domain-specific employee

behavior.[31] These approaches have been quite successful, particularly in the safety domain, as both primary[40] and meta-analytic research[41–44] have linked safety climate to an increase in employees' safety-related behaviors, ultimately reducing accidents. While safety regulations already existed, the organizational climate was often the mechanism used to secure employee compliance with these regulations. Given the success of organizational climate approaches in the workplace safety domain and following the call of researchers[45,46] to treat IS like workplace safety, we apply the approach to IS. To do this, we build on validated and well-known safety climate measures to develop the Information Security Climate Index (ISCI).

We define IS climate as a multidimensional construct consisting of the shared perceptions of the IS policies and their manifestations in the organization. These can be categorized into the following: what is practiced in the organization, the observed importance placed on IS in the organization, and the laxness surrounding IS activities. That is, organizations with strong IS climates have clear rules and procedures for employees' handling of confidential data. Moreover, importance is placed on keeping data secure, even if it means employees taking extra time to do so. This is manifested in management's, particularly the direct supervisor's, encouragement of the secure handling of confidential data and the correction of instances where employees treat data in an insecure fashion. We propose that the ISCI will be related to employees' IS motivation and behaviors and empirically test this proposition. This prediction is grounded in the safety climate literature where research[41–44] has linked safety climate to employees' motivation to engage in safety-related behaviors and engage in actual behaviors such as safety compliance and safety participation.

Methods

Sample

Participants were recruited through email addresses contained in a public database available on the Florida Department of Business and Professional Regulation website. We chose four of the larger healthcare occupations to represent a wide range of activities and settings. These included certified nursing assistants (CNA's), dentists, pharmacists, and physician assistants (PA's). Given inaccuracies of the database including retirements and incorrect data listed for individuals, it was not possible to calculate the number of eligible participants who received invitations to participate.

Survey instrument

Likert-type scale surveys were used to assess each variable. The ISCI was used to assess IS climate. The ISCI was developed using two previous pilot studies, which are detailed in Supplemental Appendix 1. The scale contains 9 items along three subscales. These resulting items were based on a series of factor analyses designed to reduce the initial item pool to a reasonable number of items. After examining the resulting items, we subsequently named the three subscales: practices (i.e. behaviors and discussions that are actively initiated by the supervisor in the interest of promoting IS), importance (i.e. the importance placed on the protection of confidential data), and laxness (i.e. the prioritization of other activities, particularly work activities, over IS). The laxness subscale was reverse coded so that higher scores on all subscales indicated a stronger IS climate. Items were assessed along a 5-point Likert-type scale with 1 indicating "strongly disagree" and 5 indicating "strongly agree."

To assess IS-related motivation and behavior, we adapted three commonly used safety indicators[47] to the IS domain (see Supplemental Appendix 2). These include one indicator of motivation and two indicators of behavior (i.e. compliance and participation). Consistent with the definition

of safety motivation, IS motivation refers to the extent to which employees believe that IS is worthwhile or of value. Along these lines, IS compliance refers to the degree to which employees abide by core rules that concern the protection and usage of private data. Finally, IS participation refers to extra role behaviors in which employees go above and beyond simple rule application or compliance and engage in behaviors that promote the safe handling of data throughout the workgroup and organization. Each scale contained three items assessed along a 5-point scale with 1 indicating "strongly disagree" and 5 indicating "strongly agree." Higher scores indicated a higher level of motivation, compliance, or participation.

Given that these three measures were general in nature, we designed a checklist of specific high-risk IS behaviors (also referred to as high-risk security behavior checklist) to cross-validate with a behavior-specific scale. The checklist contained seven items focusing on the frequency in which the healthcare professional engaged in behaviors that could expose confidential patient data here. These items aligned with some of the frequently cited employee behaviors that led to the exposure of patients' data in reported US healthcare data breaches.[5] All items were assessed along a 4-point scale with 1 indicating "none" and 4 indicating "three times or more" (with the exception of the first two items where 4 indicated "five or more times"). Examples include "How many times in the past year have you taken a laptop or other device home that had sensitive information?" and "How many times in the past year have you left a computer unlocked with patient data showing?" To obtain a score, we took an average of each participant's responses across all seven items. Higher scores indicate higher risk security behaviors. Original items are depicted in Supplemental Appendix 3.

Analyses

Demographic statistics were calculated using SPSS version 24. As a first step, we provide demographic information such as gender, age, race/ethnicity, highest level of education, and work setting for the total sample as well as for each of the four occupational groups.

We then conducted a factor analysis on the ISCI. Factor analyses are used to group like scale items together. Researchers typically use two types of factor analyses: exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). An EFA is used when researchers are unsure of the number of predetermined factors. This helps researchers to set the number of factors and determine which items load onto each factor through an inspection of item loadings. As can be seen in Supplemental Appendix 1, a series of EFAs were conducted early in the scale development process (Supplemental Appendix 1, pilot study 1). Once a preliminary factor structure is set using the EFA, a CFA is used to "confirm" or test these results (as was done in pilot study 2 reported in Supplemental Appendix 1). In this study, using the Mplus 7.1 program,[48] we use a CFA to confirm the ISCI's factor structure obtained from the prior two studies.

In the third step of our analyses, we used SPSS version 24 to calculate the mean, standard deviation, potential range, and observed range for each study variable. We also calculated Pearson product-moment correlation coefficients between all study variables and use the correlations between the ISCI and the motivation/behavior variables to demonstrate the utility of implementing an IS climate. As part of this analysis, we also explore the relationships between the ISCI, motivation, behavior variables, and demographic variables (i.e. age, sex, and education). Finally, in order to detect whether there were differences among occupational groups on the ISCI, motivation, compliance, participation, and high-risk security behavior checklist, we conducted a one-way multivariate analysis of variance (ANOVAs) using SPSS version 24. A MANOVA is used to detect differences among factors (i.e. the four occupational groups) on multiple variables, in this case, the ISCI and the motivation/behavioral variables under investigation. A MANOVA is preferable over a series of

univariate analyses of variance (ANOVAs) equations because it helps to reduce Type I error rates, takes into account relationships among dependent variables, and provides an overall index of significance. If the MANOVA is significant, it is then appropriate to examine the one-way ANOVA results for each variable. If the one-way ANOVA results are significant, post hoc tests are used to pinpoint the mean differences.

Results

Demographics

A total of 261 employees across the four occupational groups responded to the survey, with usable data received from 252 employees (male = 91, female = 136, with the remaining 25 individuals declining to provide that information). The mean age was 46.57 (SD = 13.45) and the sample was mostly white (67.5%). Participants worked in a variety of medical settings including hospitals, physicians' offices, rehabilitation centers, and nursing homes. On a whole, the sample was well educated with 34.9 percent reporting their highest degree earned was at the doctoral level and 26.9 percent reporting their highest degree earned was at the master's level. Table 1 contains a breakdown of demographics of each of these groups.

ISCI CFA

A second-order CFA was conducted using Mplus 7.1.[48] Each scale item was loaded onto the proposed scale factor. Then, each of the three first-order factors was loaded onto a second-order latent factor, representing overall IS climate. Based on recommendations in Gefen et al.,[49] results indicated adequate fit for the proposed factor structure ($\chi^2_{(32)} = 109.356$, $p = 0.000$, root mean square error approximation (RMSEA) = 0.099; comparative fit index (CFI) = 0.934; Tucker–Lewis index (TLI) = 0.907). Although the RMSEA was above the generally accepted 0.08 cutoff, both CFI and TLI were above 0.90. However, one item on the practices scale had a low factor loading (0.436). Upon inspection ("Issues related to the protection of private data are discussed in my workplace"), we chose to delete this item because it was not supervisor initiated as were the remainder of subscale items. We reran the CFA with the 9-item scale version and this yielded slightly better fit ($\chi^2_{(36)} = 1139.115$, $p = 0.000$, RMSEA = 0.095; CFI = 0.951; TLI = 0.927). As a point of comparison, results of a CFA with all items loading onto a single factor indicated poor fit ($\chi^2_{(35)} = 547.558$, $p = 0.000$, RMSEA = 0.243; CFI = 0.562; TLI = 0.437). Moreover, the fit for the second-order CFA was significantly better than the fit for this comparison CFA ($\Delta\chi^2_{(1)} = 591.557$, $p < 0.01$). Therefore, based on recommendations[49] and results of the single factor CFA, the second-order CFA was retained. Supplemental Appendix 4 contains these nine items along with the three subscales which constitute the final scale.

Linking the ISCI to employee motivation and behavior

The full correlation matrix is available in Table 2. Cronbach's alphas were above the 0.70 threshold[50] with the exception of the high-risk security behavior checklist variable. This scale was designed as a formative and not a reflective scale, rendering Cronbach's alpha, and other internal consistency metrics, an inappropriate measure of reliability.[51] This practice is not uncommon in the behavioral sciences and can be seen with a number of scales.[51] Overall, correlations among study variables indicate significant relationships between the ISCI and outcome variables of IS motivation and IS behavior. Correlations between sub-factors of the ISCI and the motivation as well as

Table 1. Sample demographics.

	Total sample	CNA's	Dentists	Pharmacists	PA's
Total sample	252	43	49	89	71
Male, % (n)	36.1 (91)	4.7 (2)	46.9 (23)	51.7 (46)	28.2 (20)
Mean age, years (SD)	46.57 (13.45)	45.46 (13.43)	49.52 (14.10)	47.73 (13.64)	43.63 (12.38)
Race/ethnicity, % (n)					
Asian	3.6 (9)	0 (0)	2.0 (1)	4.5 (4)	5.6 (4)
Black	8.3 (21)	18.6 (8)	2.0 (1)	10.1 (9)	4.2 (3)
Hispanic	9.1 (23)	14.0 (6)	14.3 (7)	4.5 (4)	8.5 (6)
White	67.5 (170)	58.1 (25)	77.6 (38)	65.2 (58)	69.0 (49)
Other	3.2 (8)	2.3 (1)	0 (0)	6.7 (6)	1.4 (1)
Declined to respond	8.3 (21)	7.0 (3)	4.1 (2)	9.0 (8)	11.3 (8)
Level of education, % (n)					
MD/PhD	35.3 (89)	0 (0)	93.9 (46)	43.8 (39)	5.6 (4)
Master's degree	26.6 (67)	4.7 (2)	0 (0)	14.6 (13)	73.2 (52)
Bachelor's degree	16.7 (42)	16.3 (7)	0 (0)	31.5 (28)	9.9 (7)
Some college	11.5 (29)	62.8 (27)	0 (0)	0 (0)	1.4 (1)
High school degree	1.6 (4)	9.3 (4)	0 (0)	0 (0)	0 (0)
Declined to respond	8.3 (21)	7.0 (3)	6.1 (3)	10.1 (9)	9.9 (7)
Work setting, % (n)					
Hospital	29.4 (74)	23.3 (10)	10.2 (5)	38.2 (34)	35.2 (25)
Physician's office	24.6 (62)	4.7 (2)	65.3 (32)	2.2 (2)	36.6 (26)
Rehabilitation center	1.6 (4)	9.3 (4)	0 (0)	0 (0)	0 (0)
Nursing home/long-term care facility	5.2 (13)	25.6 (11)	0 (0)	2.2 (2)	0 (0)
Retail/pharmacy chain	11.1 (28)	0 (0)	0 (0)	31.5 (28)	0 (0)
Urgent care/walk-in clinic	3.2 (8)	0 (0)	4.1 (2)	0 (0)	8.5 (6)
Hospice	1.6 (4)	9.3 (4)	0 (0)	0 (0)	0 (0)
Private home	2.0 (5)	9.3 (4)	0 (0)	0 (0)	1.4 (1)
Education	2.4 (6)	2.3 (1)	2.0 (1)	1.1 (1)	4.2 (3)
Mail order/call center	1.6 (4)	0 (0)	0 (0)	4.5 (4)	0 (0)
Other	9.1 (23)	7.0 (3)	14.3 (7)	11.2 (10)	4.2 (3)
Declined to respond	8.3 (21)	9.3 (4)	4.1 (2)	9.0 (8)	9.9 (7)

CNA's: certified nursing assistants; PA's: physician assistants.

three behavior variables were significant and in the expected directions (r's ranged between 0.25 and 0.47, p's < 0.01). In addition, correlations between the overall ISCI and motivation ($r = 0.50$, $p < 0.01$), compliance ($r = 0.57$, $p < 0.01$), participation ($r = 0.57$, $p < 0.01$), and high-risk security behavior checklist ($r = -0.46$, $p < 0.01$) were significant and in the expected directions. Results also suggest that older employees were significantly more likely to engage in IS participation and significantly less likely to engage in high-risk security behaviors. In addition, females reported a significantly poorer IS climate than males but also reported engaging in significantly more IS participation behaviors and significantly fewer high-risk security behaviors.

Differences among occupational groups

Results of the one-way MANOVA indicated support for a multivariate main effect for occupational groups (Wilks' $\lambda = 0.841$, $F(15, 643.612) = 2.770$, $p < 0.001$, partial eta squared $= 0.057$). The

Table 2. Study correlations.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Organizational climate											
(1) Practices											
(2) Importance	0.40**										
(3) Laxness (R)	0.28**	0.34**									
(4) Total	0.81**	0.73**	0.67**								
Motivation and behavior											
(5) Motivation	0.27**	0.52**	0.38**	0.50**							
(6) Compliance	0.39**	0.44**	0.46**	0.57**	0.73**						
(7) Participation	0.47**	0.39**	0.37**	0.57**	0.53**	0.72**					
(8) HRSB	−0.37**	−0.25**	−0.39**	−0.46**	−0.34**	−0.49**	−0.44**				
Demographics											
(9) Age	0.13	−0.04	0.01	0.07	0.00	0.12	0.22**	−0.18**			
(10) Sex	−0.19**	−0.17*	−0.08	−0.20**	−0.10	−0.09	−0.09	0.13*	−0.27**		
(11) Education	0.00	−0.16*	−0.12	−0.11	−0.05	0.01	−0.02	−0.07	0.10	0.27**	
Descriptive statistics											
Mean	3.12	4.49	4.37	3.98	4.64	4.5	4.21	1.33	46.57	1.60	2.10
SD	1.02	0.72	0.68	0.61	0.49	0.56	0.71	0.42	13.45	0.491	1.11
Cronbach's alpha	0.85	0.86	0.76	0.81	0.84	0.84	0.79	0.58	–	–	–
Potential range	1–5	1–5	1–5	1–5	1–5	1–5	1–5	1–4	–	–	1–5
Minimum	1.00	1.00	1.00	2.00	3.00	1.67	2.00	1	20	–	1
Maximum	5.00	5.00	5.00	5.00	5.00	5.00	5.00	3.14	78	–	6

HRSB: high-risk security behaviors; SD: standard deviation.
Information Security Climate Index (ISCI) laxness was reverse coded. Gender is coded as 1 = male and 2 = female, Education is coded as 1 = MD/PhD, 2 = Master's degree, 3 = Bachelor's degree, 4 = some college, 5 = high school degree. N ranges from 223 to 252.
**$p < 0.01$.
*$p < .05$.

Table 3. Group means.

Occupational group	ISCI Total		Motivation		Compliance		Participation		High-risk security behaviors checklist	
	Mean	SD	Mean	SD	Mean	SD	Mean	SD	Mean	SD
CNA's	3.86	0.71	4.55	0.57	4.42	0.59	4.16	0.72	1.26	0.42
Dentist	4.01	0.67	4.50	0.52	4.41	0.59	4.22	0.70	1.31	0.39
Pharmacist	4.15	0.48	4.79	0.39	4.70	0.45	4.38	0.70	1.22	0.30
PA's	3.83	0.58	4.57	0.49	4.34	0.61	4.01	0.69	1.51	0.49

ISCI: Information Security Climate Index; CNA's: certified nursing assistants; PA's: physician assistants; SD: standard deviation.

Table 4. Significant post hoc tests (Tukey).

DV	Occupational category	Occupational category	Mean difference	Standard error	Significance
ISCI total	Pharmacist	PA's	0.3162	0.09584	0.006
Motivation	Pharmacist	CNA's	0.2446	0.09129	0.039
		Dentist	0.2910	0.08652	0.005
		PA's	0.2259	0.07740	0.020
Compliance	Pharmacist	CNA's	0.2849	0.10532	0.037
		Dentist	0.2902	0.09982	0.021
		PA's	0.3584	0.08930	0.000
Participation	Pharmacist	PA's	0.3651	0.11373	0.008
High-risk security behaviors checklist	PA's	CNA's	0.2504	0.07991	0.010
		Dentist	0.2047	0.07607	0.038
		Pharmacist	0.2954	0.06507	0.000

DV: dependent variables; ISCI: Information Security Climate Index; CNA's: certified nursing assistants; PA's: physician assistants.

observed power to detect a significant effect was 0.996. Given the detection of a significant main effect, we inspected the resulting univariate main effects (one-way ANOVAs), which examined whether there were differences in occupational groups for each variable. Significant main effects were detected for all variables: ISCI total ($F(3, 240)=4.324$, $p<0.01$, partial eta squared $=0.052$, power $=0.864$), motivation ($F(3, 240)=5.260$, $p<0.01$, partial eta squared $=0.062$, power $=0.926$), compliance ($F(3, 240)=6.396$, $p<0.01$, partial eta squared $=0.984$, power $=0.967$), participation ($F(3, 240)=3.519$, $p<0.05$, partial eta squared $=0.043$, power $=0.778$), and high-risk security behavior checklist ($F(3, 240)=7.389$, $p<0.01$, partial eta squared $=0.086$, power $=0.984$).

The significant ANOVA results indicate that there are mean differences among the occupational groups but do not pinpoint these differences. Therefore, Tukey post hoc tests were used to compare the mean scores among all occupational groups on the variables of interest. The occupational group means and standard deviations are reported in Table 3 and significant results of Tukey post hoc tests are reported in Table 4. Tukey post hoc test results indicate that for both motivation and compliance, the pharmacists' mean scores were significantly better than for the other three occupational groups. For the ISCI, the pharmacists' mean score was significantly better than only the PA's. Finally, for the high-risk security behavior checklist, the PA's engaged in

more high-risk security behavior than the other occupations. There were no significant differences between the pharmacists and the other occupational groups.

Discussion

The root of the majority of breaches lies with employee negligence and/or carelessness surrounding IS, something that cannot be fully mended through legislative or technological remediation.[8–11] As a result, it is necessary to focus on changing employees' behavior surrounding IS. To do this, we introduce the ISCI, a parsimonious (i.e. nine items) tool that was developed using two pilot studies, representing an extensive validation effort based on best practices in scale development.[50,52] The ISCI can be used by a variety of healthcare organizations to quickly and inexpensively assess their IS climate. This will allow these organizations to make decisions regarding where they should target IS interventions. The current approach differs from that of other instruments that take a case study approach to auditing organizations' policies, regulations, and training as opposed to employees' behavioral reactions to them.

Implications

The results of this study have important practical implications. Fundamentally, IS climate has the potential to positively impact employees' motivation and behavior, thereby ultimately reducing the number of data breaches. Given most data breaches are due to insider actions or lack of actions, a focus on organizational features that might affect employee behavior would be an obvious point of intervention. A number of studies in the safety climate literature have shown that training can be used to improve climate.[53] Such approaches could be modified to improve the IS climate of organizations that deal with sensitive data. Second, it seems that older employees are more careful with confidential data than are younger employees. Given that younger employees are often considered to be more "tech savvy," this finding was unexpected. It could be that older employees are more conscientious and therefore are more careful with patient data. Another interesting finding was that despite HIPAA laws governing all occupations, pharmacists seemed to have the best IS climate, motivation, and behaviors while PA's had some of the worst scores. Perhaps this occurred because the pharmacists, who often handle patients' sensitive data in front of other members of the public, are more aware of the importance of IS. Regarding PA's, it could also be the case that they sometimes consult with patients in waiting rooms in front of other patients and prioritize discussing a patient's health information over IS. Regardless of the reasons underlying the observed occupational differences, these results point to the need for additional IS training, especially for PA's. While some training should target the incumbents, research[38] suggests that training for the incumbents' supervisor might be more important given the central role he or she plays in shaping the organizational climate.[36,37]

Limitations

There are several limitations that should be kept in mind when interpreting the results of this study. First, the focus on IS could conflict with patient safety and care. This type of tension between competing priorities is inherent to the organizational climate approach and specifically exists in the safety climate domain between safety and expediency. That is, in order to behave safely, employees often have to work more carefully and slowly, thereby reducing productivity. The same tension likely exists in the IS climate domain as data security could compete with providing expedient or

quality care. This study did not directly address this underlying tension, but future studies should directly examine these competing priorities.

Another limitation is that the ISCI did not assess opportunities for training, which could reinforce desirable IS practices. Although the initial set of items contained several items related to training, the factor analysis did not support the inclusion of these items, indicating that these items were strongly related to other practice items and therefore subsumed within this factor. One reason for this could be that training supports the organizational climate but might not be a central component given organizational climate's focus on policies, practices, and procedures. In other words, training programs may alert employees of the proper practices and existing policies and procedures but that does not necessarily mean that IS will be prioritized in the workplace.

Furthermore, only four occupation groups in a single state were surveyed. Additional research, including additional occupational groups, throughout the United States is needed to generalize study findings. In addition, it is important to note that study data were cross-sectional and therefore causality cannot be inferred. Finally, this study did not examine whether IS climate differs among settings. It could be that retail pharmacies, where pharmacists are most often employed, have stronger IS climates than private practices. Future research should examine these settings to tease apart the role of the setting and the role of the occupation.

Conclusion

In conclusion, data breaches will likely continue to occur for the foreseeable future. Despite concerns about external hackers, much of the danger originates within organizations in the form of careless and/or negligent employee behaviors. An organizational climate approach represents a promising way to fundamentally change behavior. Study results indicated that an IS climate is related to desired employee behaviors, and thus, it can be potentially helpful for changing behavior surrounding information privacy and security.

Acknowledgements

All authors made a substantial intellectual contribution to the body of work.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Supplemental material

Supplemental material for this article is available online.

References

1. Doyle K. Health data breaches on the rise, 2015, https://www.reuters.com/article/us-health-data-security/health-data-breaches-on-the-rise-idUSKCN1M524J
2. Ponemon Institute, LLC. *Cost of data breach study: global analysis*, 2014, https://centurybizsolutions.net/wp-content/uploads/2014/12/IBM.pdf.

3. Scannell K and Chon G. Cyber security: attack of the health hackers, 2015, https://www.ft.com/content/f3cbda3e-a027-11e5-8613-08e211ea5317
4. Samy GN, Ahmad R and Ismail Z. Security threats categories in healthcare information systems. *Health Informatics J* 2010; 16(3): 201–209.
5. Ponemon Institute, LLC. Sixth annual benchmark study on privacy & security of healthcare data, 2016, https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf
6. U.S. Department of Health and Human Services Office for Civil Rights. Breach portal: notice to the secretary of HHS Breach of unsecured protected health information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
7. Kolbasuk McGee M. "Wall of shame" hits new milestone for health data breaches. *Data Breach Today*, 2017, https://www.databreachtoday.com/wall-shame-hits-new-milestone-for-health-data-breaches-a-10184
8. Verizon Risk Team. 2013 Data breach investigations report, 2013, http://www.eventtracker.com/eventtracker/media/eventtracker/files/collateral/verizon-data-breach-2013.pdf
9. *Secure web applications: building a security culture*. London: United Business Media, 2012.
10. Apkan N. Hacking health care records reaches epidemic proportions, 2016, https://www.scientificamerican.com/article/hacking-health-care-records-reaches-epidemic-proportions/
11. Blumenthal D and McGraw D. Keeping personal health information safe: the importance of good data hygiene. *JAMA* 2015; 313(14): 1424.
12. Haried P, Claybaugh C and Dai H. Evaluation of health information systems research in information systems research: a meta-analysis. *Health Informatics J* 2019; 25(1):186–202.
13. Schneider B, Ehrhart M and Macey W. Organizational climate and culture. *Annu Rev Psychol* 2013; 64: 361–388.
14. Victor B and Cullen J. A theory and measure of ethical climate in organizations. In: Frederick D (ed.) *Research in corporate social performance and policy*. Greenwich, CT: JAI Press, 1987, pp. 51–71.
15. Zohar D. A group-level model of safety climate: testing the effect of group climate on microaccidents in manufacturing jobs. *J Appl Psychol* 2000; 85(4): 587–596.
16. McKay P, Avery D and Morris M. Mean racial-ethnic differences in employee sales performance: the moderating role of diversity climate. *Pers Psychol* 2008; 61: 349–374.
17. Schneider B, White S and Paul MC. Linking service climate and customer perceptions of service quality: test of a causal model. *J Appl Psychol* 1998; 83(2): 150–163.
18. Kuenzi M and Schminke M. Assembling fragments into a lens: a review, critique, and proposed research agenda for the organizational work climate literature. *J Manage* 2009; 48: 1075–1089.
19. Chang S and Lin C. Exploring organizational culture for information security management. *Ind Manage Data Syst* 2007; 107: 438–458.
20. D'Arcy J and Greene G. Security culture and the employment relationship as drivers of employees' security compliance. *Inf Manag Comput Secur* 2014; 22: 474–489.
21. Ruighaver S, Maynard SB, Chang S, et al. Organisational security culture: extending the end-user perspective. *Comput Secur* 2007; 25: 56–62.
22. Van Niekerk J and Von Solms R. Information security culture: a management perspective. *Comput Secur* 2010; 29: 476–886.
23. Von Solms R and Von Solms B. From policies to culture. *Comput Secur* 2004; 23: 275–279.
24. Vroom CVSC. Towards information security behavioural compliance. *Comput Secur* 2004; 23: 191–198.
25. Chan M, Woon I and Kankanhalli A. Perceptions of information security in the workplace: linking information security climate to compliant behavior. *J Inf Privacy Secur* 2005; 1: 18–41.
26. Goo J, Yim M and Kim D. A path to successful management of employee security compliance: an empirical study of information security climate. *IEEE T Profess Commun* 2014; 57: 286–308.
27. da Veiga A and Eloff JHP. A framework and assessment instrument for information security culture. *Comput Secur* 2010; 29: 196–207.
28. da Veiga A and Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Comput Secur* 2015; 49: 162–176.

29. da Veiga A and Martins N. Defining and identifying dominant information security cultures and subcultures. *Comput Secur* 2017; 70: 72–94.
30. Cram WA, Proudfoot JG and D'Arcy J. Organizational information security policies: a review and research framework. *Eur J Inf Syst* 2017; 26: 605–641.
31. Reichers AE and Schneider B. Climate and culture: an evolution of constructs. In: Schneider B (ed.) *Organizational climate and culture*. San Francisco, CA: Jossey-Bass, 1990, pp. 5–39.
32. Ashkanasy NM, Broadfoot LE and Falkus S. Questionnaire measures of organizational culture. In: Ashkanasy NM, Wilderom CP and Peterson MF (eds) *Handbook of organizational culture and climate*. Thousand Oaks, CA: SAGE, 2000, pp. 131–145.
33. Schein EH. *Organizational culture and leadership*. 4th ed. San Francisco, CA: Jossey-Bass, 2010, p. 179.
34. Bruursema K. *How individual values and trait boredom interact with job characteristics and job boredom in their effects on counterproductive work behavior*. Doctoral Dissertation, University of South Florida, Tampa, FL, 2007.
35. Gatersleben B, Murtagh M and Abrahamse W. Values, identity and pro-environmental behavior. *Contemp Soc Sci* 2014; 9: 374–392.
36. Zohar D and Hofmann D. Organizational culture and climate. In: Kozlowski S (ed.) *The Oxford handbook of organizational psychology*. New York: Oxford University Press, 2012, pp. 643–666.
37. Zohar D and Luria G. A multilevel model of safety climate: cross-level relationships between organization and group-level climates. *J Appl Psychol* 2005; 90(4): 616–628.
38. Zohar D and Luria G. The use of supervisory practices as leverage to improve safety behavior: a cross-level intervention model. *J Safety Res* 2003; 34(5): 567–577.
39. Herath T and Rao HR. Protection motivation deterrence: a framework for security policy compliance in organisations. *Eur J Inf Syst* 2009; 18: 106–125.
40. Neal A and Griffin MA. A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels. *J Appl Psychol* 2006; 91(4): 946–953.
41. Beus J, Dhanani L and McCord MA. A meta-analysis of personality and workplace safety: addressing unanswered questions. *J Appl Psychol* 2015; 100(2): 481–498.
42. Beus JM, Payne SC, Bergman ME, et al. Safety climate and injuries: an examination of theoretical and empirical relationships. *J Appl Psychol* 2010; 95(4): 713–727.
43. Christian MS, Bradley JC, Wallace J, et al. Workplace safety: a meta-analysis of the roles of person and situation factors. *J Appl Psychol* 2009; 94(5): 1103–1127.
44. Clarke S. Safety leadership: a meta-analytic review of transformational and transactional leadership styles as antecedents of safety behaviours. *J Occup Organ Psychol* 2013; 86: 22–49.
45. Foster NJ. Culture sets the tone for effective cyber security. *RMA J* 2014; 97: 1–8.
46. Baldi M and Gold S. Treat security like safety. *Hydrocarb Process* 2014; 93: 47–50.
47. Neal A and Griffin MA. Safety climate and safety at work. In: Barling J and Frone MR (eds). *The psychology of workplace safety*. Washington, DC: American Psychological Association, 2004, pp. 15–34.
48. Muthén L and Muthén BO. *Mplus user's guide*. 7th ed. Los Angeles, CA: Muthén & Muthén, 1998–2012.
49. Gefen D, Rogdon E and Straub D. An update and extension to SEM guidelines for administrative and social science research. *MIS Quart* 2011; 35: iii–xiv.
50. Nunnally JC. *Psychometric theory*. 2nd ed. New York: McGraw-Hill, 1978.
51. Spector PE and Jex SM. Development of four self-report measures of job stressors and strain: interpersonal conflict at work scale, organizational constraints scale, quantitative workload inventory, and physical symptoms inventory. *J Occup Health Psychol* 1998; 3(4): 356–367.
52. DeVellis RF. *Scale development theory and applications*. Thousand Oaks: CA: SAGE, 1991.
53. Lee J, Huang YH, Cheung JH, et al. A systematic review of the safety climate intervention literature: past trends and future directions. *J Occup Health Psychol* 2019; 24: 66–91.