Appendix 1. Development of the ISCI Survey Instrument

Item Writing

To develop the Information Security Climate Index (ISCI), study authors identified 206 relevant items from the safety literature.[1-6] These items were then adapted to the information security domain by the study authors. Additional items, not based on prior scales, were written specifically to reflect cybersecurity climate. Authors completed three rounds of item writing and revisions in order to ensure that the adapted and new information security items retained their original meaning but fit within an information security context. The items were then screened for clarity and redundancy, reducing the item pool to 74 distinct items to be empirically examined.

Pilot Study 1

To pilot test these items, authors collected a sample of 222 working individuals (male = 33; female = 177; with 12 not providing this information) recruited from classes at a large southeastern U.S. university. All items were assessed along a six point Likert scale with 1 indicating "disagree very much" and 6 indicating "agree very much." To empirically examine the dimensionality of the underlying construct, and to reduce the number of items to a reasonable number, an initial maximum likelihood factor analysis with varimax rotation was conducted. An examination of the scree plot, a graphical depiction of factors accounted for by the analysis, suggested that three underlying factors accounted for 66.85% of the total variance with factor 1 accounting for 53.22% of the variance, factor 2 accounting for 8.75% of the variance, and factor 3 accounting for 4.89% of the variance. Each additional factor accounted for less than 2.5% of the variance. We then re-ran the factor analysis, rotating three orthogonal factors. To keep factors as distinct as possible, items that loaded at least .70 on one factor but not above .35 on another factor were retained. This resulted in 14 items. Upon inspection, three items were

deleted: “I loan my work laptop to friends and family when I am not using it,” “My supervisor seriously considers any worker's suggestions for improving data security,” and “My employer requires that employees who save organization information to personal devices, like smart phones, follow organization security policies for that data.” The first item was deleted because it reflected a specific behavior and not climate. The second item was deleted because its meaning was duplicative of an existing item. Finally, the third item was deleted because, while reflective of good organizational practices, it was too specific to assess climate across organizations. This is because many organizations have policies that require that employees store data solely on organizational property. This resulted in 4 items on factor 1, 3 items on factor 2, and 4 items on factor 3 for a total of 11 items.

The resulting rotated component matrix for this factor analysis is available in Table A1. An inspection of the content suggested that the three factors assessed meaningful and distinct aspects of climate. Items on the first subscale, named “Practices” reflected information security practices within the organization. This included behaviors and discussions that are actively initiated (particularly by the supervisor) in the interest of promoting information security. Items on the second subscale termed “Importance” focused on the priority given to information security. It concerns the importance people in the organization place on the protection of confidential data. Finally, items on the third subscale focused on the competing interests between information security and the completion of work tasks. As a result, we named this subscale “Laxness” and define it as the prioritization of other activities (particularly work activities) over information security. To keep a consistent scaling where high scores indicate a favorable organizational climate for promoting information security, the items on this subscale were reverse scored.

Table 1: Study 1 Exploratory Factor Analysis Results

Item	Factor		
	Practices	**Importance**	**Laxness**
Data security issues are discussed in meetings.	**.721**	.310	-.002
My supervisor frequently checks to see if we are all obeying the data security rules.	**.751**	.307	-.170
My supervisor frequently talks about data security issues throughout the work week.	**.800**	.223	-.246
My supervisor says a good word whenever he sees actions taken that promote data security.	**.733**	.253	-.215
It is worthwhile to put extra effort into maintaining data security.	.332	**.872**	-.044
It is important to maintain data security at all times.	.311	**.902**	-.016
It is important to reduce the risk of data breaches in the workplace.	.299	**.832**	.007
In my unit in order to get the work done, one must ignore some data security policies.	-.182	.069	**.802**
In my unit, data security policies and procedures are routinely ignored.	.017	-.015	**.795**
In my unit, ignoring data security procedures is acceptable.	-.015	.065	**.791**
My supervisor expects me to cut corners regarding data security and work faster when work was behind schedule.	-.197	-.009	**.766**

Scale Refinement

To ensure that healthcare professionals would easily understand the meaning of these items, we asked a subject matter expert (SME) within the healthcare field to review the 11 items. The SME suggested small changes in terminology that did not seem to affect the underlying meanings. For example, terminology reflecting "data security" and "information security" were changed to indicate "protection of private data."

We also assess content validity to ensure that that scale items reflect the proposed factor domain. To do this, we employed Hinklin and Tracey's[7] variance analysis approach whereby we

gave three information security SME's who also had training in organizational climate research the definitions of the three subscales and asked them to assign each of the 11 items into one of three subscales. SME's were provided a rating sheet and the following instructions: "Using the definitions provided, please rate each item of the 11 items on the extent to which the item captures each construct domain (i.e., practices, importance, and laxness) with 1 indicating 'not at all' and 5 indicating 'completely.'" We calculated the mean responses for each item's score on each construct domain. With one exception, the mean scores were much higher for each item within its proposed construct domain than in the other two construct domains. Therefore, we chose to discard the item, resulting in a 10-item scale with 4 items representing the Practices domain and 3 items each representing the Importance and Laxness domains.

Pilot Study 2

To confirm the factor structure derived from the exploratory factor analysis, an additional sample was collected from the same population as sample 1. This sample included 302 working individuals (male = 57) and (female = 245). Participants were asked to complete the ISCI with the items being assessed along a five point Likert scale with 1 indicating "disagree very much" and 5 indicating "agree very much" (the change to a five point scale was done in order to allow a neutral option).

To re-examine the measurement model, a second order confirmatory factor analysis was conducted in which we loaded items onto the proposed scale factor (i.e., first order factors) and then the three factors onto the second order factor of information security climate. To determine the fit of the current model, a collection of fit indices were examined. Gefen et al.[8] indicates that the fit indices of CFI and TLI should be above .90 and that the RMSEA fit index should be below .08. They also indicate that "it is acceptable that not all fit indexes be within these

threshold rules of thumb."[8p. x] Therefore, results indicated adequate support[8] with the RMSEA index just above the .08 threshold but the other fit indices above the .90 threshold [$\chi^2_{(32)}$ = 121.405, p = .000, RMSEA = .096; CFI = .941; TLI = .918]. Additionally, Cronbach alphas for the three subscale were above the .70 threshold[9] and are as follows: Subscale 1, Practices (alpha = .82); Subscale 2, Importance (alpha = .90); and Subscale 3, Laxness (alpha = .74).

Appendix 2. Adaptation of Safety Indicators to the Information Security Domain

Safety	Information Security
Motivation	
1. I feel that it is worthwhile to put in effort to maintain or improve my personal safety.	1. I feel that it is worthwhile to put in effort to protect private data.
2. I feel that it is important to maintain safety at all times.	2. I feel that it is important to protect data privacy at all times.
3. I believe that it is important to reduce the risk of accidents and incidents in the workplace.	3. I believe that it is important to reduce the risk of data breaches in the workplace.
Participation	
1. I promote the safety program within the organization.	1. Within the organization, I promote the protection of private data.
2. I put in extra effort to improve the safety of the workplace.	2. In the workplace, I put in extra effort to protect confidential data.
3. I voluntarily carry out tasks or activities that help to improve workplace safety.	3. I voluntarily carry out tasks or activities that help to protect confidential data.
Compliance	
1. I use all the necessary safety equipment to do my job.	1. I use all the necessary tools to do my job so that I do not compromise confidential data.
2. I use the correct safety procedures for carrying out my job.	2. When carrying out my job, I use the correct procedures concerning the protection of private data.
3. I ensure the highest levels of safety when I carry out my job.	3. I ensure the highest levels of data privacy when I carry out my job.

Appendix 3. High Risk Security Behavior Checklist

1. **How many times in the past week has patient data been left unattended?**

None
1-2 times
3-4 times
5 or more times

2. **How many times in the past year have you left a computer unlocked with patient data showing?**

None
1-2 times
3-4 times
5 or more times

3. **How many times in the past year have you knowingly violated a data security policy at work?**

None
Once
Twice
Three times or more

4. **How many times in the past year have you shared sensitive information with someone you should not have?**

None
Once
Twice
Three times or more

5. **How many times in the past year have you taken home sensitive information without permission?**

None
Once
Twice
Three times or more

6. **How many times in the past year have you put a personal thumb drive into a work computer without permission?**

None
Once
Twice
Three times or more

7. **How many times in the past year have you taken a laptop or other device home that had sensitive information?**

None
Once
Twice
Three times or more

Appendix 4. Information Security Climate Scale and Subfactors

Definition: Shared perceptions of the information security policies and their manifestations in the organization. These can be categorized into the following: what is practiced in the organization, the observed importance surrounding information security in the organization, and the laxness surrounding information security activities.
Factor 1: Practices
Definition: Practices refers to behaviors and discussions that are actively initiated by the supervisor in the interest of promoting information security.
1. My supervisor frequently checks to see if we are all obeying rules related to the protection of private data.
2. Throughout the work week, my supervisor frequently talks about issues related to the protection of private data.
3. My supervisor says a good word whenever he sees actions taken that promote the protection of private data.
Factor 2: Importance
Definition: The importance placed on the protection of confidential data.
1. In my workplace it is worthwhile to put extra effort into protecting private data.
2. In my workplace it is important to maintain the protection of private data at all times.
3. In my workplace it is important to reduce the risk of data breaches.
Factor 3: Laxness
Definition: Prioritizing other activities (particularly work activities) over information security.
1. In my workplace in order to get the work done, one must ignore some policies related to the protection of private data.
2. In my workplace, policies and procedures regarding the protection of private data are routinely ignored.
3. My supervisor expects me to cut corners regarding the protection of private data and work faster when work is behind schedule.