THE HUMAN FACTOR IMPACT ON COMMUNITY COLLEGE SECURITY CULTURE

by

GAIL VOLZ

B.S., University of Georgia, 1985

M.S., Rensselaer Polytechnic Institute, 1988

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2025

The human factor impact on community college security culture

Gail Volz, *Middle Georgia State University, gail.volz@mga.edu*

Abstract

As community colleges increase their dependence on technology, cyber adversaries increase attacks on community colleges. The community college's security culture establishes the user's capacity to protect information resources. The purpose of this research is to investigate the human aspects of security culture in community colleges by analyzing the security knowledge, attitudes, and behaviors of faculty, staff, and students. Multiple regression analysis is used to determine which variables, knowledge, attitude, or behavior, contribute significantly to predicting security culture. The findings indicate all three variables significantly contribute to an organization's security culture. The study results support the development of changes to the community college's security policy and procedures to minimize cyber-attack impacts.

Keywords: Cyber security culture, KAB Model, Community college, HAIS-Q

Introduction

Current research identifies higher education institutions (HEIs) as a top target for hackers, with nearly 2,300 attacks per week. Community colleges play an increasingly significant role in providing new, innovative, and critically needed higher education (HE) and workforce opportunities (Mayfield et al., 2022). Over the last decade, community colleges have increased their dependency on technology. Community colleges are designed to be open environments combining sensitive, publicly available, and proprietary information in one technology infrastructure. This infrastructure supports an ecosystem that includes a mixture of faculty, staff, and students (Cheng & Wang, 2022). The ecosystem's dependency on technology exposes the community college to cyber threats.

Historically, community colleges rely on technology augmented with training and awareness programs to prevent cyber threats (Wiley et al., 2019). With the cyber adversary focused on community colleges increasing, technological mitigations are not sufficient to combat the increasing threats. Technological approaches augmented with training do not address the human aspect introduced by users. Understanding the role of the human element is essential for implementing or improving HEI security posture (Durojaiye et al., 2020).

This study examines the human aspects of security culture in community colleges by analyzing the security knowledge, attitudes, and behaviors of faculty, staff, and students. This study will answer the following research question:

RQ1: Which of the three independent variables (security knowledge, attitude, and behavior) are significant in predicting security culture?

The research results will identify the independent variables (security knowledge, attitude, and behavior) that contribute significantly to predicting the dependent variable (security culture). By understanding community college faculty, staff, and students' security culture, gaps in security operations can be identified, and potential gap solutions can be provided to leadership. Furthermore, this information offers a foundation for a community college security culture baseline, which can be utilized to compare against future research.

The remainder of this paper is organized as follows: literature review; methodology; results; discussion; and conclusion.

Review of Literature

Early information security research focused on corporate and government entities (Hina et al., 2019; Durojaiye et al., 2020). With the increase in cyber-attacks on HEIs, researchers redirected their attention to HEIs. From a review of a wide range of subjects, a recurring theme developed. This theme singled out the avoidance of technology as the sole information security solution (Durojaiye et al., 2020; Parsons et al., 2013).

The goal of security culture is to create an environment that encourages and supports users to protect information assets. Various fields of study, such as psychology, economics, behavioral sciences, and management, contribute to the definition of security culture. Several information security studies attempt to define security culture (Phillips et al., 2023; Uchendu et al., 2021, Hina et al., 2019). Defining security culture is complicated due to the multiple terms used to refer to the concept. These terms include security culture, cybersecurity culture, and information security culture. Uchendu et al. (2021) concluded that no widely used definition existed. Proposed definitions incorporated a myriad of concepts including organizational culture (Phillips et al., 2023; Uchendu et al., 2021), social-cultural measures (Uchendu et al., 2021), Protection Motivation Theory (Hina et al., 2019), organizational functions (Uchendu et al., 2021) and Theory of Planned Behavior (TPB) (Hina et al., 2019). A common thread throughout the definitions is a connection between positive cybersecurity implementation and behavior (Hina et al., 2019; Phillips et al., 2023; Uchendu et al., 2021). Security researchers agree that security culture incorporates the assumptions, attitudes, beliefs, values, and knowledge that individuals use to interact with an organization's systems (Wiley et al., 2019). Measuring security culture presents a unique challenge to the organization. Parsons et al. (2014) identified that users' knowledge, attitudes, and behaviors play a role in measuring security culture.

The Knowledge, Attitude, and Behavior (KAB) model originated in education research and is implemented heavily in the health, criminology, and environmental psychology fields. The model defines three domains: cognitive (knowledge), affective (attitude), and psychomotor (behavior). The knowledge domain incorporates all information that a person accumulates related to a particular subject area. The attitude domain defines a person's way of feeling (perceptions) about an object. The behavior domain identifies the way a person acts to a given set of conditions (Schrader & Lawless., 2004). Kruger and Kearney (2006) developed a prototype for assessing information security awareness based on the KAB model. Parsons et al. (2013) extended Kruger and Kearney's work by developing the Human Aspects of Information Security Questionnaire (HAIS-Q). The historical use of HAIS-Q across multiple disciplines investigating multiple populations makes it an excellent candidate for the study of security culture in community colleges.

Uchendu (2021) identified knowledge as a key part of security culture. Multiple studies have demonstrated that as users' cybersecurity knowledge increases, their attitude toward information security improves, resulting in improved information security behavior (Parsons et al., 2017; Parsons et al., 2013; Li et al., 2021). Durojaiye et al. (2020) concluded that investing in training and awareness programs focusing on communication, engagement, collaboration, and social engineering would increase security posture at higher education institutions. According to Durojaiye et al. (2020), these factors influence personnel and students' views of cybersecurity compliance. In addition, Durojaiye et al. (2020) recommended cybersecurity culture as a future research area. Li et al. (2021) conducted an empirical study investigating faculty, staff, and student cybersecurity perceptions on information security compliance. Their study concluded faculty and staff exhibit more compliant cyber behaviors. They recommended analyzing participants' behavior vice prospective perception in future studies. Nguyen and Le's (2024) investigation highlighted the effect of education level on cybersecurity knowledge. They found that security knowledge and attitude explain a significant amount of the variance in employee self-reported security behavior.

Attitude represents the individual's perception of the psychological object. According to Schrader and Lawless (2004), an individual's knowledge may inform their attitude about a topic, and how they feel about

it may influence behavior. Research conducted by Parsons et al. (2013) identified generic courses that simply lecture on information security, increasing knowledge only, are less effective than courses that influence security attitudes. They suggest courses that teach both knowledge and why it matters are necessary for security posture improvement. Investigating the effect of employee organizational attitudes on security compliance, Kam et al. (2021) determined that employee perceptions are key factors in how they behave. They concluded that employees with an attitude in favor of stability and control promoted more positive security-related behaviors.

Effective cyber security protects an organization's data by using acceptable behaviors. Hina et al. (2019) recommended security culture creation as a solution to issues associated with negative security compliance behavior. Alanazi et al. (2022) studied the aspects of young adults' cybersecurity behaviors. Their study concluded that the need for cybersecurity behavior and intention to practice cybersecurity were related to following good cybersecurity behaviors. Hong et al. (2023) extended the KAB model to include social factors. Analyzing the effects of social educational level (SEL) on information security knowledge, attitude, and behavior, their results identified that SEL has a strong effect on all KAB variables. Nguyen and Le (2024) studied cyber behavior with respect to age and education level. They found younger employees display a more positive attitude and behavior toward information security compared to older counterparts. They postulate, with significant organizational support, that younger employees with better behavior can positively influence older colleagues.

The Human Aspects of Information Security - Questionnaire (HAIS-Q) developed by Parsons et al. (2013) utilizes the Knowledge, Attitude and Behavior (KAB) model which assumes knowledge, attitude, and behaviors are connected and affect an individual's actions. The questionnaire has been validated by many studies, including Parsons et al. (2013), Parsons et al. (2017), Hong et al. (2023), and Xu et al. (2023), to name a few. The populations utilized with the questionnaire included students, the general public, employees from the government, financial institutions, and HEIs. The questionnaire design uses a modular approach, allowing for only relevant items to be implemented (Parsons et al., 2013; Parsons et al., 2017; Hong et al., 2023). Validation results identify that an increase in security knowledge positively impacts attitude and behavior (Parsons et al., 2017). Exploiting the modular approach, Hong et al. (2023) explored potential relationships between employee knowledge, attitude, behavior, and social education. Xu et al. (2023) utilized the HAIS-Q to investigate KAB effects based on gender, discipline, and grade of students. Like Hong et al. (2023), Xu et al. (2023) modified the instrument. Their results provided additional HAIS-Q validation in the higher education environment.

Over the last decade, higher education security research concentrated on managerial aspects, cybersecurity perceptions, information security compliance, and information security awareness. The data from these studies supported the development of information security programs in HEIs (Cheng & Wang, 2022; Durojaiye et al., 2020). However, cyber breaches against HEIs continue to occur. As evident in the multiple calls for future research to include security culture, security culture is an underdeveloped research domain.

Methodology

Participants

This study utilized a convenience sample of the faculty, staff, and students at a community college in the southeastern portion of the United States. The researcher received approval from the Institutional Review Board (IRB) to survey human subjects. Participants received an email inviting them to participate in the survey hosted by SurveyMonkey. This type of distribution presents possible challenges to response quality and rate. According to Parson et al (2014), self-reporting behavioral responses are susceptible to the participants either providing socially acceptable responses or not providing accurate responses due to fear of punishment for wrongdoing. Neither issue is expected as study participants were not asked to provide

identifiable information and were assured confidentiality and anonymity. The survey was sent to 3047 subjects.

Of the 210 responses 23 responses were found to only contain demographic data and were deleted. Four more responses contained one missing response each and were deleted. The survey contains 18 security-based statements. Of the 18 statements, 10 were positively worded and 8 were negatively worded. The responses were examined for replies made without regard to statement content. Participants who consistently choose strongly disagree or strongly agree exhibit this type of response. No response met the criteria. This resulted in 183 surveys completed for a response rate of 6%. The 6 % response rate falls within an acceptable response rate range of 5% - 30% (Le Masson, 2023).

Instrumentation

The study utilized the HAIS-Q instrument developed by Parsons et al. (2013). The original HAIS-Q instrument contained seven (7) focus areas. Each focus area contains three (3) statements in each of the domains (Knowledge, Attitude, and Behavior). The base instrument contains 63 total statements. This study follows Parsons et al. (2017) recommendation of using aspects of the instrument for a particular study by limiting the focus areas to two - Internet Use and Mobile Devices. In addition to using a subset of the original statements, statement verbiage was modified for use with US English in a collegiate setting. In total, participants responded to 23 statements. The constructs are demographics - 5 items, cyber knowledge - 6 items, cyber attitude - 6 items, and cyber behavior - 6 items. Two cyber professionals and one educational professional reviewed the survey statements for completeness. Updates from the reviewers were incorporated into the final survey statement list. The instrument is a 5-point Likert-type and includes the following scoring strategy: 5 = Strongly Agree, 4 = Agree, 3 = neither agree nor disagree, 2 = disagree, 1 = strongly disagree.

Procedures

Using the professional internet survey company, SurveyMonkey, the survey was distributed to 3047 participants via email. The participants were required to accept the consent form to complete the survey. After 3 weeks of data collection, the responses were exported from SurveyMonkey to Excel and imported into the Statistical Package for Social Science (SPSS) program. The collected data was inspected by the researcher before analysis to ensure data integrity and completeness.

Multiple regression analysis was used to answer the research question. The multiple regression analysis process looks at the regression analysis model coefficients table to determine the predictor (independent) variables most influential in predicting the dependent variable (Thompson, 2012). In addition to multiple regression analysis, descriptive statistics were generated for the demographic data, dependent variable, and independent variables.

Results

Demographic data is presented in Table 1. Table 2 presents the descriptive statistics for the independent variables (Knowledge, Attitude, and Behavior) and dependent variable (Security Culture). To check the reliability of the items, Cronbach's α coefficients are calculated for each of the independent variables. The Cronbach's α for each variable is reported in Table 3. All variables show acceptable levels of reliability. According to Hair et al. (2010), Cronbach's α values above 0.6 may be considered acceptable.

Table 1

Demographic Descriptive Statistics, n = 183

Characteristic	*n*	%	Characteristic	*n*	%
Age			Academic School		
18-20	22	12	Arts & Science	24	13.1
21-30	49	26.8	Business, Cyber & Design	73	39.9
31-40	36	19.7	Health Science	44	24
41-50	34	18.6	Professional	13	7.1
Over 50	42	23	Engineering	14	7.7
			Other	15	8.2
Gender			Role		
Female	116	63.4	Faculty	35	19.1
Male	65	35.5	Student	114	62.3
Other	2	1.1	Staff	34	18.6
HE Security Course					
Yes	55	30.1			
No	128	69.9			

Table 2

Variable Descriptive Statistics, n = 183

Variable	M	SD
KNOWLEDGE	4.16	0.77
ATTITUDE	4.57	0.73
BEHAVIOR	4.18	0.57
SC	4.28	0.42

Table 3

Independent Variable Cronbach's α

Variable	*n*	Cronbach's α
KNOWLEDGE (Q1, Q3, Q6, Q7, Q8)	5	0.82
ATTITUDE (Q13, Q14)	2	0.67
BEHAVIOR (Q12, Q15, Q16, Q17, Q18)	5	0.62

Regarding the research question, a multiple regression test is used to analyze the data as the data contains multiple predictor (independent) variables and one outcome (dependent) variable. Multiple regression test assumptions ensure the robustness of the prediction model generated. Multiple regression analysis assumptions include *n* Quota, linearity, homoscedasticity, multicollinearity, and normality (Knapp, 2018).

The *n* Quota assumption ensures the sample population is large enough to provide a generalization to the population at large. The minimum sample size is based on calculations using both the continuous and

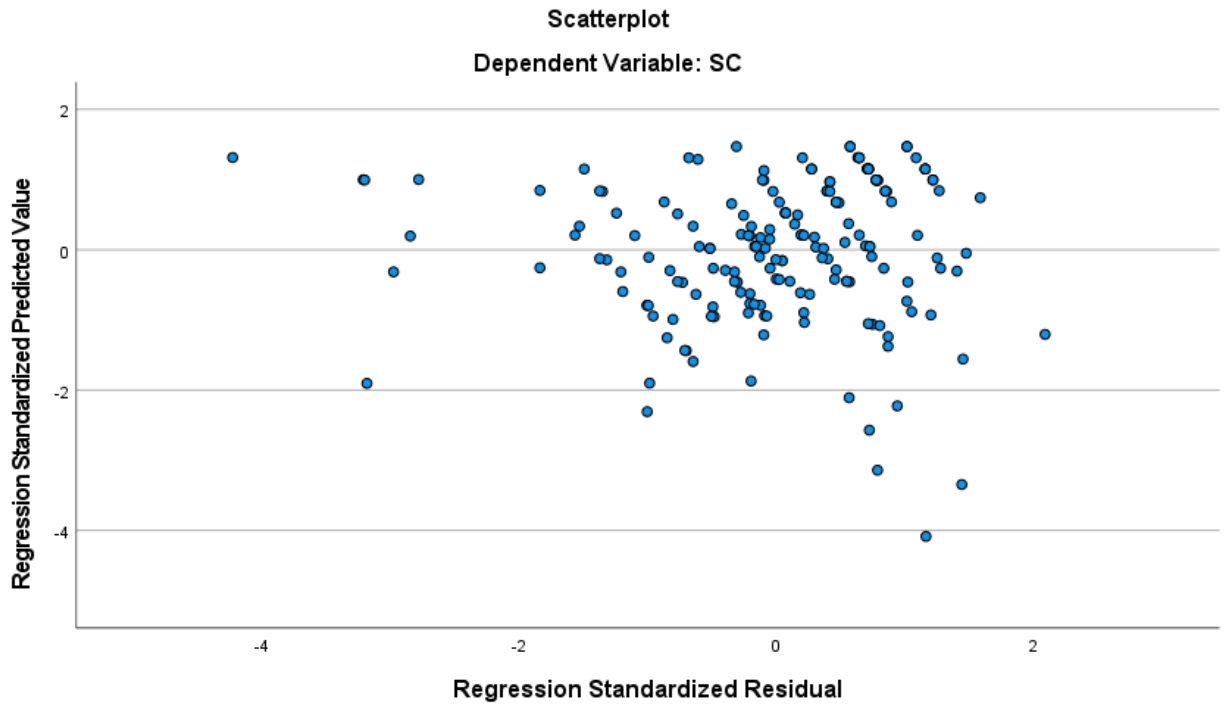
categorical data analyzed (Knapp, 2018). This study analyzed three continuous variables; therefore, the minimum *n* is 30. The study contained 183 usable responses. The *n* Quota assumption is met.

Multiple regression analysis assumes a linear relationship exists between the independent and dependent variables. To validate the linearity between the independent and dependent variables scatter plots are generated. One scatter plot per independent variable paired with the dependent variable is examined for data points falling around the best-fit line (Knapp, 2018). Examination of the three individual scatter plots revealed no violation of linearity. The linearity assumption is met.

Homoscedasticity is an indication of consistent variance differences between the predicted and actual values across different values of the independent variable. Inconsistent variances can lead to skewed results. To check for homoscedasticity, a scatter plot of the residuals against predicted values is generated. The plot is examined for a cluster of data points within ±2 standard deviations (Knapp, 2018). Examination of the scatter plot revealed that 93% of the points met the requirement (Figure 1). The homoscedasticity assumption is met.

Figure 1

Residual Scatter Plot



Multicollinearity occurs when two or more independent variables are highly correlated. The non-existence of multicollinearity is indicated by the tolerance level values above .1 and the variance inflation factor (VIF) values below 10 for all predictor variables (Knapp, 2018). Table 4 presents the multiple regression test coefficients table data. The tolerance level and VIF values reported indicate the nonexistence of multicollinearity. The multicollinearity assumption is met.

In multiple regression, normality pertains to the distribution of the residuals in the outcome variable (Knapp, 2018, p. 326). To test for normality, a histogram with the normal curve is built for the unstandardized

Table 4

Multiple regression coefficients (Dependent Variable: SC)

Variable	Unstandardized Coefficients		Standardized Coefficients	t	Sig	Collinearity Statistics	
	β	Std. Error	β			Tolerance	VIF
(Constant)	0.948	0.083		11.456	0.000		
KNOWLEDGE	0.315	0.013	0.579	23.935	0.000	0.833	1.200
ATTITUDE	0.147	0.014	0.254	10.860	0.000	0.892	1.121
BEHAVIOR	0.322	0.018	0.437	18.153	0.000	0.841	1.189

residuals. The normal curve is examined for symmetry. No notable skewness was found in the residual histogram. Therefore, the normality assumption is met. To determine which independent variable is most influential in predicting the dependent variable, the regression analysis model coefficients table is examined. The interpretation of the coefficient table is contingent upon three critical tests (Thompson, 2012).

First, a multicollinearity test is performed. As shown previously, the tolerance level and VIF values reported indicate the nonexistence of multicollinearity.

Second, the model summary or goodness of fit test results are analyzed to determine if the model is a good representation of the relationship between the independent and dependent variables. A good representation is indicated by the coefficient of determination (R^2) values between 0 and 1, where 1 identifies a perfect fit. The adjusted R^2 value indicates the dependent variables predict the SC variable well ($R = .955$, $R^2 = .913$, and $R^2adj = .911$).

Third, the Analysis of Variance (ANOVA) test is performed to show a linear relationship between the dependent and independent variables. ANOVA *p*-values of < .05 indicate the independent variables reliably predict (linear relationship) the dependent variable (Knapp, 2018). The test indicated a linear relationship between the dependent variables (KNOWLEDGE, ATTITUDE, BEHAVIOR) and security culture (SC) ($F(3, 179) = 624.48$, $p < .001$**).** This model is significant, and we can conclude that the variables, KNOWLEDGE, ATTITUDE, and BEHAVIOR, together predict the dependent variable.

To determine which independent variable is most influential in predicting the dependent variable, the regression coefficient (β) for each independent variable is reviewed. The positive β values indicate each of the independent variables positively affects the dependent variable. The variable with the largest regression coefficients (β) accounts for the most variance in the dependent variable and therefore is the most influential. Regarding the variables, KNOWLEDGE, ATTITUDE, and BEHAVIOR, the most influential variable on security culture (SC) is KNOWLEDGE ($\beta = .579$, $p = .000$).

Discussion

This research investigated the human aspects of security culture in community colleges by analyzing the security knowledge, attitudes, and behaviors of faculty, staff, and students. The analysis discovered that among knowledge, attitude, and behavior, security knowledge is the most influential characteristic of community college security culture. Using multiple regression analysis, the study built a security culture prediction model. This model identified all three independent variables as being significant with security

knowledge influencing security culture the most. The model's positive coefficient values for all three independent variables suggest that all three variables influence security culture positively (increasing security culture).

A positive security culture increases an organization's ability to protect its information assets (Hina et al., 2019). Understanding the role people play concerning cybersecurity enables leaders to make better security decisions. The analysis suggests that improving security knowledge increases security culture. The results are in line with Nguyen and Le (2024) and Uchendu et al. (2021). Supported by Cheng and Wang's (2022) conclusion that training and awareness can be used to build security culture, community college leaders can use the data to focus security education events to improve security posture. Security engineers can use the results to focus on detecting potential security knowledge gaps in the community college's ecosystem. This finding implies that developing security education targeted at specific groups may increase data protection, which is consistent with Durojaiye et al. (2020). Durojaiye et al. observed that the HEI student population typically does not receive onboard cybersecurity training and awareness, leading users to engage in potentially unsafe practices. Complementing the Durojaiye et al. findings, Li et al. (2021) found that as students' cyber knowledge increased, students followed safer practices.

Significance

This investigation is one of a small number of studies to examine security culture within the community college ecosystem. The literature review revealed that historically HEI cybersecurity research targeted University populations (4-year schools). The community college ecosystem is an underrepresented population. In addition, the study provides both theoretical and practical contributions.

From a theoretical perspective, it establishes a foundation of data to further investigate higher education security culture. Understanding the community college security culture provides insights on how to increase security posture. Prior research focused on using the KAB model to analyze relationships between Information Security Awareness (ISA) and individual demographics (gender, age, class standing, etc.). Many of these studies called for security culture investigations (Cheng and Wang, 2022; Hina et al., 2019; Wiley et al., 2019; Durojaiye et al., 2020). Also, the study provides reliability data for a scaled-down HAIS-Q implementation. This finding supports Parsons et al. (2017) HAIS-Q modular design assertion.

Practical contributions include identifying where HEI leaders and security practitioners should focus their attention to increase security culture. Community college leaders and security practitioners can use this information to develop policies and procedures to mitigate cyber-attack impacts. Furthermore, this study provides a whole ecosystem (faculty, staff, and students) security culture analysis supporting the call for future investigations to use system-wide approaches (Cheng and Wang, 2022). The study method can be used before and after educational events to assess training progress by comparing it to baseline data.

Limitations

This study provides exploratory evidence that a community college user's security knowledge is the key factor in security culture. Limitations to this study include exploratory results, limited sample size, and self-reporting. The HAIS-Q design allows for the implementation of only relevant items (Parsons et al., 2017). Most studies found during the literature review applied all 63 original HAIS-Q statements. This study delivered initial insights on the use of a scaled-down HAIS-Q. Future studies should provide additional validation and reliability of a scaled-down HAIS-Q implementation. In addition, the exploratory results identified knowledge as the key influential KAB element on security culture but did not identify specific groups to target with education. Future studies should explore specific demographic areas to target knowledge training events. Study participants were recruited using an unsolicited email administered by SurveyMonkey. This type of study participant recruitment is common however, it is susceptible to low

response rates (Parsons et al., 2014). The small sample may not be generalizable to the entire population. Future research should utilize other methods of survey distribution to increase response rates. Self-reporting is also a common data collection method. This type of collection method is prone to bias, recall errors, and social desirability reporting (Wash et al., 2017). Future studies using alternative reporting methods should be considered to verify or exclude findings.

Conclusion

This study investigated the human effects on community college security culture. The literature review assessed HEI security research which exposed the linkage between a user's security knowledge, attitude, and behavior and an organization's security posture. During the literature review, the KAB model was discovered to explain the connection between the user's actions and security. In addition, the literature review revealed the HAIS-Q as an information security awareness evaluation tool. The methodology section outlined the processes used to collect and analyze data. The results found that all predictor variables (knowledge, attitude, and behavior) significantly affected the outcome variable (security culture) with knowledge being the most influential. The discussion section identified the findings and discussed the significance and limitations of the research. Recommendations for future studies included further validation of the scaled-down HAIS-Q, identification of specific target demographics for education, and implementation of alternative survey methods to include response rates and quality.

Over the last decade, community colleges have increased their dependency on technology in both the classroom and administratively. The recent growth of cyber-attacks targeting HEIs exposes community colleges to increased cyber vulnerabilities and threats. Historically, HEI security research has not included community college populations (Hina et al., 2019; Kam et al., 2021; Li et al., 2021; Parsons et al., 2017; Wiley et al., 2019; Xu et al., 2023). This study focused on human effects on community college security culture. Understanding the knowledge, attitudes, and behaviors of faculty, staff, and students provides an avenue to identify gaps in security implementation strategies and develop potential gap solutions for leadership.

References

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136. https://doi.org/10.1016/j.chb.2022.107376

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information*, 13(192). https://doi.org/10.3390/info13040192

Durojaiye, T., Mersinas, K., & Watling, D. (2020). What Influences People's View of Cyber Security Culture in Higher Education Institutions? An Empirical Study. *The Sixth International Conference on Cyber-Technologies and Cyber-Systems*. https:// pure.royalholloway.ac.uk/ws/portalfiles/portal/43620729/T_Durojaiye_K_Mersinas_D_Watling_2021_What_influence_people_s_views_of_Cyber_Security_Culture_CYBER21_.pdf

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: A Global Perspective*. Pearson College Division.

Hina, S., Dominic, D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, 87. https://doi.org/10.1016/j.cose.2019.101594

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies*, 28, 439–470. https://doi.org/10.1007/s10639-022-11121-5

Kam, H.-J., Mattson, T., & Kim, D. J. (2021). The "Right" recipes for security culture: a competing values model perspective. *Information Technology & People*, 34(5), 1490-1512. https://doi.org/10.1108/ITP-08-2019-0438

Knapp, H. (2018). Intermediate Statistics Using SPSS. Sage.

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

Le Masson, V. (2023 July 19). The magic number: how to optimize and improve your survey response rate. Retrieved 10 February 2025 from https://www.kantar.com/inspiration/research-services/what-is-a-good-survey-response-rate-pf#:~

Li, L., Shen, Y., & Han, M. (2021). Perceptions of Information Systems Security Compliance: An Empirical Study in Higher Education Setting. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 6226-6231. https://hdl.handle.net/ 10125/71371

Mayfield, A., White, C. C., Downs, T., & Erlandson, D. (2022). Expanding advocacy for community college success. In C. Cutler White (Ed.), *Advocacy for change: Positioning community colleges for the next 75 years. New Directions for Community Colleges*, 197, 13–28. John Wiley & Sons, Inc. https://doi.org/10.1002/cc.20494

Nguyen, B. H., & Le, H. Q. N. (2024). Investigation on information security awareness based on KAB model: the moderating role of age and education level. *Information & Computer Security*, 32(1). https://doi.org/10.1108/ICS-09-2023-0152

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013, 4-6 December). The development of the human aspects of information security questionnaire (HAIS-Q). In Hepu Deng and Craig Standing (Eds.), A*CIS 2013: Information systems: transforming the future: Proceedings of the 24th Australasian Conference on Information Systems*, 1-11. https://www.researchgate.net/publication/286610727_The_development_of_the_human_aspects_of_information_security_questionnaire_HAIS-Q

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computer & Security*, 42, 165-176. http://dx.doi.org/10.1016/j.cose.2013.12.003

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*, 66, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Schrader, P. G. & Lawless, K. A. (2004). The Knowledge, Attitudes, & Behaviors Approach. *Performance Improvement*, 43 (9), 8-15. https://doi.org/10.1002/pfi.4140430905

Thompson, S. (2012). Regression Estimation. In W.A. Shewhart, S.S. Wilks and S.K. Thompson (Eds.), *Sampling*, (1st ed., pp. 115-124). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118162934.ch8

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109. https://doi.org/10.1016/j.cose.2021.102387

Wash, R., Rader, E., & Fennell, C. (2017). Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures. In G. Mark & S. Fussell (Eds.), *CHI'17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2228–2232. ACM. https://doi.org/10.1145/3025453.3025911

Wiley, A., McCormac, A., & Calci, D. (2019). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security,* 88. https://doi.org/10.1016/j.cose.2019.101640

Xu, X., Hong, W. C. H., Kolletar-Zhu, K., Zhang, Y., & Chi, C. (2023). Validation and application of the human aspects of information security questionnaire for undergraduates: effects of gender, discipline, and grade level. *Behavior & Information Technology*. https://doi.org/10.1080/0144929X.2023.2260876